Online ISSN : 0975-4172
Print ISSN : 0975-4350
DOI : 10.17406/GJCST

Global Journal

of Computer Science and Technology: E

Network, Web & Security

Highlights

- Cyber Crime and Its Entext
- Nationwide Level Strategic Method
- Non- Orthogonal Multiple Access
- Techniques and Tools for Cybercrime

Discovering Thoughts, Inventing Future

VOLUME 23 ISSUE 1 VERSION 1.0

Global Journal of Computer Science and Technology: E
Network, Web & Security

Global Journal of Computer Science and Technology: E
Network, Web & Security

Volume 23 Issue 1 (Ver. 1.0)

Open Association of Research Society

Incorporation No.: 0423089
License No.: 42125/022010/1186
Registration No.: 430374
Import-Export Code: 1109007027
Employer Identification Number (EIN):
USA Tax ID: 98-0673427

Global Journals Inc.

*(A Delaware USA Incorporation with "Good Standing"; **Reg. Number: 0423089**)*

Sponsors: Open Association of Research Society
Open Scientific Standards

Publisher's Headquarters office

Global Journals® Headquarters
945th Concord Streets,
Framingham Massachusetts Pin: 01701,
United States of America
USA Toll Free: +001-888-839-7392
USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

Global Journals Incorporated
2nd, Lansdowne, Lansdowne Rd., Croydon-Surrey,
Pin: CR9 2ER, United Kingdom

Packaging & Continental Dispatching

Global Journals Pvt Ltd
E-3130 Sudama Nagar, Near Gopur Square,
Indore, M.P., Pin:452009, India

Find a correspondence nodal officer near you

To find nodal officer of your country, please email us at *local@globaljournals.org*

eContacts

Press Inquiries: *press@globaljournals.org*
Investor Inquiries: *investors@globaljournals.org*
Technical Support: *technology@globaljournals.org*
Media & Releases: *media@globaljournals.org*

Pricing (Excluding Air Parcel Charges):

Yearly Subscription (Personal & Institutional)
250 USD (B/W) & 350 USD (Color)

Editorial Board

Global Journal of Computer Science and Technology

Dr. Stefano Berretti

Ph.D. in Computer Engineering and Telecommunications, University of Firenze Professor Department of Information Engineering, University of Firenze, Italy

Dr. Abdurrahman Arslanyilmaz

Computer Science & Information Systems Department Youngstown State University Ph.D., Texas A&M University University of Missouri, Columbia Gazi University, Turkey

Dr. Lamri Sayad

Ph.d in Computer science, University of BEJAIA, Algeria

Dr. Tauqeer Ahmad Usmani

Ph.D in Computer Science, Oman

Dr. Hazra Imran

Ph.D in Computer Science (Information Retrieval), Athabasca University, Canada

Dr. Magdy Shayboub Ali

Ph.D in Computer Sciences, MSc in Computer Sciences and Engineering, BSc in Electronic Engineering, Suez Canal University, Egypt

Dr. Nurul Akmar Binti Emran

Ph.D in Computer Science, MSc in Computer Science, Universiti Teknikal Malaysia Melaka, Malaysia

Dr. Asim Sinan Yuksel

Ph.D in Computer Engineering, M.Sc., B.Eng., Suleyman Demirel University, Turkey

Dr. Anis Bey

Dept. of Computer Science, Badji Mokhtar-Annaba University, Annaba, Algeria

Alessandra Lumini

Associate Researcher Department of Computer Science and Engineering University of Bologna Italy

Dr. Rajesh Kumar Rolen

Ph.D in Computer Science, MCA & BCA - IGNOU, MCTS & MCP - MIcrosoft, SCJP - Sun Microsystems, Singhania University, India

Dr. Rajneesh Kumar Gujral

Ph.D in Computer Science and Engineering, M.TECH in Information Technology, B. E. in Computer Science and Engineering, CCNA Certified Network Instructor, Diploma Course in Computer Servicing and Maintenance (DCS), Maharishi Markandeshwar University Mullana, India

Dr. Aziz M. Barbar

Ph.D. IEEE Senior Member Chairperson, Department of Computer Science AUST - American University of Science & Technology Alfred Naccash Avenue Ashrafieh, Lebanon

Dr. Federico Tramarin

Ph.D., Computer Engineering and Networks Group, Institute of Electronics, Italy Department of Information Engineering of the University of Padova, Italy

Dr. Chutisant Kerdvibulvech

Dept. of Inf. & Commun. Technol., Rangsit University Pathum Thani, Thailand Chulalongkorn University Ph.D. Thailand Keio University, Tokyo, Japan

Dr. Roheet Bhatnagar

Ph.D in Computer Science, B.Tech in Computer Science, M.Tech in Remote Sensing, Sikkim Manipal University, India

Contents of the Issue

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 23 Issue 1 Version 1.0 Year 2023
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Performance Study of Downlink Users in Non-Orthogonal Multiple Access (NOMA) for 5G Communications

By Mwewa Mabumba, Simon Tembo & Lukumba Phiri
University of Zambia

Abstract- An outline of NOMA principles is provided in this article. Furthermore, this page discusses cooperative NOMA and its variations, explains power allocation in detail as a technique of resource allocation for NOMA, and gives an overview of the research challenges related to NOMA. We then, use a two-case scenario, to suggest a dynamic power allocation (DPA) plan for the downlink NOMA users, albeit it can also be expanded to many use cases. The DPA relies on channel state information (CSI) to guarantee the quality of service (QOS) for cell center customers (user c). The Outage probability (OP) as a critical performance criterion simulation data is also provided, and they demonstrate a notable performance improvement when DPA is employed compared to fixed power allocation.

Keywords: *NOMA, 5G, Power allocation, Cooperative NOMA.*

GJCST-E Classification: *LCC Code: TK5103.2*

Strictly as per the compliance and regulations of:

Performance Study of Downlink users in Non-Orthogonal Multiple Access (NOMA) for 5G Communications

Mwewa Mabumba [α], Simon Tembo [σ] & Lukumba Phiri [ρ]

Abstract- An outline of NOMA principles is provided in this article. Furthermore, this page discusses cooperative NOMA and its variations, explains power allocation in detail as a technique of resource allocation for NOMA, and gives an overview of the research challenges related to NOMA. We then, use a two-case scenario, to suggest a dynamic power allocation (DPA) plan for the downlink NOMA users, albeit it can also be expanded to many use cases. The DPA relies on channel state information (CSI) to guarantee the quality of service (QOS) for cell center customers (user c). The Outage probability (OP) as a critical performance criterion simulation data is also provided, and they demonstrate a notable performance improvement when DPA is employed compared to fixed power allocation.

Keywords: NOMA, 5G, Power allocation, Cooperative NOMA.

I. The Introduction

The newest member of the multiple access family, non-orthogonal multiple access (NOMA), has received praise as a viable way to increase spectral efficiency in fifth-generation (5G) cellular communication networks [1], [2]. A low latency, excellent dependability, enormous connection, superior fairness, and high throughput are among the properties of NOMA, a suggested multiple-access solution for 5G and beyond networks [2] [2]. The multiple access strategies listed below, including FDMA, TDMA, CDMA, and OFDMA, have been implemented in cellular networks of the first through fourth generations [3]. The term "traditional orthogonal multiple access (OMA) technologies" refers to all of these multiple access schemes [4]. The number of users served in OMA is usually tiny, as the number of resources allocated is generally limited. The allocation of resources does not result in intra-cell interference in OMA, making it simple to retrieve data on many users. A new technology known as NOMA is being developed for 5G, which is expected to contribute to the development of novel radio access systems. In a NOMA system, a base station uses a superposition coding algorithm to transmit the users' signals. It also uses interference cancellation techniques to prevent a disturbance at the reception side [5]. The downlink NOMA enables several users to share a single medium at the same time, frequency, or code while using varying power levels [6], [7], which enhances the performance of the channel in several ways, including energy efficiency, fairness, and spectrum efficiency [8]. NOMA allows many users to share the same time, frequency, and code resources at varied power levels, in contrast to traditional orthogonal multiple access (OMA) techniques. The traditional OMA technology struggles to meet the expectations of a growing user base due to orthogonal resource limitations. Strong users benefit from better channel conditions than weak users, who do not [1]. The allocation of a higher power to users with more vulnerable channels is moved by supporting a certain quality of service (QOS) or improving user fairness, and this QOS is usually quantified by $R_i \geq r_i$ where r_i is the minimum required rate for user i [3]. For signal decoding to be accomplished at the reception side, strong users implement the SIC technique while weak users decode their messages by treating the strong users' messages as noise [1]. The received signals are ranked according to the signal-to-interference-noise ratio or the power from the largest to the most minor [9]. In general, user fairness is increased by giving users with good channel circumstances low power and giving users with lousy channel conditions high power [10]. The users served to achieve imbalanced rates, which could be crucial in cases with tight fairness limitations, given that NOMA is based on the SIC order [7]. Power efficiency is vital for ultra-Reliable low latency communications (URLLC) since the NOMA system has a power delay tradeoff, especially when many devices are battery-powered. As a result, we recommend using dynamic power allocation.

Fig. 1. is an example of a two-user downlink NOMA system in the power domain with SIC being implemented at user 1 (user c) and superposition coding at the transmission side where the transmitter transmits multiple users signals at the same time [11], in this case, signals of user c and user e. The transmitted signal is given by:

$$S_t = \sum_{i=1}^{n} \sqrt{P\alpha_i} x_i \quad (1)$$

Author α σ ρ: Department of Electrical and Electronics Engineering, University of Zambia, Box 37392, Lusaka, Zambia.
e-mail: mwewa97@gmail.com

Where: P = total transmitted power, α_i = power allocation coefficient, and x_i = modulated information of users.

The significant contribution of this paper is to theoretically analyze the outage performance of dynamic power allocation strategy that can be applied to a downlink scenario with two users. This PA ensures the quality of service for the cell center user. This power allocation is then used for performance analysis. Mainly, outage probability is used as a criterion to analyze the system performance under two conditions:

1. Considering only the path loss.
2. Taking into consideration both path loss and shadowing.

The rest of the paper is organized as follows: the next section highlights some of the NOMA research challenges, and related works on improving the performance of users in non – orthogonal multiple access, and section III discuss performance improvement of users in NOMA by further breaking it down into two parts, i.e., power allocation and cooperative NOMA, in section IV the performance analysis and outage probability is used as the performance metric, in section V we present the simulation results and discussion, and finally section VI gives the conclusion.

II. Related to Works

When compared to OMA systems, one of the major drawbacks of NOMA is the receiver's complexity brought on by the use of SIC, as well as the added implementation complexity for signal decoding. The complexity of receiving also grows with the number of users in the cell. Therefore, a high-performance nonlinear detection algorithm is required at each stage of SIC, for error-free propagation [12]. Another difficulty unique to the NOMA method is that once a SIC error occurs, all user information is decrypted with errors.This is a flawed SIC and a study topic that NOMA hasn't fully covered yet [13].

In cooperative NOMA, the combined effect of multiple copies of user messages increases the complexity on the user's side and degrades the overall performance. It also increases the system complexity of user cooperation [14].

Due to the many advantages that NOMA offers, recently, the secrecy issue of NOMA has been studied [15]. Since relays re-transmit a copy of the information symbols that are summed up via SC and transmitted over the same frequency band, which means that once the carrier frequency is successfully located by the eavesdropper, all users' messages may be intercepted, the challenge of realizing secure communications with NOMA remains. This is especially true in NOMA cooperative relay networks [16].

Further research and development are required in NOMA to make the 5G goal a reality.

The improved performance of users in NOMA has been studied actively in recent years, and the most common one is the study of fixed power allocation to address the issue. Still, in this power allocation the concentration is on the cell edge user neglecting the cell center user as its quality of service gets compromised. A reversed relay-assisted NOMA network is introduced considering user fairness. The model has been analyzed in terms of all KPIs (e.g., EC, OP, BER) with a more accurate imperfect SIC model and imperfect CSI [17]. As a result, the authors of [18] developed a novel power allocation strategy called a dynamic power allocation scheme that aims to balance service quality for consumers with varying data rates.

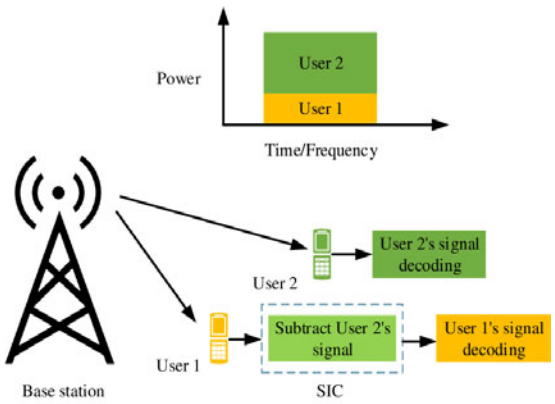


Fig. 1: Power Domain Downlink NOMA System with Two users

The power allocation for NOMA based on proportional fairness scheduling is studied for both max-sum-rate and max–min–rate problems [19].

The performance of different NOMA schemes including two-user MU-NOMA and multichannel NOMA (MC-NOMA), is investigated using optimal power allocation, and the performance measures used are

max-min fairness, sum rate, and energy efficiency for downlink NOMA for performance factors such as sum rate and energy efficiency [5]. A dynamic power distribution approach for the downlink NOMA scheme that ensures user equity by improving the quality of service (QOS) of both users has been looked at in [20]. A downlink NOMA system with cooperative full-duplex relaying is being studied. This technique allows the close user to act as a full-duplex relay for the far-off user.To reduce the likelihood of an outage, they first fix the power allocation (PA) for the base station and nearby users before calculating PA analytically at the BS and relay using closed-form equations [21]. Two scenarios, immediate channel state information at the transmitter and average CSI, have been used to examine power allocation (PA) algorithms that ensure fairness for downstream users [7]. They developed algorithms that produce the best result in both cases. To increase performance for a cell-edge user of two-user NOMA systems in downlink circumstances, two cooperative relaying strategies, namely on/off full-duplex relaying (on/off-FDR) and on/off-half-duplex relaying (on/off-HDR), have been studied [22]. A new definition of fairness based on information theoretic grounds addressed the user fairness issue in power-domain NOMA [10]. The performance of the NOMA scheme in terms of outage probability and achievable sum rate for a fixed power allocation was analyzed [6]. Several major NOMA schemes for 5G have been discussed and compared from the aspects of fundamental principles, key features, receiver complexity, engineering feasibility, etc. Compared to conventional OMA, NOMA allows controllable interferences to realize overloading at the cost of a modest increase in receiver complexity [23]. A method was proposed to adjust the user rate according to the instantaneous channel state information (CSI). First, the optimization problem is transformed into an equivalence problem. By setting some parameters to represent a set of user sum rate allocation problems, constructing a penalty function by the interior point method, and gradually adjusting the penalty factor to solve the extreme point and get the optimal solution [9].

Through this literature review, it could be seen that researchers have tried to improve the fairness of users in NOMA by using cooperative relaying, dynamic power allocation, etc. However, there still exists a research gap in NOMA that ensures the quality of service. To this end, we'll investigate the impact of power allocation on the performance of users in NOMA systems.

III. Performance Improvement of users in Noma

There are several ways in which the performance of a NOMA system can be improved for users. In this section, we outline two essential features that will enhance the performance of a NOMA system, and these are; power allocation and cooperative relaying.

a) Power Allocation (PA) in NOMA

PA plays an important role in NOMA, as users are multiplexed in the power domain [11]. It directly impacts system performance, like interference management, rate distribution, and user admission. An inappropriate PA could lead to an unfair rate distribution among users and system outage due to successive interference cancellation (SIC) failure. When PA schemes are being designed, it is cardinal to scrutinize several things like users' channel conditions, availability of channel state information (CSI), quality of service (QoS) requirements, etc. Some of the PA performance metrics that are widely adopted include the number of admitted users, sum rate, energy efficiency, user fairness, outage probability, and total power consumption [24]. Thus, the goal of PA in NOMA is to achieve either more admitted users, a higher sum rate and energy efficiency (EE), or balanced fairness under minimum power consumption.

There are different types of power allocation, each trying to accomplish a specific goal, such as maximizing the sum rate, the ergodic capacity, energy efficiency, etc [25]. To improve user fairness generally, low power is distributed to users with good channel gain, and high strength is allocated to those with poor channel gain [26]. Recently, in some NOMA systems series, user fairness issues have received attention [6].

As discussed in [27], [28], some fixed power allocation methods are adopted. This plan uses a recursive iteration technique to perform power allocation, where a recursive attribution is a number larger than zero but less than one. More power will be given to the user who has fewer channel conditions. The recursive attribution size, which is determined by the system and is fixed, also affects how much power there is between the two users. It can ensure that users with lower channel gains are given more power, but these users may experience unfairness and may not satisfy different QOS criteria from other users.

The inspiration for us to develop our proposed power allocation scheme that ensures the quality of service for the cell center user was obtained from [18]. The mathematical model of the proposed system is illustrated using equations (2) to (4) and taking the basics of fixed power assignment as the reference.

$$\alpha_e > \alpha_c, \alpha_e + \alpha_c = 1 \tag{2}$$

$$R_e^N = \log_2\left(1 + \frac{\alpha_e |h_e|^2}{\alpha_c |h_e|^2 + \frac{1}{\rho}}\right) \tag{3}$$

$$R_c^N = \log_2(1 + \rho\alpha_c |h_c|^2) \tag{4}$$

Where:

α_e = power allocation for user e

α_c = Power allocation for user c

h_e & h_c = Channel coefficient for users e and c

R_e^N & R_c^N = Data rate for users e and c

ρ = Transmit SNR

b) Cooperative NOMA (C-NOMA)

Cooperative NOMA is another important concept that, when combined with NOMA, improves the system performance for users in downlink transmission, and further improves system efficiency in terms of capacity and reliability [13]. In downlink transmission, channel conditions may vary due to the near-far problem and self-interference. The users in various channel conditions can be categorized as strong or weak. In C-NOMA, the strong users can serve as relays for the weak users, which has the potential to utilize the spatial degree of freedom (DoF) even for users with a single antenna [29]. Furthermore, users in strong channel conditions employ SIC at the receiver in NOMA by decoding messages of users who belong to weak channel conditions is the main advantage in C-NOMA [14]. We will consider a four-node system network, i.e., BS, Users A, B, and C, as shown in Fig. 2 [30]. The BS transmits the message for user A, which is superimposed with symbols of both A and C. Therefore, user A should subtract the messages of users B and C before decoding its message using SIC. Similarly, user C decodes its message C. In this approach, users A and C are considered as relays and forward their messages. As a result, three copies of messages are received via different channels (two copies through the cooperative phase and one from the direct phase).

- *Coordination phase:* Users exchange their source data and control messages with each other and, or the destination. The source user broadcasts its data to both the relay and the destination.
- *Cooperation phase:* Users retransmit their messages to the destination cooperatively. The relay forwards the source's data either by itself or cooperating with the source to enhance reception at the destination [31].

To ensure cooperation among users, different relaying protocols and techniques could be employed, and this depends on the relative user location, channel conditions, and transceiver complexity. The cooperative communication protocols which would be outlined include Amplify and Forward (AAF) and Decode and Forward (DAF) protocols [32]. AAF: was proposed and analyzed in [32], where each user receives a noisy version of the signal transmitted by its partner, then amplifies it and retransmits it to the base station. The base station receives two independently faded versions of the signal and combines them to make better decisions on information detection. The main drawback of this method lies in the fact that noise contained in the signal is amplified as well and is often used when the time delay, caused by the relay to decode and encode the message has to be minimized or when there is limited computing time/power available to the relay.

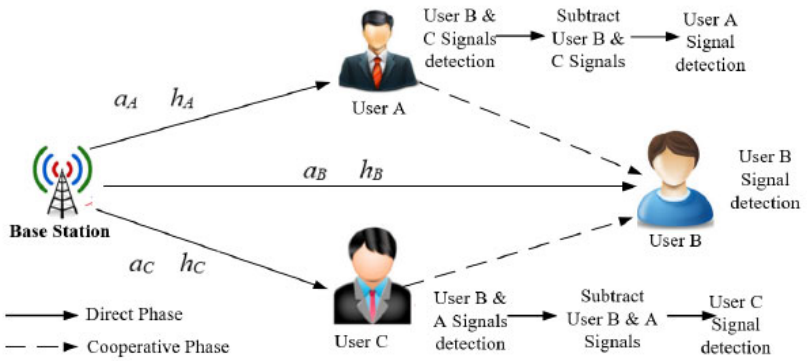


Fig. 2: An Example of Three User Cooperative Relay Network with NOMA

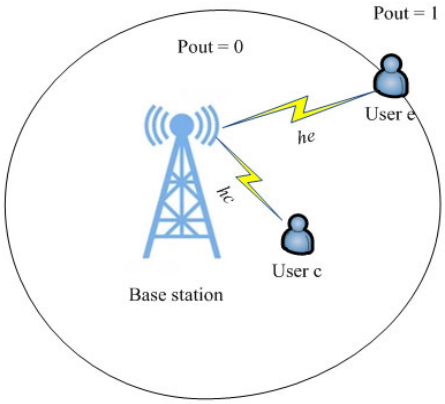
DAF: An example of this can be found in [33]. This strategy follows that the relay station decodes the received signal from the source node, re-encodes it, and forwards it to the destination station. It is the most often preferred method to process data in the relay since there is no amplified noise in the signal sent [31].

IV. Performance Analysis

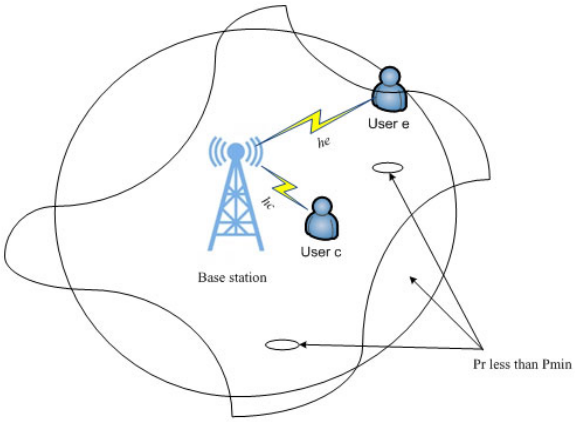
In this section, we analyze the proposed power allocation in terms of outage probability to evaluate its performance and also give an overview of outage probability under two conditions, i.e., path loss only and pass loss and shadowing.

a) Outage Probability (OP)

Outage probability is defined as the point at which the received power (Pr) falls below a given threshold (Pmin) [22]. Fig. 3 shows outage probability under two conditions, i.e., a) considering path loss only, which gives a deterministic model, and b) considering path loss and shadowing which gives a continuous system. In Fig. 3a), the power decay as the users move further away from the transmitter is the same power as received in the circle. When a specific threshold is met, there is no outage, and there is no chance that there will be one. Once the boundary is exceeded probability of being in an outage is one. Fig. 3 b) It can be observed from the shadowing that some parts of the cell are also experiencing an outage, and the received power there is below the threshold.



a) Outage Probability with Path Loss only



b) Outage Probability– Pathloss and Shadowing

Fig. 3: a) & b) Outage Probability

Since NOMA enables users to share a single bandwidth, each user's data rate must not exceed the channel capacity. To offset the latency brought on by SIC, users should decode data at a rapid pace. An outage occurs and data loss results when a user's data rate surpasses Shannon's rate [34]. The generalized expression for the probability of an outage is given below:

$$P_{total} = 1 - P_r\{R_e^N > R_e^T, R_c^N > R_c^T\} \quad (4)$$

Where; R_e^T & R_c^T are target rates for users e and c

V. Simulation Results and Discussion

Through simulation, we assess the effectiveness of the suggested resource allocation strategies in this section. Fig. 4 shows the outage probability achieved by the scheme and is shown as a function of the minimum data rate for the cell edge user when fixed power allocation (FPA) is used and $\alpha_e = 0.95, \alpha_c = 0.05$. The distances from the BS to the users are set at $d_e = 500m, d_c = 100\,m$ for Figs. 4 and 5 and the path loss exponent $\epsilon = 4$. It can be seen from Fig. 4 that FPA is performing very poorly, despite having user c close to the BS, and the probability of the system

failing is relatively high all the time when the target rate is more significant than 4.5 bps. This is because FPA does not take into consideration the channel state information and also does not take the target rate requirements into account.

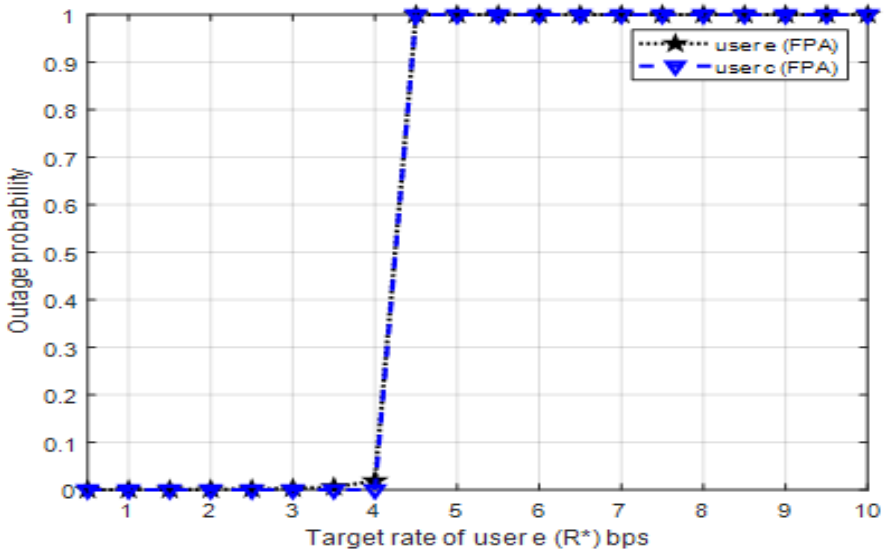


Fig. 4: Relationship between OP and Target rate for user e in DPA for $\mathrm{d_e} = 500\mathrm{m},\ \mathrm{d_c} = 100\mathrm{m}$ from the BS with SNR = 30dBm

For the proposed dynamic power allocation (DPA) in Figs. 5 and 6, it can be seen that there's a lower outage probability because α_e & α_c are dynamically adjusted based on target rate requirements and channel state information (CSI). For DPA in Fig. 5, it is shown that the outage of user ecompared to Fig. 4 has gradual increase as its target rate requirements increase. As the target rate increases, this is the expectation, and the chances of the user e achieving that target rate become lower and lower. This would thus lead to an increase in its outage probability. At 10 bps we see the same failure rate results for both users.

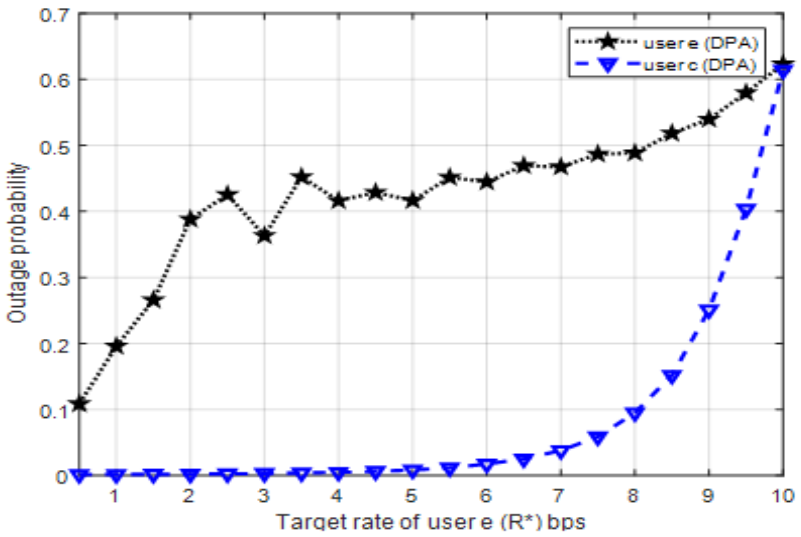


Fig. 5: Relationship between OP and target rate for user e in DPA for $d_e = 500m,\ d_c = 100m$ from the BS with SNR = 30 dBm

In Figure 6, at a data rate of 1 bps we don't expect any failure for the likelihood of being in an outage for user c is at 0, but at 10 bps the probability of being in an outage is at 20% for user c.

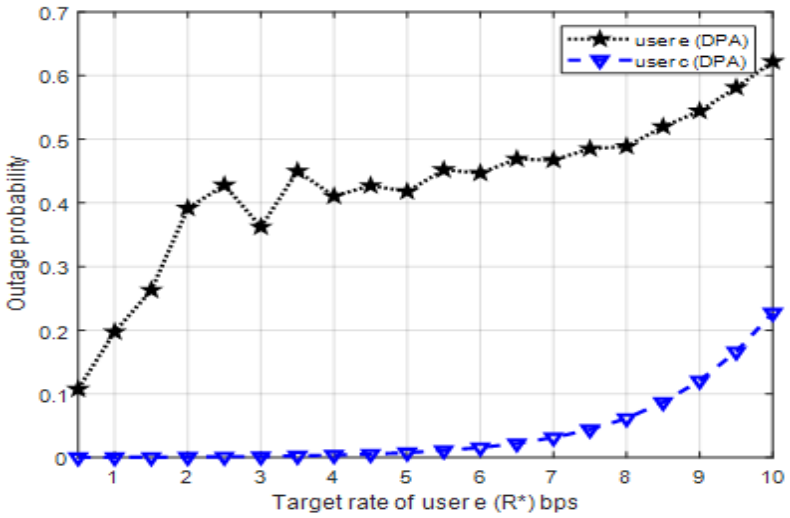


Fig. 6: Relationship between OP and Target Rate for user e in DPA for $d_e = 500m,\ d_c = 10m$ from the BS with SNR = 30 dBm

Meanwhile, at the same speed of 10 bps user e's probability of failure is 62%. Also, it can be seen that at 10 bps user's c's performance improves compared to Fig. 5 as the user is closer to the BS and the probability of failure is at 20%.

The behavior of FPA for varying distances is the same as in Fig. 4 and this is because FPA,as earlier alluded, does not take the CSI into account. From Fig. 5 and 6, it can be seen that as the distance keeps on varying, the performance of user c keeps improving, and we are rest assured that the quality of service for user c is not compromised.

VI. Conclusion

This research study provides a summary of the NOMA principle and goes into further detail about the power allocation resource allocation technique as a means of enhancing NOMA users' performance. It can be seen from the results that the proposed DPA enhances the system performance as compared to FPA. Additionally, we describe the cooperative relaying scheme, which is another technique for enhancing user performance through the employment of relays. Typically, users that have better channel conditions serve as relays. Additionally, we emphasize the research problems that NOMA may face in the future.

References Références Referencias

1. Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li, and K. Higuchi, "Non-orthogonal Multiple Access (NOMA) for Cellular Future Radio Access," in *IEEE Veh. Technol. Conf. (VTC Spring)*, Dresden, Germany, June 2013.
2. T. Shimojo, A. Umesh, D. Fujishima, and A. Minokuchi, "Special articles on 5G technologies toward 2020 deployment," *NTT DOCOMO Tech. J,* vol. 17, no. 4, pp. 50-59, 2016.
3. M. Vaezi, R. Schober, Z. Ding, and H. V. Poor, "Non-orthogonal multiple access: Common myths and Critical Questions," pp. 1-1, 2019.
4. Z. Ding, C. Zhong, D. W. K. Ng, M. Peng, H. A. Suraweera, R. Schober, and H. V. Poor, "Application of smart antenna technologies in simultaneous wireless information and power transfer," *IEEE Commun. Mag.,* vol. 53, no. 4, pp. 86-93, April, 2015.
5. Y. Huang, J. Wang, and J. Zhu, "Optimal power allocation for downlink NOMA systems in multiple access techniques for 5G wireless networks and beyond," *Cham. Springer,* 2019.
6. Z. Ding, Z. Yang, P. Fan, and H. V. Poor, "On the performance of non-orthogonal multiple access in 5G systems with randomly deployed users," *IEEE Sig. Process. Lett.,* vol. 21, no. 12, pp. 1501-1505, 2014.
7. S. Timotheou, and I. Krikidis, "Fairness for Non-orthogonal multiple access in 5G systems," *IEEE Sig. Process. Lett.,* vol. 22, no. 10, pp. 1647-1651, 2015.
8. J. Choi, "Non-orthogonal multiple access in coordinated two point systems," *IEEE Commun. Lett.,* vol. 18, no. 2, pp. 313-316, 2014.
9. J. Li, and Q. Wang, "Power allocation method of downlink non-orthogonal multiple access system based on alpha fair utility function," *Inf. Process Syst.,* vol. 17, no. 2, pp. 306-317, April, 2021.
10. G. Gui, H. Sari, and E. Biglieri, "A new definition of fairness," *IEEE Commun. Lett.,* vol. 23, no. 7, pp. 1558-2558, July, 2019.
11. S. M. R. Islam, M. Zeng, and O. A. Dobre, "NOMA in 5G systems: Exciting Possibilities for Enhancing Spectral Efficiency," *IEEE Tech. Foucs,* vol. 1, no. 2, Jun, 2017.

12. M. Hussain, and H. Rasheed, "Hindawi," 30 November 2020. [Online]. Available: https://www.hindawi.com/journals/wcmc/2020/8845371/. [Accessed 25 May 2023].
13. S. M. R. Islam, N. Avazov, O. A. Dobre, and K. S. Kwak, "Power domain Non-orthogonal multiple access (NOMA) in 5G Systems: Potentials and Challenges," *IEEE Commun. Surveys & Tutorials,* vol. PP, no. 99, pp. 1-1.
14. Z. Ding, M. Peng, and H. V. Poor, "Cooperative Non-orthogonal multiple access (NOMA) in 5G Systems," *IEEE Commun. Lett.,* vol. 19, no. 8, pp. 1462-1465, 2015.
15. Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Trans. Wireless Commun.,* vol. 16, no. 3, pp. 1656-1672, March 2017.
16. D. Wan, M. Wen, F. Ji, H. Yu, and F. Chen, "Non-orthogonal Multiple Access for Cooperative Communications: Challenges, Opportunities, and Trends," Jan 2018.
17. F. Kaya, and H. Kaya, "Improved user fairness in decode - forward relaying non-orthogonal multiple access schemes with imperfect SIC and CSI," *IEEE access,* vol. 8, pp. 97542-97545, June 2020.
18. Z. Yang, Z. Ding, P. Fan, and N. Al-Dhahir, "A general power allocation scheme to guarantee quality of service in downlink and uplink NOMA systems," *IEEE Trans. Wireless Commun.,* vol. 15, no. 11, pp. 7244-7257, Nov, 2016.
19. J. Choi, "Power allocation for max-sum-rate and max-min-rate proportional fairness in NOMA," *IEEE Commun. Lett.,* vol. 20, no. 10, pp. 2055-2058, Oct 2016.
20. M. Mabumba, and S. Tembo, "Dynamic Power Allocation as a way of Improving the Performance of Users in Non-orthogonal Multiple Access for 5G Communications," *IJISRT,* vol. 8, no. 5, pp. 0928-0931, 2023.
21. L. Zhang, M. Xiao, and J. Liu, "Outage probability analysis and optimization in downlink NOMA systems with cooperative full-duplex relaying," in *IEEE 86th Vehicular Tech. Conf.*, Toronto, Sep 2017.
22. T. N. Do,D. B. da Costa, T. Q. Duong, and B. An, "Improving the performance of Cell-edge users in NOMA using Cooperative Relaying," *IEEE J. Sel. Areas Commun.,* vol. 10, pp. 0090-6778, Dec, 2017.
23. L. Dai, B. Wang, Y. Yuan, S. Han, I. Chih-lin, and Z. Wang, "Non-orthogonal multiple access for 5G: Solutions, Challenges, Opportunities, and Future research trends," *IEEE Commun. Mag,* vol. 53, no. 9, pp. 74-81, Sep, 2015.
24. S.M.R. Islam, M. Zeng, O. A. Dobre, and K. S. Kwak, "Resource allocation for down;ink NOMA systems: Key techniques and open Issues," Dec, 2017.
25. M. Atrouche, S. Ayad, and B. Mounir, "Comparative study of fairness and fixed power allocation algorithms in Non-orthogonal multiple access systems," IEEE, 2022.
26. Q. Bi, L. Liang, S. Yang, and P. Chen, "Non-orthogonal multiple access technology for 5G systems," *Telecommunications Science,* vol. 31, no. 5, pp. 14-21, 2015.
27. L. Zhang, "Application of adaptive anti-intersymbol interference in satellite communication," *Journal of Northeast Electric Power University,* vol. 37, no. 3, pp. 103-106, 2017.
28. Z. Sun, and Y. Li, "Hybrid pre-coding algorithm based on sum-rate maximization for millimeter wave MIMO system," *Journal of Northeast Electric Power University,* vol. 37, no. 6, pp. 100-106, 2017.
29. W. Zhiqiang, et al., "A Survey of Downlink Non-orthogonal Multiple Access in 5G Wireless Communication Networks," *ZTE Communications,* vol. 14, no. 4, pp. 17-25, Oct, 2016.
30. U. Samaratunge, R. Dlnis, and D. N. K. Jayakody, "Recent Advances and future Research challenges in Non-orthogonal multiple access for 5G networks," in *VTC Spring*, May, 2018.
31. Wei Lin et al., "Performance Analysis of Cooperative Networks with Random Decode - Forward relaying," in *10th IEEE Int. Conf. High Performance Comput.*, Dalian, Sep, 2008.
32. J. N. Lanemen, G. W. Wornell, and D. N. C. Tse, "An Efficient Protocol for Realizing Cooperative Diversity in Wireless Networks," in *IEEE ISIT*, Washington, DC, June, 2001.
33. A. Sendonaris, E. Erkip, and B. Aazhang, "User Cooperation Diversity Part 1 and Part 2," *IEEE Trans. Commun.,* vol. 51, no. 11, pp. 1927-1948, 2003.
34. L. Bhardwaj, R. K. Mishra, and R. Shankar, "Sum rate capacity of non-orthogonal multiple access scheme with optimal power allocation," *Defense Modelling and Simulation,* 2021.
35. Y. Huang, J. Wang, and J. Zhu, "Optimal power allocation for downlink NOMA systems," in *Multiple Access Techniques for 5G Wireless Networks and Beyond*, Springer Internationl, 2019, pp. 195-196.

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 23 Issue 1 Version 1.0 Year 2023
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Cyber Crime and It's Extent

By Aadesh & Sweetluck

Abstract- Any crime that uses a computer or network is considered a cybercrime, sometimes known as computer crime. People and businesses are exposed to the expanding hazards of cybercrime as a result of their increased reliance on technology. Nowadays, it's pretty typical for us to use computers for our daily tasks. For instance, we use personal computers, smart phones, public surfing areas, and other devices to pay our life insurance premiums, electricity bills, reserve aircraft, train, or bus tickets, order books, and so forth. Since then, the number of people conducting business online has grown quickly due to the ease it offers the user to conduct business without being physically present in the region where the transaction takes place. Along with the rise in cybercrime, there are also an increasing number of users doing online transactions. Online users must be aware of these types of attacks and exercise caution when conducting online transactions due to the rise in cyber attacks. In this context, the paper will review the growth of cybercrimes in India and measures taken by the government of India to combat the cybercrimes.

Keywords: cybercrime, cyberlaw, cybercrimes in india, it act 2000, effects caused by cybercrime, cyber security, extent of the crime.

GJCST-E Classification: DDC Code: 363.25968 LCC Code: HV8079.C65

Strictly as per the compliance and regulations of:

Cyber Crime and It's Extent

Aadesh[α] & Sweetluck[σ]

Abstract- Any crime that uses a computer or network is considered a cybercrime, sometimes known as computer crime. People and businesses are exposed to the expanding hazards of cybercrime as a result of their increased reliance on technology. Nowadays, it's pretty typical for us to use computers for our daily tasks. For instance, we use personal computers, smart phones, public surfing areas, and other devices to pay our life insurance premiums, electricity bills, reserve aircraft, train, or bus tickets, order books, and so forth. Since then, the number of people conducting business online has grown quickly due to the ease it offers the user to conduct business without being physically present in the region where the transaction takes place. Along with the rise in cybercrime, there are also an increasing number of users doing online transactions. Online users must be aware of these types of attacks and exercise caution when conducting online transactions due to the rise in cyber attacks. In this context, the paper will review the growth of cybercrimes in India and measures taken by the government of India to combat the cybercrimes.

Keywords: cybercrime, cyberlaw, cybercrimes in india, it act 2000, effects caused by cybercrime, cyber security, extent of the crime.

I. Introduction

The Internet changes everything. It challenges our beliefs about how things ought to work, including how governments ought to be run, how businesses ought to be operated, how teachers ought to instruct students, and even how housewives ought to create new dishes. It muddles our preconceived notions about what we believe to be true about the world, about one another, and about ourselves. It is simultaneously freeing, thrilling, difficult, and terrifying. Most individuals still find the Internet to be mysterious, intimidating, confusing, and frightening. The Internet has grown tremendously, and with that expansion have come more chances for cybercrime. Since the Internet has spread so quickly over the world, computer crimes have expanded to include not only hacking and cracking but also extortion, fraud, money laundering, software piracy, and corporate espionage, to mention a few. Law enforcement authorities have expressed frustration over lawmakers' incapacity to keep cybercrime legislation abreast of the rapidly advancing technology landscape. Legislators must simultaneously strike a balance between the opposing objectives of individual liberties like free expression and privacy and the necessity to preserve the integrity of the world's public and private networks. In section 2 and 3 of this article, we begin by providing an overview of types of cybercrimes, and their effects. Then in Section 4 we will discuss the extent of it in India and then in Section 5 we will identify the precautions that we can use to stay away from this crime.

Author α σ: e-mail: aadesh47taneja@gmail.com

II. Types of Cyber Crime

Now it is the time to articulate the types of cybercrime:

1. *Identity Theft:* Identity theft, commonly referred to as identity fraud, is a crime where a forger acquires significant pieces of personally identifying information.
2. *Online Scams:* Online scams take advantage of their victims by using internet-connected services or software to commit fraud against them or in some other way exploit them.
3. *Cyber Stalking:* a crime where the perpetrator harasses the victim using electronic messaging, such as email or instant messages, or by posting messages to a website or discussion forum.
4. *Illegal Content:* Illegal content frequently consists of offensive, hurtful, or manipulative material intended for people who are harmed, most often psychologically.
5. *Unwanted Programs:* Despite the likelihood that people downloaded it, a potentially unpleasant programme is one that may be unwanted. They are frequently downloaded along with a desired programme by the user.

III. Effects of the Crime

1. The psychological effects of cyber threats may even surpass those of traditional terrorism, depending on who the attackers and victims are. Online attacks and crimes can cause emotional trauma to victims, which can make them depressed.
2. It may have an effect on an individual's or a family's financial situation. The report concludes that cybercrime costs nearly $600 billion annually, or nearly 1% of global GDP.

IV. Extent of the Crime in India

India, home to the world's second-largest internet-connected population, was no exception to the growing digital village. Our digital societies are open to new vulnerabilities as a result of the world wide web's increased connectivity, despite the fact that it promises significant progress. Cybercrime has expanded at a rate comparable to that of emerging technologies and has no boundaries. Cybercrimes were estimated to have

cost Indian consumers more than 18 billion dollars in 2017. However, these were only estimates based on the numbers that were reported. Due to a lack of cybercrime awareness or classification mechanisms, the actual figures may be under-reported in a country like India. A dedicated online portal for reporting cybercrimes and other recent government initiatives may be to blame for the sudden rise in online crimes beginning in 2017.

When compared to the rest of the country, Uttar Pradesh in the north had the highest number of cybercrimes, with over six thousand cases filed with the authorities in 2018.

That year, Karnataka, India's tech state, followed suit. The majority of these cases were filed under the IT Act. In 2019, India saw a significant rise in the number of cybercrimes reported. Over 44.5 thousand incidents of cybercrime were recorded that year. During the time period that was measured, Uttar Pradesh and Karnataka had the largest proportions.

V. Precautions to be Taken

1. Never share your OTP/Password to anyone.
2. Scan your device on regular basis.
3. Never provide your personal information on your social media.
4. Enable 2 factor authentication on your social media handles.

VI. Conclusion

Despite the fact that not everyone is a victim of cybercrime, they are still at risk. Computer-based crimes come in all shapes and sizes, and not all of them take place behind a computer. The identity of the hacker varies from 12 to 67 years old. The victim would not even be aware that they were being hacked because the hacker could reside on three different continents. The problem of the 21st century is crimes committed via computer. Criminals no longer need to rob banks or be outside to commit crimes, thanks to advancements in technology. Everything they require is in their lap. They no longer have guns as their weapons; They use passwords and mouse cursors to attack. Therefore, you must prepare yourself and adhere to all instructions.

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 23 Issue 1 Version 1.0 Year 2022
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Cyber Security Model for a Roblox-based Metaverse Architecture Framework

By Professor Gabriel Kabanda, Dr. Colletor Tendeukai Chipfumbu & Tinashe Chingoriwo
Woxsen University

Abstract- The adoption of virtual reality (VR) and augmented reality (AR) headsets in futuristic and science fiction has made it possible for the Metaverse to exist as a single, universal, immersive virtual universe. By extending technology outside of our physical reality, the Metaverse alters the human experience. The four categories we use to categorize metaverse definitions are environment, interface, interaction, and social value. Currently, it is unclear what the metaverse's structure and elements are. A cybersecurity framework for these devices is necessary as the world grows more interconnected and immersive technologies are increasingly widely used in business, government, and consumer markets. Used was a literature review. The goal of the study is to create a cybersecurity model for a Roblox-based Metaverse architecture framework that can be applied to internationalization, the value chain of education, and the delivery of online and e-learning education. The research is conducted using the Interpretivist Paradigm.

Keywords: metaverse, augmented reality, virtual reality, internationalization, e-learning, cyber-security, artificial intelligence, machine learning, blockchain technology.

GJCST-E Classification: DDC Code: 721 LCC Code: TH151

Strictly as per the compliance and regulations of:

A Cyber Security Model for a Roblox-based Metaverse Architecture Framework

Professor Gabriel Kabanda [α], Dr. Colletor Tendeukai Chipfumbu [σ] & Tinashe Chingoriwo [ρ]

Abstract- The adoption of virtual reality (VR) and augmented reality (AR) headsets in futuristic and science fiction has made it possible for the Metaverse to exist as a single, universal, immersive virtual universe. By extending technology outside of our physical reality, the Metaverse alters the human experience. The four categories we use to categorize metaverse definitions are environment, interface, interaction, and social value. Currently, it is unclear what the metaverse's structure and elements are. A cybersecurity framework for these devices is necessary as the world grows more interconnected and immersive technologies are increasingly widely used in business, government, and consumer markets. Used was a literature review. The goal of the study is to create a cybersecurity model for a Roblox-based Metaverse architecture framework that can be applied to internationalization, the value chain of education, and the delivery of online and e-learning education. The research is conducted using the Interpretivist Paradigm, which is characterized by a subjectivist epistemology, a relativist ontology, a naturalist methodology, and a balanced axiology. Both the qualitative methodology and the quantitative methodology with an experimental research design were applied. A systematic literature review was conducted on the metaverse, AR and VR. By describing each aspect of the metaverse, we categorized definitions of the metaverse into four categories: environment, interface, interaction, and social value.The interface is based on the level of immersion and there are physical, immersive, and 3D interface options available. There are realistic, unreal, and blended environments in the metaverse. Social networking, teamwork, and persona discourse are the three categories used to describe interaction in the metaverse. A major advantage of 6G is that it facilitates instant communication in phones, computers, wearable devices, robotics, and more. The Cybersecurity model for a Roblox-based Metaverse architecture framework developed is a Bayesian Network, which is a directed acyclic graph that has an associated probability distribution function that can be used for multivariate analysis.

Keywords: metaverse, augmented reality, virtual reality, internationalization, e-learning, cybersecurity, artificial intelligence, machine learning, blockchain technology.

Author α: Adjunct Professor of Machine Learning. Woxsen School of Business, Woxsen University, Hyderabad, India.
e-mails: gabrielkabanda@gmail.com , Gabriel.Kabanda@woxsen.edu.in
Author σ: Department of Information and Marketing Sciences. Midlands State University Faculty of Business Sciences.
e-mail: chipfumbuc@staff.msu.ac.zw
Author ρ: DPhil (Information Technology) Candidate Faculty of Technology, Zimbabwe Open University.
e-mail: chingoriwot89@gmail.com

I. Introduction

The Metaverse is a virtual iteration of the Internet as a single, universal, immersive virtual world made possible by the use of virtual reality (VR) and augmented reality (AR) headsets in futuristic and science fiction. The Metaverse modifies the human experience by extending technology beyond our physical reality. The Metaverse is essentially a network of 3D virtual worlds focused on social connections, potentially exposing students to inappropriate content. Roblox is an open-source platform that can be used for online education to enable interactive 3D virtual environments in physical and online classrooms, with some basic cybersecurity mechanisms. Metaverse is a combination of virtual reality (VR), augmented reality (AR), mixed reality (MR), blockchain, web3, crypto-currencies, social media, etc. Metaverse provides users with a multilingual experience, which is a key requirement for successful internationalization that breaks down language barriers and enables easier and more affordable exchange programs. The metaverse has many advantages in science that outweigh disadvantages such as physical limitations when working with VR and AR. Developing a Roblox-based Metaverse architecture framework is worth investing in promoting internationalization and the education value chain. The Metaverse can be seen as the channel of the future for online /e-learning education. Internationa lization is the extension of the international, cross-cultural, or global aspects of post-secondary education to its objectives and functions, in order to improve the quality of teaching and research for all students and staff as well as making meaningful contributions to the society. It is a deliberate process that we incorporate into our offerings [1].

Internationalization is “a cross-border, cross-cultural approach to the purpose, function and delivery of post-secondary education in order to improve and enhance the quality of teaching and research for all scholars and staff, and to integrate inter- or global dimensions to society” [1]. This description reflects the increased mindfulness that internationalisation has to come more inclusive and less potty by not faste-ning generally on mobility but further on the class and literacy out-comes. The internationalization of higher education (IoHE) has been influenced by the globalisation of our economies and societies and the increased significance of knowledge. IoHE is driven by

a dynam-dynamic and constantly evolving combination of political, profitable, socio-cultural cultural and academic dimensions. These motives take different forms and confines in the different regions and countries, and in institutions and their programmes. Internationalization is primarily motivated by the increased significance of reputation (frequently symbolised by rankings), visibility and competitiveness; the competition for talented scholars and scholars; short-term and/ or long- term profitable earnings; demographic considerations; and the focus on employability and social engagement. Some of the key recommendations for internationali-zation include the following:

Address the challenges of imbalances in credit and degree mobility and inter-institutional cooperation that arise from major differences in higher education systems, processes and funding.

1. Recognize the growing popularity of internships and build options to combine internships with language and cultural training and study abroad.
2. Support the critical role of academic and administrative staff in advancing internationalization of higher education (IoHE).
3. Promote greater cooperation between higher education and industry in relation to student and staff mobility.
4. Pay more attention to the importance of "internationalization at home" and integrate international and intercultural learning outcomes into the curriculum of all students.
5. Remove barriers that prevent joint strength development.
6. Develop innovative models of digital and blended learning as tools to complement IoHE.
7. Direct IoHE towards internationalization at other educational levels (primary, secondary, vocational, adult).
8. Promote bilingual and multilingual learning in primary and secondary education as a basis for diversity-based language policy.
9. To increase opportunities and synergies, remove obstacles to internationalization of research and education at all levels.

Rodoff classified the metaverse into seven layers: infrastructure, human interface, decentralization, social computing, the creator economy, discovery, and experience [2]. The metaverse can be successfully used in E-Learning as a solution for subjects that rely entirely on convergence and cannot be taught online or through distance learning, such as medical and engineering courses. Although there are many different types of E-Learning environments, metaverse-based systems can also be used to provide safe and efficient environments for education and business by utilizing virtual reality technologies and continuously researching and attempting to expand learning experiences [2]. As a result, all known learning systems will rely on the virtual learning environment in the metaverse (VLE). The metaverse also incorporates the Internet, web technologies, and virtual reality. The Metaverse roadmap, according to [2], is divided into four sections: augmented reality, life logging, mirror worlds, and virtual worlds. A roadmap of this type can be divided into four dimensions: external, extended, intimate, and simulative [2], with specific techniques such as content editing, smart devices, VR, AR, blockchain, digital twin, XR, cloud computing, and avatars being used in various proportions.

a) Background

One of the major expectations and focuses of Industry 4.0, the architecture of the Fourth Industrial Revolution, is to connect the digital/cyber/virtual world with the physical world, hence the emphasis on cyber-physical systems. Virtual and augmented reality can play a role in the early stages of true business transformation, where optimization and productivity gains (quantity, quality, speed, and flexibility) are more important than late stages. Augmented Reality (AR) is a digitally enhanced version of the real physical world that uses technology to deliver digital visuals, sounds, or other sensory stimuli. Augmented Reality (AR) enhances your surroundings by incorporating digital elements into your live view, which is frequently accomplished through the use of your smartphone's camera. Augmented reality experiences include Snapchat lenses and the game Pokemon Go. Augmented reality can be used by retailers and other businesses to promote their products and services, launch novel marketing campaigns, and collect unique user data. Unlike virtual reality, which creates its own cyber environment, augmented reality simply adds to what is already there. Virtual Reality (VR) refers to a completely immersive experience in which the physical world is absent. VR immerses people in experiences, often using much more expensive technologies such as headsets. As a result, virtual reality (VR) is a fully immersive experience that simulates the real world.

Users of VR headsets like the HTC Vive, Oculus Rift, and Google Cardboard can experience both real-world and fantastical settings, such as being in the center of a noisy penguin colony or riding a dragon. Contrarily, augmented reality often uses a real-world view of something (such as a mobile phone camera) as the basis before projecting or pasting the image onto a screen or viewer. Table 1 below provides an illustration of how the distinction between VR and AR depends on the device you desire and the experience itself.

Table 1: Difference between AR and VR

Augmented Reality (AR)	Virtual Reality (VR)
AR uses a real-world environment	VR is completely virtual
AR users can control their presence in the real world	VR users are controlled by the system
AR can be accessed with a smartphone	VR requires a headset device
AR augments both virtual and real worlds	VR only augments fictional reality
AR enables individualized learning and improves the learning process	VR enables immersive learning in an interactive environment. The education sector will benefit from these new opportunities.
AR offers a wide range of applications that are constantly being improved, and can increase accuracy and efficiency	VR users can explore all facets of the virtual world.
Experience and knowledge can be shared over long distances	Experience is not easily shareable.

We must first employ sensors and cameras to acquire data about the user's actual surroundings in order to develop AR. In order to generate immersive interactions, realistic augmented reality also needs powerful computation to analyze inputs like acceleration, location, pitch, and depth in real time. The use of projection allows augmented reality devices to add a digital rendering to the environment after gathering data from the actual world. Future educational systems will primarily use virtual learning environments. It is crucial to keep such a structure in place to protect future generations. In order to create a future e-learning environment and offer a thorough and efficient educational process, it is crucial to integrate new and difficult technology [2].

This study investigates how the metaverse functions and what unique technologies are there in it. There is no agreement on the layers, the number of levels they should have, or what should be included in one layer and omitted from another despite the fact that numerous scholars have proposed layers for the metaverse framework or architecture. Numerous systems that operate within or make use of the metaverse have also been proposed, although they are unable to fully benefit from the metaverse's advantages. The suggested virtual learning environment ELEM, which was modified from the Metaverse framework used by [2], is seen in Figure 1. A user, several devices, and a metaverse component made up of infrastructure, avatars, and technologies make up ELEM for the metaverse [2].

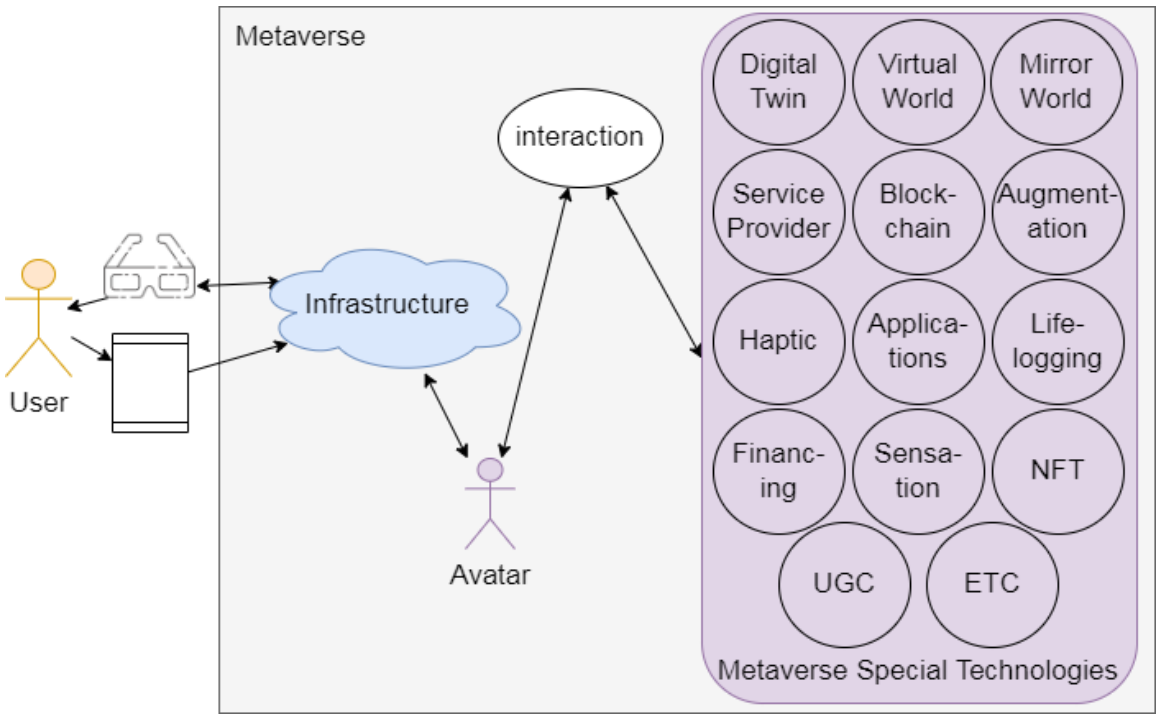


Figure 1: Metaverse Framework (Source: [2], page 8)

There are currently no rules to reduce the security and privacy hazards of the metaverse because it is a relatively new phenomenon. Our ability to trust the technology that underpins virtual experiences is severely compromised as a result. Cybersecurity is a technique for defending against online attacks on programs, networks, and systems [3] defines cybersecurity as the defense of programs, networks, and systems against harmful digital attacks. To defend the confidentiality, integrity, and accessibility of computer resources, networks, software, and data from intrusion, a variety of policies, tactics, technologies, and procedures are used in cybersecurity. Intrusion detection and virus detection are the two key applications in cybersecurity. The following traits characterize current cybersecurity trends:

- Phishing and Social Engineering, which includes sending fraudulent emails that look like emails from legitimate sources
- Ransonware, a type of malicious software commonly used to extort money by blocking access to files and computer systems until a ransom is paid
- Vulnerability to the Internet of Things (IoT)
- Cloud vulnerabilities and cloud security
- Third-party vulnerabilities
- Internal attacks
- Compliance with data rights

A blockchain is a data structure that is kept in many databases and contains transaction records in the form of a block. When replicated, it functions primarily as a Digital Transaction Ledger (DLT) spread over a computer network [3]. Each transaction in a block is added to the ledger of each participant. A block is a collection of transactions. One of the most well-known applications of blockchain technology is cryptocurrency. Digital money protected by encryption are known as cryptocurrencies, which make counterfeiting and double-spending practically impossible. Peer-to-peer networks, distributed consensus, and public key cryptography are the main foundations of blockchain technology. According to [3], the following six elements are required to create a robust blockchain technology network:

- *Cryptography:* Block-hain transactions are validated and secure due to the complex calculations and cryptographic evidence among involved parties;
- *Immutability:* Any records created in a block chain cannot be altered or removed;
- *Provenance:* Refers to the ability to trace each transaction's lineage inside the block-chain ledger;
- *Decentralization:* Each participant in the block-chain structure gets access to the entire distributed database due to decentralization. The consensus algorithm enables network control as contrasted to the centrally-based approach;
- *Anonymity:* Each member of the blockchain network is anonymous; they just have a created address, not a user identity. This protects user privacy, particularly in a public block-chain setup;
- *Transparency:* The block-chain system cannot be corrupted. Since it takes a lot of computer power to totally wipe the blockchain network, this is extremely unlikely to occur.

b) Statement of the Problem

Network Intrusion Detection Systems (NIDS) have increased due to the rapid developments of the internet. NIDS distinguishes between legitimate network users and malicious users, monitors system usage, and identifies behavior that violates security policies. Traditional firewall protection and similar mechanisms have proven inadequate as hackers deliberately circumvent firewall protection. Therefore, it is fundamental to find effective solutions that can dynamically and adaptively defend network systems. Cryptocurrencies are growing in popularity and countries around the world are finding it difficult to manage them. So far, many developing countries have not enacted regulations on cryptocurrencies.

c) Main Purpose

The objective is to develop a cybersecurity model for a Roblox-based Metaverse architecture framework that can be used in internationalization, education value chain, and online /e-learning education delivery.

d) Research Objectives

The key research objectives of the research are to:

1. Review the Virtual Reality (VR) and Augmented Reality (AR) architectural frameworks concerning their suitability for education delivery purposes.
2. Ascertain the institutional capacity building requirements for a Metaverse-based academic virtual environment.
3. Determine the challenges associated with copyright and intellectual property (IP) violations faced by universities and Professors with regards the learning materials against for use in a metaverse environment.
4. Assess the cybersecurity risks of a Roblox-based Metaverse educational environment and their impact on internationalization and the education value chain.
5. Develop a cybersecurity model for a Roblox-based Metaverse architecture framework that protects users from cyber-attacks.
6. Investigate how Blockchain technology may be effectively used to handle payments on the metaverse-based education value chain.

e) Research Questions

The research questions include the following:

1. What is the suitability of VR and AR architectural frameworks for online education delivery?

2. What are the capacity building requirements for the required investment in training academics, students and administrative staff in delivering metaverse programmes and courses?
3. How can universities and Professors safeguard their learning materials against copyright and intellectual property (IP) violations?
4. How can we develop a cybersecurity model that protects the academic space from unnecessary intrusion into and surveillance of their online classrooms?
5. In what way can user-generated content and a chat features on Roblox be protected from intrusion by predators or people posting pornography or other illegal material?
6. How can Blockchain technology be effectively used to handle payments on the metaverse-based education value chain?

II. Literature Review

a) Systematic Literature Review of Metaverse, Virtual Reality (VR) and Augmented Reality (AR)

Augmented reality is designed to move freely. In other words, whether it is a smartphone application or a pair of smart glasses, visuals are projected onto whatever you're looking at. In virtual reality, VR headsets like the Oculus Quest and Valve Index are used to entirely take over the wearer's field of vision for a 360-degree immersive perspective of his outside world swap out the sight. Between augmented reality and virtual reality, mixed reality provides an improved version of augmented reality. Immersive and realistic virtual worlds are fully enhanced by combining the visual powers of AR/VR with the cognitive skills of AI, improving entertainment, meetings, and even casual hangouts with far-flung friends and family. Virtual worlds have been utilized in the context of software engineering education (SEE) to enhance learning outcomes [4]. Typically, a person enters a metaverse (parallel virtual world) using a virtual reality (VR) equipment, enters the actual world through a digital avatar (by analogy with the user's physical self), and lives there. There is more to the Metaverse than just games and online communities. Ball [4] asserts that the Metaverse is "a vast, open network of 3D virtual worlds produced in real-time that can sustain an almost infinite number of users while maintaining individual presence and data continuity. Identity, history, rights, objects, communications, and payments are among the things that can be experienced simultaneously and persistently". Extended Reality (XR), Artificial Intelligence (AI), Blockchain, Non-Fungible Tokens (NFTs), Edge Computing, Digital Twins, Human-Computer Interaction, Immersion, Sense of Presence, and Affordances are just a few of the technologies and concepts that make up the Metaverse [4]. Research in VR and AR that is theory-based is lacking.

The use of the metaverse in Software Engineering Education (SEE) enables experiences that effectively teach software processes, allowing the student to take on the lead roles in software projects, using techniques of specific development process models, navigating in different environments (such as meeting rooms and programmers' rooms), communicating with other avatars, and interacting with and viewing Unified Modeling Language (UML) diagrams in the same way that they are seen in real-world software projects. [4] conducted a thorough analysis of the literature that took into account 105 published documents from Google Scholar and Scopus, including articles, book chapters, conference papers, conference reviews, and reviews. The systematic review work by [4] highlighted the Metaverse elements, digital currencies, AI applications in the virtual world, and blockchain-empowered technologies to discuss how blockchain and AI fuse with the Metaverse. These were some of the key findings. Notably, technological aspects of the blockchain-based Metaverse approaches, such as data collection, storage, sharing, interoperability, and privacy protection, have been examined. The research clearly illustrated the technological difficulties of the metaverse before emphasizing how blockchain may be useful. Identity, Data, Privacy, Network, Economic, Physical/Social Impact, and Governance are the categories used to group common security risks in the metaverse. From the standpoint of technology adoption, [4] begins with an expanded technology adoption model, describing how developers might expand the metaverse to satisfy user expectations and improve user interaction with this technology. On the network side, noteworthy computational, metaverse, and cloud edge-end computational difficulties, solutions, and concepts were emphasized. In software engineering, using 3D visualization is already a common technique. The portrayal of computer programs, related documents, and data that improves, streamlines, and clarifies the software engineer's mental description of how a computer system functions is known as software visualization, which is a subfield of information visualization [4]. Authoring Tools, Devices, Economy, Infrastructure, Interaction, Physical World, Security, Storage, Technology, and Virtual World are some of the major elements and technologies of the SEE metaverse, according to [4].

Early conceptual articles on VR and AR addressed possible technological applications and proposed that increased sensory acuity and breadth will alter and expand channels for information delivery [5]. The most often used definition of VR is the real-time simulation of one or more people utilizing a 3D artificial environment that they can explore and interact with [5] More specifically, the three essential components of

VR are: (1) Visualization, which allows the user to look around, typically with the aid of a head-mounted display; (2) Immersion, which induces suspension of disbelief and physically realistic representations of objects; and (3) Interactivity, which refers to the degree of control over the experience and is typically accomplished with sensors and an input device like joysticks or keyboards [5]. The terms virtual environment and virtual world are widely used in VR research. Immersion in a virtual setting gives the user the full VR experience. A persistent virtual environment that is available around-the-clock, where users can generate content, play games, and engage in real-time interaction is known as a virtual world (personal representations in 3D format).

Augmented Reality (AR) can generally be defined as augmenting the real-world environment with layers of computer-generated imagery by the device [5]. AR can almost certainly be considered a variant of VR. AR and VR are therefore at different ends of the real-virtual continuum, with one end consisting entirely of real-world objects and the other consisting entirely of synthetic or man-made objects. The difference for users is the level of immersion. In AR, much of what the user sees is still the real world, but in VR, the user is completely immersed in a virtual environment. Tourists happily escape to familiar simulated experiences such as Disneyland and become completely immersed in step-by-step alternate realities [5]. In fact, [5] argued that the application of VR/AR into the tourism experiences merely pushes this alternate reality one-step further. Research has shown that VR's greatest strength is its ability to visualise spatial environments, which is especially crucial in tourism where products are intangible and are confidence goods which consumers are not able to test in advance. Putting on a VR headset and being able to compare different destinations could help consumers make informed decisions found that for theme parks, virtual experiences provided more effective advertising compared to brochures due to the richness and interactivity of the information [5]. Studies show the ultimate goal for web based destination marketing is to provide travel information to tourists via a vicarious experience of the destination to persuade them to visit, and so VR can cater specifically to the vicarious experience by allowing the user to experience selected visual, audio, and most importantly, spatial aspects of the destination without actually being there [5]. Research conducted by [5] identified the gaps and challenges associated with VR/AR as centered around four main themes: 1) awareness of the technology; 2) usability; 3) time commitment required to learn; and 4) the willingness to replace corporeal experiences with virtual ones.

Virtual reality experiences in educational contexts are becoming increasingly important as this technology increases learner motivation and achievement through learning transfer, problem-solving skills, educational equity, and multisensory learning [6]. With the 4th Industrial Revolution and his COVID-19, there is a renewed interest in virtual reality. Technological developments such as head-mounted displays (HMD), controllers, and motion tracking systems, as well as content that applies virtual reality to games, movies, advertisements, Museum exhibits, and education, are progressing rapidly in various fields. [6]. Virtual Reality (VR) refers to the real world like simulated environments artificially created by computer technology [6]. VR aims to create immersive and interactive experiences based on highly realistic visual and auditory stimuli and rich feedback by tracking the user's position, movements and decisions. VR-based teaching has the potential to improve learner motivation, engagement, satisfaction, and transfer of learning [6].

The general definition of augmented reality (AR) is the use of a technology to add layers of computer-generated imagery to the physical environment [6]. It is almost probable that AR is a subset of VR. As a result, AR and VR are at opposite extremes of the real-virtual continuum, with one end totally made up of objects from the actual world and the other entirely made up of artificial or man-made objects related to something created by a computer. The amount of immersion is what makes a difference for users. In contrast to VR, which entirely immerses the user in a virtual environment, AR allows users to view a large portion of the real world. Tourists enthusiastically flee to well-known simulated attractions like Disneyland and fully immerse themselves in step-by-step parallel realities [6]. Earth science engineering education, medical education, STEM education, math education, computer science education, higher education, heritage education, and rehabilitation management of breast cancer survivors are some of the VR education applications listed in [6]. daily activities in chronic stroke patients; therapies for PSTD; studying a foreign language; K–12 and higher education; training in surgery, industrial skills, cognitive training for those with minor cognitive impairment; Education in science, sensorimotor skills, dentistry, and nursing; Training in evacuation; Virtual reality therapy for social anxiety disorder; neuropathic treatment Parkinson disease rehabilitation; education in anatomy and physiology, etc.

Via augmented and virtual reality technology, the metaverse has the potential to expand the physical world by enabling people to interact naturally in both real and simulated surroundings using avatars and holograms [7]. Virtual worlds and immersive games (like Second Life, Fortnite, Roblox, and VR Chat) have been referred to as the forerunners of the metaverse and provide some context for the possible socio-economic effects of a fully developed persistent cross-platform metaverse. Given that there is likely to be some blurring of the barriers between physical and digital, the potential influence on how we conduct business, engage with brands and people, and create shared experiences

might be profound. Although the infrastructure and technology to create new immersive virtual worlds on a large scale, one that human avatars might traverse between platforms, do not yet exist, researchers are increasingly looking at the transformative influence of the metaverse [7]. Marketing, education, healthcare, social interaction factors from widespread adoption, concerns with trust, privacy, bias, and the application of the law, as well as psychological impacts associated to addiction and an influence on weaker people, are just a few of the areas that will be impacted. The Metaverse has been defined as a new version of the internet that integrates the real and virtual worlds in a novel way using VR headsets, blockchain technology, and avatars [7]. Through the use of VR headsets, haptic gloves, AR, and Augmented Reality (XR), the technology that permits the construction of the Metaverse is quickly evolving and enabling users to engage in highly engaging and immersive experiences. Marketing, travel, leisure, hospitality, citizen-government interaction, health, education, and social networks might all be transformed if firms were able to modify their business models and operational capacities to function in the metaverse [7]. The many effects of a fully operational, immersive metaverse, where users can easily switch between the virtual and physical worlds within a network, are now being studied by researchers.

b) Cybersecurity Model for the Education Value Chai

Cybersecurity awareness is the degree to which internet users comprehend the significance of information security, as well as their obligations and actions to apply information security controls effectively to safeguard the networks and data of the enterprise [8]. Cybersecurity awareness in this context refers to the capacity to recognize potential threats to cyberspace, evaluate the risks, and quickly prevent or resolve issues in cyberspace to safeguard personal information and real estate security [8]. People today need a variety of digital skills to succeed in their profession and daily lives because they may take advantage of more chances as digital technology develops. This is necessary due to the growth of the digital economy and an increasingly digitalized society around the world. Across many education value chains, emerging information and communication technologies (ICTs) have led to creative new approaches to teaching and learning. Education value chains are characterized as hybrid relationships between educational systems or processes and other social and economic agents with the goal of enhancing educational quality and addressing issues encountered in the real world [9]. However, the value chain in education has developed into an appealing and fruitful environment for cyber-attacks [10]. The National Initiative for Cybersecurity Education (NICE Framework) was developed in response to these dangers with the goal of promoting cybersecurity training, education, and employee development.

c) National Initiative for Cybersecurity Education (NICE Framework)

The NICE framework is anchored on pillars that describe the categories, specialty areas, tasks and the knowledge, skills and abilities required to perform work for a certain role. Categories are a high level grouping of common cybersecurity functions that include Security Provisionals (SP), operate and maintain (OM), Oversee and Govern (OV), Protect and Defend (PD), Analyze (AN) and Investigate (IN) [11]. Specialty areas are distinct areas of cybersecurity work such as Training, Education and Awareness. The components of this framework and associated examples according to [12] are displayed in Table 2.

Table 2: NICE Framework Components Explained

NICE Framework Component	Example
Category	Oversee and Govern (OV)
Specialty Area	Training, Education, and Awareness (TEA)
Work Role	Cyber Instructional Curriculum Developer/Cyber Instructor
Task	Develop or assist in the development of computer based training modules or classes
Knowledge	Knowledge of organization issues, objectives, and operations in cyber as well as regulations and policy directives governing cyber operations
Skill	Skill in evaluating information for validity, reliability, and relevance
Ability	Ability to craft curriculum suitable for virtual environment

The NICE Framework can be used in the education value chain in the identification of training and qualification requirements for the development of critical Knowledge, Skills, and Abilities to execute cybersecurity tasks [13]. The framework serves as a reference or cybersecurity dictionary for educators in crafting curriculum, certificate or degree programs as well as training programmes or experiments that involve the Tasks, Knowledge and Skills described in the NICE Framework [12]. This in turn ensures that graduates produced have the requisite cybersecurity knowledge and skills that the industry and employers seek. That way the education curriculum across the whole education value chain remains relevant and in sync with the demands of industry.

d) Evaluation of the Roblox Architecture

The Roblox Client, Roblox Studio, and Roblox Backend are the three essential components of the Roblox Platform, which has a client-server design. The Roblox Client is the engaging front-end user interface that enables user login so that they may explore, interact with, and take part in the 3D virtual world. It is available through PCs, laptops, and mobile devices. A downloadable program called The Roblox Studio is used to design user interfaces. On the Roblox platform, it makes building, publishing, and gameplay possible. When developing various experiences, the Studio contains a ton of templates and ready-to-use materials, including 3D models and animations. The Roblox Backend is the pillar that holds a number of backend services, and the Roblox Cloud, which is essentially the platform's infrastructure and allows for the delivery of services like 3D simulations, is housed there [14]. The front-end of Roblox is shown on Figure 2.

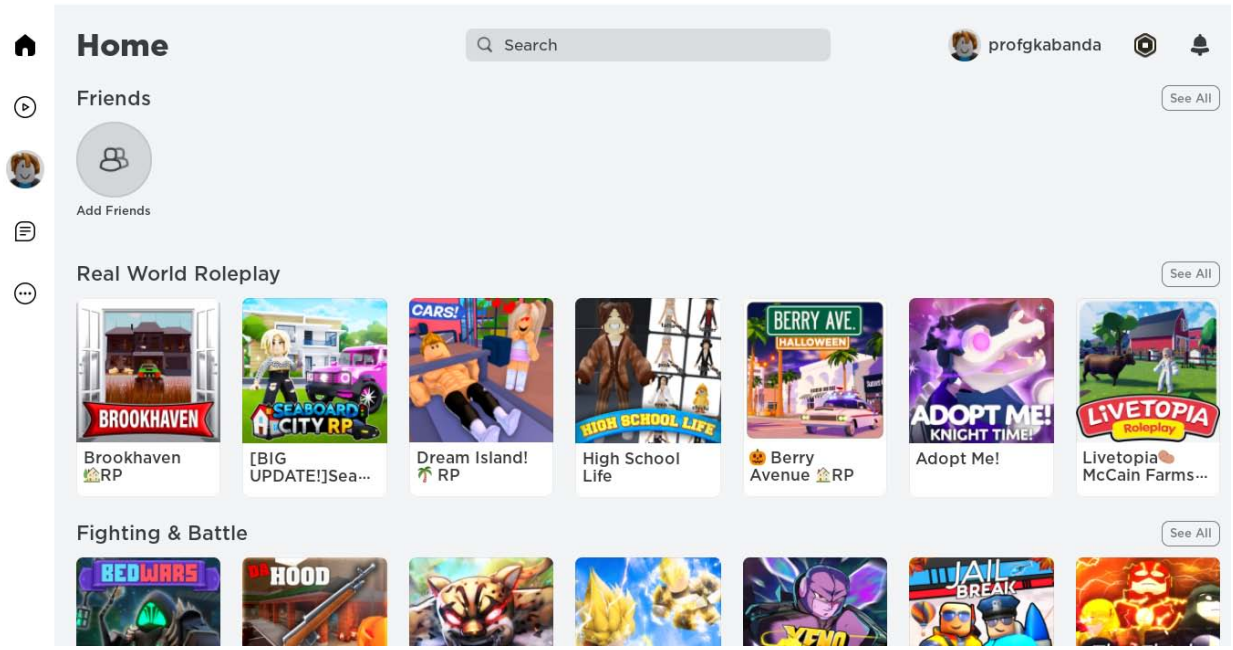


Figure 2: The Roblox Front-End

Roblox uses virtual reality to let users develop and create immersive learning environments, which boosts novelty and encourages a rise in the use of teaching and learning [15], [16]. Students that engage in immersive learning are also inspired to build the resources they employ, changing them from knowledge consumers to creators of knowledge. It makes it possible for educators from all tiers of the education value chain to use innovative teaching strategies that equip students with the abilities to foster creativity in a fun learning environment [17], [18]. The Roblox design also provides the best framework for online learning, role-playing, and promoting entrepreneurship [19] and digital citizenship [17]. The Roblox platform, which is based on the use of VR technology and the metaverse principles [21], provides students with a wide range of virtual collaboration abilities and opportunities [20]. These acquired abilities will also be available to be transferable across numerous communities. The advantages of virtual reality, however, are equally essential for creating a comfortable and safe online social environment for students of various skill levels [22].

On the other hand, it is possible that the current security frameworks will not be sufficient to handle the expanding attack surface that spans beyond only computers and networks [18]. The new models or frameworks for safety and security in the Metaverse that Roblox is based on must consequently take human psychology and the human brain into account [23]. Given the lack of anonymity in the metaverse-based Roblox architecture, confidentiality concerns are also of major concern. As a result, increased user awareness is necessary so that students can avoid the dangers presented by the immersive surroundings. The Roblox platform may additionally pose psychological risks, including as addictions [24]. In this sense, it is vital to recognize that the metaverse is still evolving, and as a result, users of platforms like Roblox may find it difficult to trust the platform due to security flaws. Additionally, because it depends on the convergence of a number of technologies that serve as enablers, such as virtual reality (VR), augmented reality (AR), edge networks, 5G, and artificial intelligence, it might take some time for it to be integrated into the value chains of education,

particularly in developing nations. These technologies have not yet been adopted in these nations.

As the Roblox metaverse has grown in popularity, numerous brands have used the Roblox game engine to create games that incorporate real-world advertisements. The majority of businesses in the Roblox metaverse create video games that advertise actual goods and occasions. For instance, a movie producer might create a game that promotes a forthcoming movie as well as potential partners' brands from industries outside than entertainment. As a result, Roblox has ingratiated itself into pop culture, collaborating with companies like Nike and television series like Stranger Things. Roblox has also merged the goods and universes of these companies into a number of immersive games.

e) The Hadoop Architecture Framework

The file system, Map Reduce engine, and Hadoop Distributed File System are all included in the Hadoop architecture (HDFS). MapReduce engines come in two flavors: Map Reduce/MR1 or YARN/ MR2. Map Reduce [34]. A framework called "map reduce" is intended to process a lot of data concurrently and widely across a group of processing units. A single master and numerous slave nodes make up a Hadoop cluster. Data Node and Task Tracker are on the slave node, whereas Job Tracker, Task Tracker, Name Node, and Data Node are on the master node. The framework aims to simplify interaction with huge data. Through the use of straightforward programming concepts, it enables the distributed processing of big datasets across computer clusters. The Hadoop architecture has established itself in businesses and industries that must work with massive, sensitive data sets that require effective processing [34]. As a result, the Hadoop framework is a framework that permits the processing of huge data sets that are organized into clusters. The Hadoop architecture consists of a number of modules supported by a sizable ecosystem of technologies and offers a range of services to address big data issues [35]. It consists of Apache projects as well as a number of paid tools and services. Most of the time, these important components are supplemented or supported by tools or solutions. Together, these instruments can offer services including data absorption, analysis, storage, and maintenance.

Hadoop Distributed File System (HDFS), Processing/Computation layer *(Map Reduce), Yet Another Resource Negotiator* (YARN), and *Hadoop Common* are the four main components of the Hadoop architecture [36]. The Hadoop framework application operates in a setting that offers distributed computing and storage across computer clusters [37]. The Hadoop framework is made to expand from a single server to tens of thousands of servers, each of which provides local computing and storage [38]. Numerous significant corporations, including Facebook and Google, have used Hadoop, a well-liked open source MapReduce implementation [39]. The Hadoop framework is presented in Figure 3.

The main or most important part of the Hadoop ecosystem is *HDFS,* which is in charge of storing massive amounts of structured and unstructured data across numerous nodes while also keeping the metadata in the form of log files [35]. It is made up of a Name node (which carries Meta data, or information about data), and a Data node (stores the actual data). HDFS is a file system that was specifically created to store enormous datasets on commodity hardware, storing data in diverse forms on numerous devices [40]. The Name Node and the Data Node are HDFS's two constituent parts. The master daemon is the Name Node [41]. There is just one Name Node that is active. It stores all the infomation and controls the Data Nodes. The slave daemon, however, is Data Node. There can be multiple Data Nodes and its purpose is for storing the actual data.

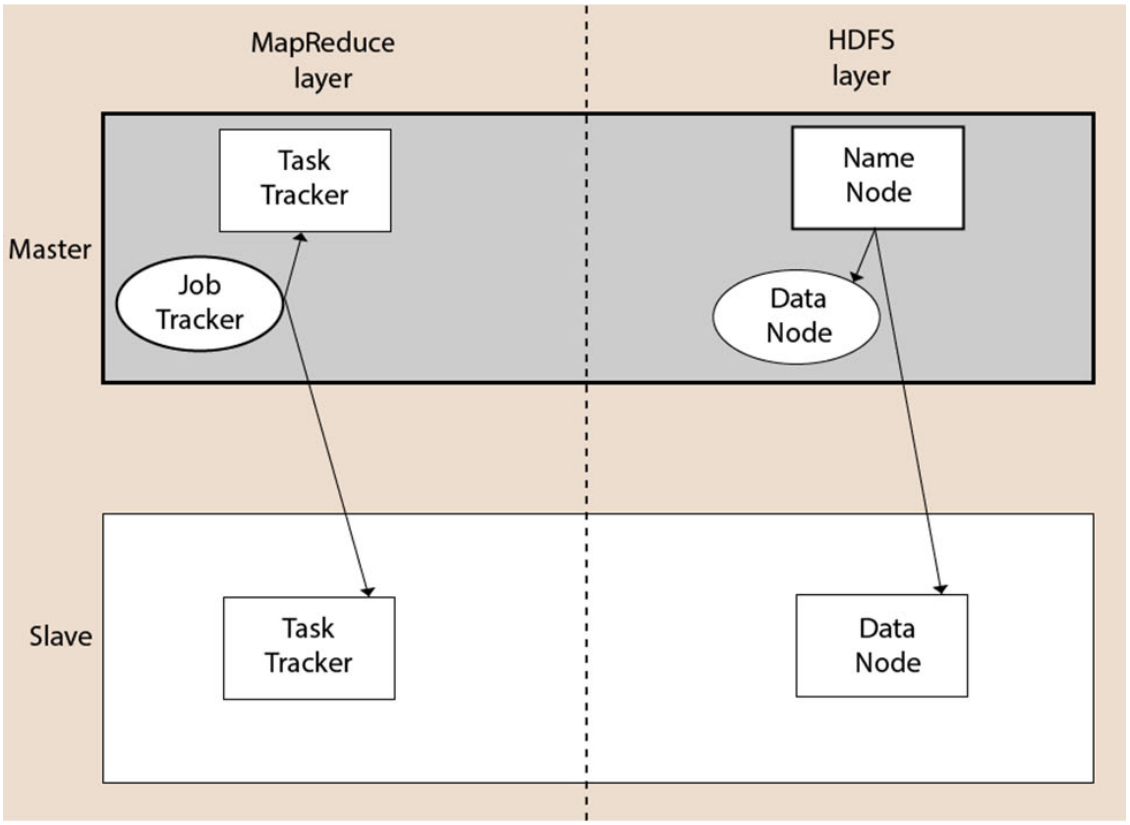


Figure 3: Hadoop framework

The *Yet Another Resource Negotiator* (YARN), which aids in managing resources across clusters, is the other part of the Hadoop framework [42]. For the Hadoop System, it manages scheduling and resource allocation. There are two parts to YARN. The master daemon is Resource Manager (Master). It controls how resources like CPU, memory, and network bandwidth are distributed. The slave daemon, NodeManager (Slave), reports resource utilization to the Resource Manager.

Another component is *Map Reduce.* By utilizing distributed and parallel algorithms, Map Reduce enables the continuation of the processing's logic and aids in the creation of applications that reduce large data sets to manageable ones [34]. Map Reduce is a parallel programming model for creating distributed systems that process massive volumes of data quickly and fault-tolerantly on vast clusters of cheap hardware. Map Reduce employs the two methods Map() and Reduce (), the former of which performs data sorting and filtering and groups the results into groups [35]. The Reduce () method later processes the key-value pair-based output that Map produces. On the other hand, Reduce () aggregates the mapped data to do the summary. Reduce(), in its simplest form, takes the output produced by Map () as input and splits the tuples into smaller groups.

The Hadoop framework has the benefit of making it simple to create and test distributed systems. It is effective and uses the underlying parallelism of the CPU cores to automatically divide the data and work across the computers [43]. In order to provide fault-tolerance and high availability (FTHA), the framework Hadoop does not rely on hardware; rather, the Hadoop library itself has been built to recognize and manage problems at the application layer. Again, machines can be dynamically added to or deleted from the cluster, and Hadoop keeps running unabated.

f) Blockchain Technology Application Model

An open financial ledger or record called a blockchain is where every transaction is verified and approved. A blockchain is intended to function as a decentralized network of numerous computers, often known as nodes [44]. With blockchain technology, each node acts as a network administrator who willingly joins the network, creating a distributed database design. A blockchain is virtually impossible to hack since there is no centralized data in its architecture. Distributed ledger technology is another name for blockchain technology. It enables participants to achieve transactions, transfer assets, and secure the settlement of transactions at a cheap cost [45]. Traceability, transparency, smart contracts, and security are the four main characteristics of blockchain technology. These features ensure that the technology is applicable in a wide range of fields in

addition to its primary use as a cryptocurrency, including government elections, healthcare, logistics, identity management, supply chain, and others. An increasing collection of ordered documents known as blocks are supported by the blockchain architecture [46]. Each block keeps a connection to the preceding block and a timestamp. A blockchain is virtually impossible to exploit since there is no centralized information in its architecture [47]. Block chain applications can have positive effects on an existing business model, including [48], [49], and [50].

1. Because of the variety of advantages it offers, block chain technology has gained widespread use.
2. The block chain is a perfect register for cooperative business ventures because there is no central authority in charge of monitoring operations.
3. The use of digital signatures and verification in block chains helps thwart fraud.
4. Information is not centralized, which prevents data loss.
5. *Simplicity:* more integration between procedures from various entities, simplified processes
6. *Traceability:* Transactions are easily traceable, and the ledger's immutability ensures that they are attributed to the right parties and can be proven to have occurred.
7. *Better performance:* By integrating and automating processes, operations and other activities can perform more quickly.
8. *Stronger relationship:* Greater process integration and simplification imply the development and maintenance of stronger bonds with other stakeholders (participants to the same supply chain).

Block Chain Can be Either Centralised, Decentralised or Distributed as Shown Below on Figure 4.

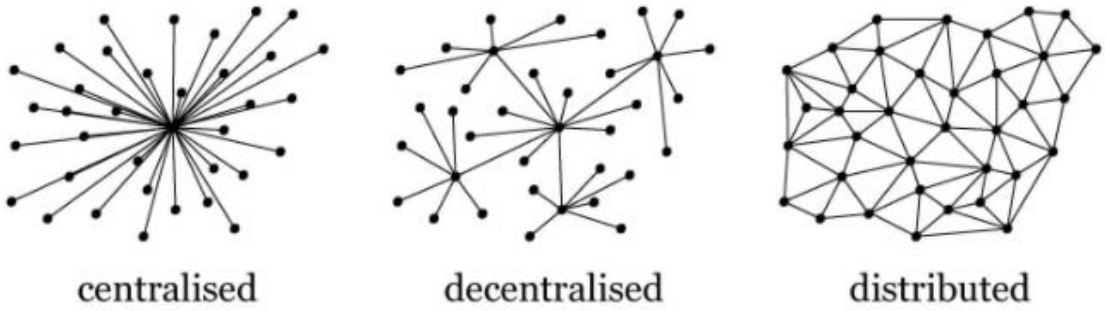


Figure 4: Blockchain Distribution Options

The components of the blockchain architecture are-

1. *Node:* which is a computer in the blockchain architecture, is one of its constituent parts (each node has an independent copy of the entire blockchain ledger)
2. *Transaction:* A data record that is confirmed by blockchain users and acts as a nearly unchangeable affirmation of the legitimacy of a financial transaction or contract.
3. *Block:* A compartment for encrypted data that includes a native hash code to identify the block, a hash code from the block before it in the chain of blocks, and a series of time-stamped transactions.
4. *Chain:* Blocks arranged in a line.
5. *Miners:* Nodes that validate blocks before integrating them into the blockchain structure are known as miners.
6. *Consensus (protocol):* A set of guidelines and agreements for using blockchain technology.

The Blockchan cyber vulnerabilities identified by [3] are as follows.

- *Blockchain code vulnerabilities* from programs that rely heavily on encryption algorithms or may have underlying software coding flaws.
- *Blockchain platform vulnerabilities from* applications caused by software running on platforms with known security issues and general-purpose operating system.
- *End-User vulnerabilities,* such as online wallet hacking, private key theft, etc.
- *Wallet controls* - Although digital wallet companies are now reducing personal risks and offering better key management services, using passwords and other user authentication controls still carries a significant level of risk.

III. Research Methodology

The General Thinking of Researchers about The Research Work is Shown on Figure 5.

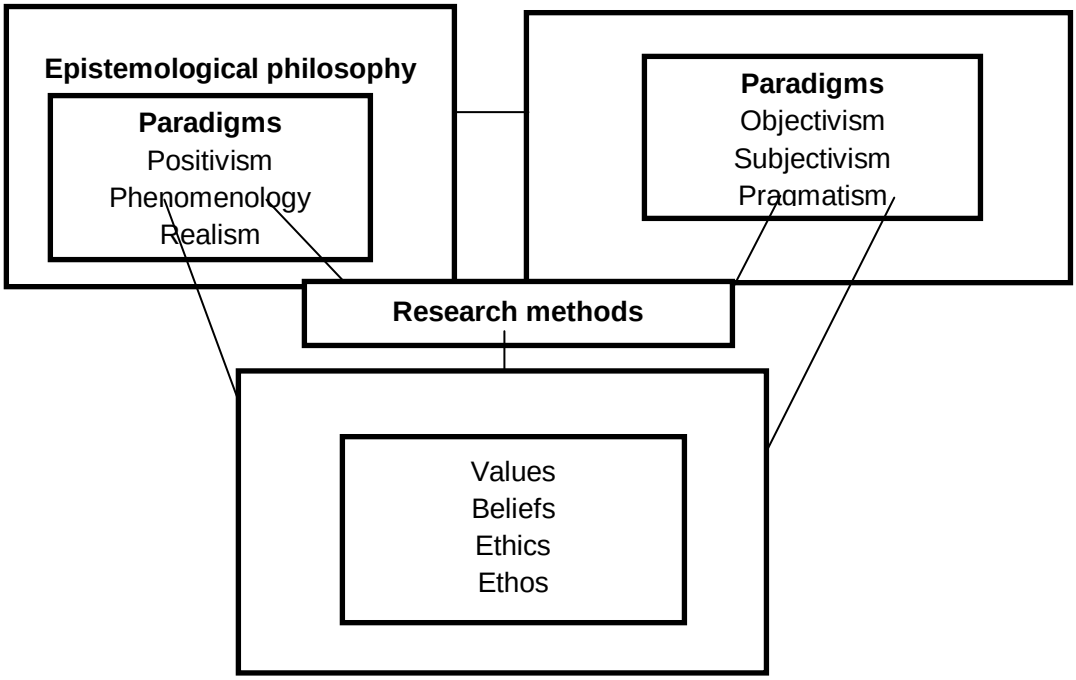


Figure 5: Research Philosophy and Paradigms

a) Epistemological Philosophy

This is how the researcher thinks of legitimate knowledge structures [25]. Researchers have access to his three main epistemological tenets: positivism, realism, and interpretivism [26]. The pragmatism paradigm was used in conducting this research. In order to determine the truth regarding the cybersecurity implications of computer vulnerabilities, a methodical and scientific approach was used during the data collection procedure.

b) Ontological Belief

According to [25], ontology is concerned with the nature of reality and raises issues with the assumptions that researchers make about how the world functions and the commitment to holding specific viewpoints. Positivism is the belief that social entities actually exist, independent of the social players who care about them [25].

c) Axiological Belief

The researcher admitted that the relevance of ethics in the study process was crucial. In order to have an unbiased evaluation of the topic under study, the researcher made an effort to maintain their separation from the respondents during the data gathering time. The respondents were treated with respect and in a manner that was socially just. The researcher also thought the research had a positive net impact on Zimbabwean organizations, as putting its recommendations into practice is expected to result in better cybersecurity measures. For the purpose of ensuring that the industry obtains high-quality suggestions on information technology and cyber-attacks, data were accurately evaluated. Additionally, the researcher made an effort to protect the confidentiality of the respondents' personal data.

d) Research Approaches

A research approach is a strategy that includes phases from general hypotheses to specific methods of data collecting, analysis, and interpretation. As a result, it depends on the type of research problem being addressed. There are fundamentally two types of research approaches:

1. Inductive/qualitative
2. Deductive/quantitative.

e) Qualitative/inductive Research

This strategy places a lot of attention on the techniques used to gather or produce data. However, it gives less weight to the methods of data interpretation that need analysis. Furthermore, using an inductive method, concepts, themes, and models are typically derived from careful study of secondary data. As a result, it is frequently utilized for qualitative data analysis. This starts with the choice of the study area and develops a theory. The inductive strategy comprises combining various secondary data into a succinct

the research's goals and its findings gleaned from the raw data. Additionally, make those connections visible to others and how they will advance the study's goal, as well as building a theory based on the experiences and procedures made apparent by the text data [27]. The study's goal is to comprehend a phenomenon, as shown by the choice of an inductive approach through thematic analysis (a "data driven" approach). Hypothesis testing is not its main concern. This strategy was partially used in this investigation.

f) Quantitative Research/deductive

Making the relationship between what is known and what might be learnt by research requires the use of statistical analysis, which is frequently a component of quantitative research approaches. As a result, knowing the relationships between variables using either descriptive or inferential statistics is necessary for data analysis using quantitative methodologies. Descriptive statistics facilitate population conclusions and parameter estimation [28]. To test hypotheses, statistical analysis is needed for quantitative data. The deductive method is frequently utilized because it allows researchers to move from general to specific reasoning. Additionally, the researcher draws a theoretical framework (hypothesis) from general viewpoints, tests it, and draws a specific conclusion as a result. The deductive method of analysis or reasoning entails the investigation of theories, creation of theoretical frameworks or hypotheses, statistical testing of hypotheses, observation, and validation of a certain conclusion deduced logically from premises [29]. For this investigation, deductive research was the most useful. When huge volumes of data were collected and analyzed using descriptive and inferential statistics, which all needed deductive thinking, quantitative research was equally utilised.

IV. Key Findings, Data Analysis and Interpretation

a) Metaverse, Virtual Reality (VR) and Augmented Reality (AR)

The Metaverse uses technology to transcend our physical reality, changing the human experience. By describing each aspect of the metaverse [7], as seen on Figure 6, we categorize definitions of the metaverse into four categories: environment, interface, interaction, and social value. In terms of the interface, the metaverse is also divided into categories based on the level of immersion, such as 3D and virtual reality (VR) [7]. Although users can experience a great deal of immersion when using VR devices in a 3D environment, the metaverse provides more than just the usage of VR devices in 3D environments. Metaverse definitions focus on interactions for users and non-player characters that go beyond ordinary talks in addition to settings and interfaces (NPCs). There are realistic, unreal, and blended environments in the metaverse. Based on an actual environment, the fused environment displays some irrational characteristics. The designer's intent and interpretation are properly reflected in the realistic metaverse's depiction of geography and natural features [7]. Avatars cannot exist in two places at once in the realistic metaverse, and movement speed is constrained similarly to how it is in the physical universe. Avatars and holograms can be used to work, interact, and socialize via simulated shared experiences in the new metaverse concept, according to Mark Zuckerberg. This integrated immersive ecosystem allows users to cross barriers between the virtual and real worlds with ease [7]. There are physical, immersive, and 3D interface options available. For the metaverse to remain continuous and to encourage user interaction, immersion is a crucial component. Social networking, teamwork, and persona discourse are the three categories used to describe interaction in the metaverse. It is challenging to define and use the social networking experience in the metaverse effectively.

The metaverse provides tasks that are challenging to do in reality as a complement to the real world in a variety of ways. It takes the place of familiar settings (such as offices, SNS, in-person classes, and medical care) and enables things that would be difficult to complete in reality due to issues like cost [7]. As a tool, the metaverse reduces complexity (such as in aircraft engineering) and boosts coherence from a multimodal perspective. The aim is the metaverse itself [7]. The metaverse's operating system needs a lot of users in order to remain sustainable, and seamless services are accessible even on relatively basic mobile devices. Environmental design must take the scalability of the current limited environment into account for long-term service.

It is vital to constantly develop open source platforms that can facilitate collaboration between different developers and a top expert group in order to grow the environment and make use of it [7]. The sustainability of the metaverse depends on an intuitive user interface.

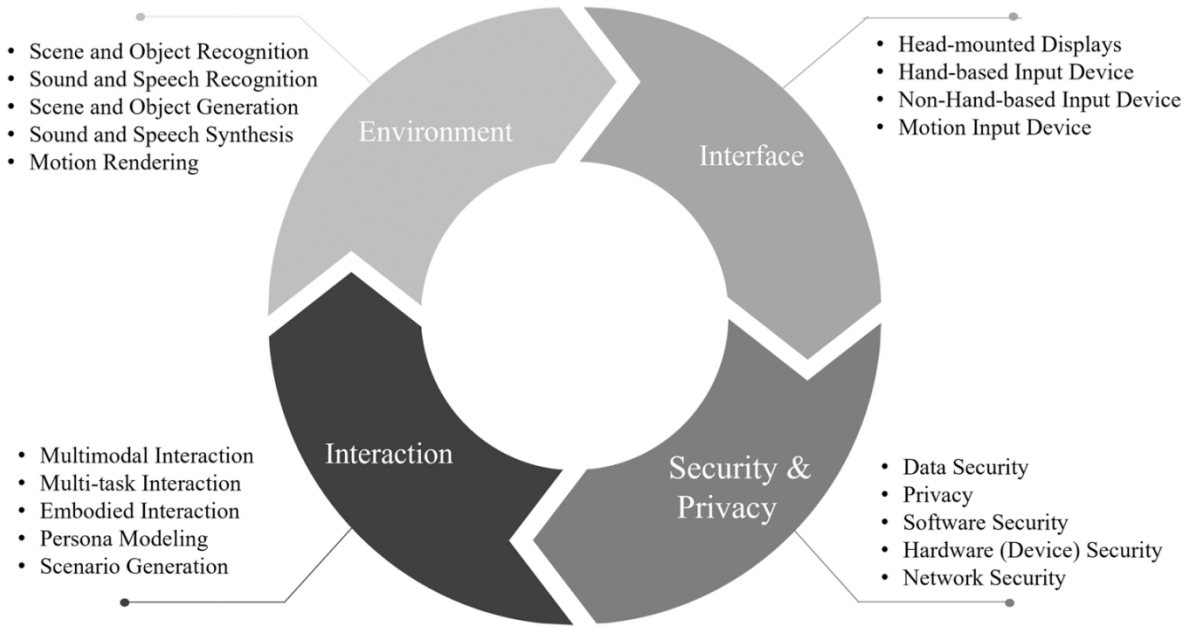


Figure 6: Metaverse with the Environment, Interface, Interaction, Security and Privacy [7]

Figure 7 Below Depicts How The Metaverse Is Conceptualized.

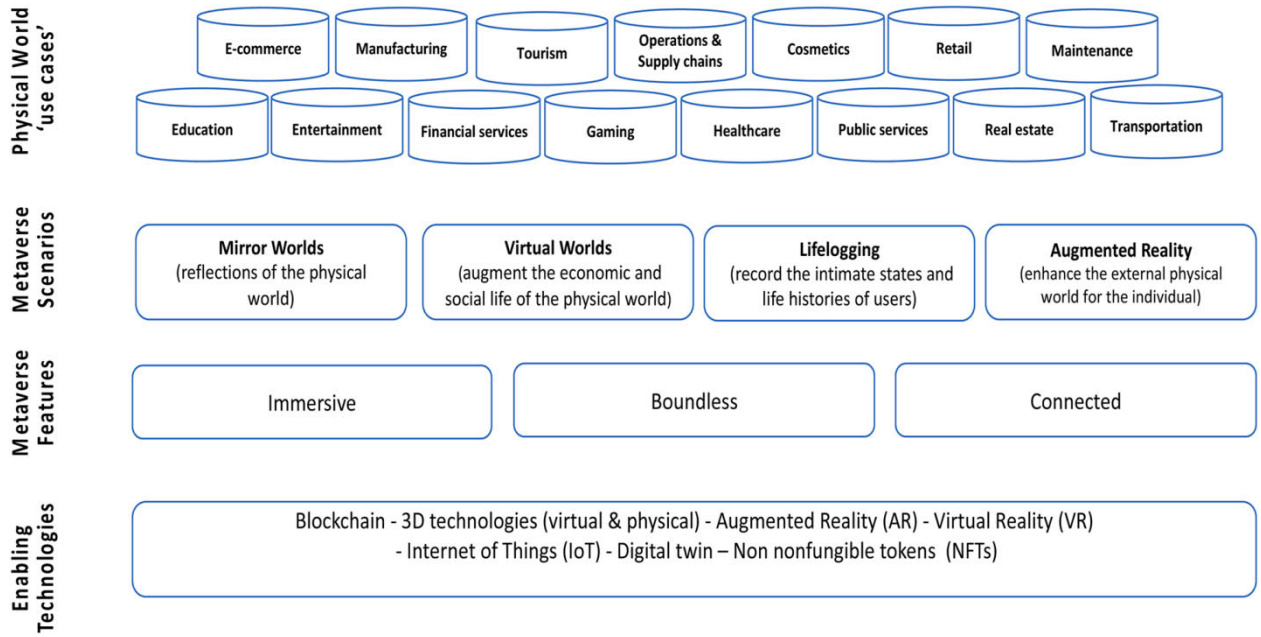


Figure 7: Conceptualisation of the Metaverse (Source [7])

Holograms and eye-attached lenses are useful additions to augmented reality and virtual reality. Additionally, some user interfaces shield young users from unwanted sounds by muffling and expressing them in the actual world. The majority of interfaces in the metaverse consist of visual and supplemental auditory forms. Despite extensive research on metaverse technology, privacy and security in the metaverse have received very little attention. In the metaverse, security and privacy are major concerns, just like on social networking sites. In order to identify a user, malicious users can track and gather real-time biometrics (such as facial expressions and vocal inflections) and metaverse users' behavior (such as their interactions with other users and purchasing actions). The metaverse is constructed in a cyber (or digital) environment, so we must take cybersecurity and privacy concerns into account in order to provide consumers with appropriate services securely and effectively. To ensure that people and systems are protected from a variety of risks and

vulnerabilities, cybersecurity and privacy should offer a variety of measures, approaches, and solutions [7]. A universe without nations, boundaries, or gender is the metaverse. Beyond the current humanistic approach, a fresh viewpoint is required. Since the metaverse incorporates various concepts like marketing, management, and strategy research, it spans a wide range of disciplines. The main components of the metaverse economy are cryptocurrencies and non-fungible tokens (NFTs), such as bitcoin and ethereum. NFTs enable the verification of these assets and even identities while representing ownership of virtual in-game items, virtual avatars, real estate properties, and other assets [7]. Similar to how money functions in the normal economy, cryptocurrencies function similarly in the metaverse economy.

b) Cybersecurity on the Education Value Chain and Blockchain

A cybercrime threat or vulnerability must be positioned in a multidisciplinary perspective. However, the nation's educational system has been stove-piping such a cybersecurity strategy for decades. While understanding the technical aspects of the cyber environment, networked systems, operating systems, and the security threats that surround them is given more importance, little to no attention is paid to the human actors and their decision-making processes, which are crucial to the success of a cyber-attack. In actuality, cyber-attacks have increased in frequency and cost to enterprises, organizations, economies, and other infrastructure-related institutions. The world has become more network-centered in the twenty-first century, and the rapid development of internet technology has given rise to a contemporary cybersecurity culture and a complex threat environment in the higher education sector. The future of the fourth industrial revolution is a system called Blockchain.

The blockchain is a public ledger that stores collections of transactions, referred to as blocks, that are chronologically and cryptographically connected. Excellent security, immutability, and program expertise dependent on the Blockchain architecture and the nature of the consensus protocol used by the Blockchain are the primary characteristics linked with it. Blockchain technology has produced a payment system that accepts both cash and non-monetary payments. With features of distribution, centralized ledger alteration connects parties who are jointly responsible for various parts of a single authoritative ledger. The complete abolition of a centralized regulating authority was associated with the dispersal of ledgers and the development of a system in which certain individuals kept copies of the entire ledger system. A major novel that has been circulated requires agreement from those who have copies in order to make adjustments or additions, and each addition or change is duly recorded in each copy of the ledger as well as with authority.

c) Institutional Capacity Building Requirements for a Metaverse-based Academic Virtual Environment

A platform based on content businesses like gaming is now being created using metaverse technology [30]. Accordingly, [30] lists and illustrates the four definitions of the Metaverse in Figure 8 and Table 3.

Table 3: Definitions of the four types of Metaverse

Classification	Definition
Augmented Reality	It is a technology that enhances work efficiency by augmenting virtual information in real space in real time and allowing users to interact with the augmented virtual information.
Lifelogging	It is a technology that captures, stores, and depicts everyday experiences and information about objects and people.
Virtual Reality	It refers to a specific environment or situation or the technology itself that is like reality but is not real, created by artificial technology.
Mirror Worlds	It is a digital representation of the real world that makes an effort to geographically accurately map real-world structures. It provides a software utility model of actual environments and how they function.

As seen in Figure 6, the horizontal axis is a measure of user immersion intensification and the extent to which the external environment is reflected (intimate). On the other hand, the vertical axis displays a criterion for differentiating between simulation in the virtual world and the augmentation of reality, which is a setting in which information is implemented. This standard divides the vertical axis into augmentation and simulation and the horizontal axis into intimate and outward elements. Four subcategories of the metaverse can be identified: augmented reality, life logging, mirror worlds, and virtual worlds.

The lines separating the actual world and the Metaverse world will eventually merge to the point that it is possible to forget that you are in cyberspace. Based on the convergence of technologies like virtual reality (VR) and augmented reality (AR), which enable multimodal interactions with virtual surroundings, digital objects, and people (AR), the metaverse is a post-reality world, a continuous and enduring multiuser environment

that combines physical reality with digital virtuality [31]. The Metaverse is an ever-available web of socially networked immersive experiences for multiple users that allows for real-time, embodied user conversation and dynamic interactions with digital objects. The Metaverse concept is summarized on Figure 7. The Metaverse is an ever-available web of socially networked immersive experiences for multiple users that allows for real-time, embodied user conversation and dynamic interactions with digital objects. Institutional capacity building requirements for a Metaverse-based academic virtual environment is centered on investments in Mixed Reality (MR) and the Metaverse concept shown on Figure 9. Mixed reality (MR) can combine social media connectivity with immersive VR and AR technologies' unique features [31]. Online education will push the boundaries of informal education and social interactions in the Metaverse. Physical presence in the classroom won't be valued as a distinctive educational experience any longer. Telepresence, avatar body language, and facial expression conformance will make virtual meetings equally as productive as in-person ones. Additionally, MR in the Metaverse can support active mixed education to develop deeper, more enduring knowledge [31]. Additionally, it can contribute to the democratization of education by enabling equitable participation without regard to a person's location.

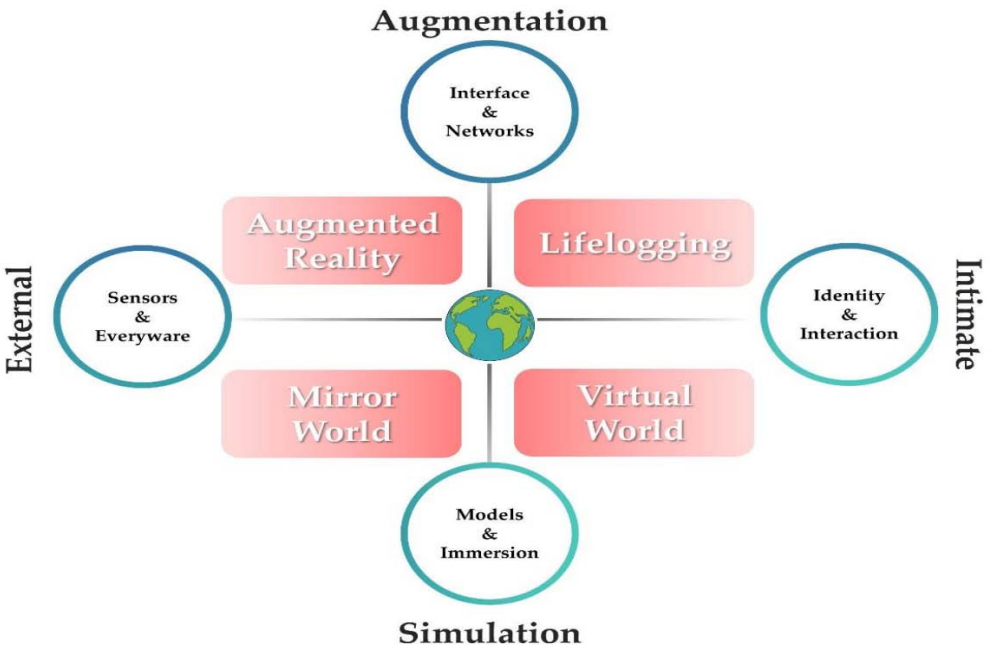


Figure 8: The Four types of Metaverses (Source: [30], page 3)

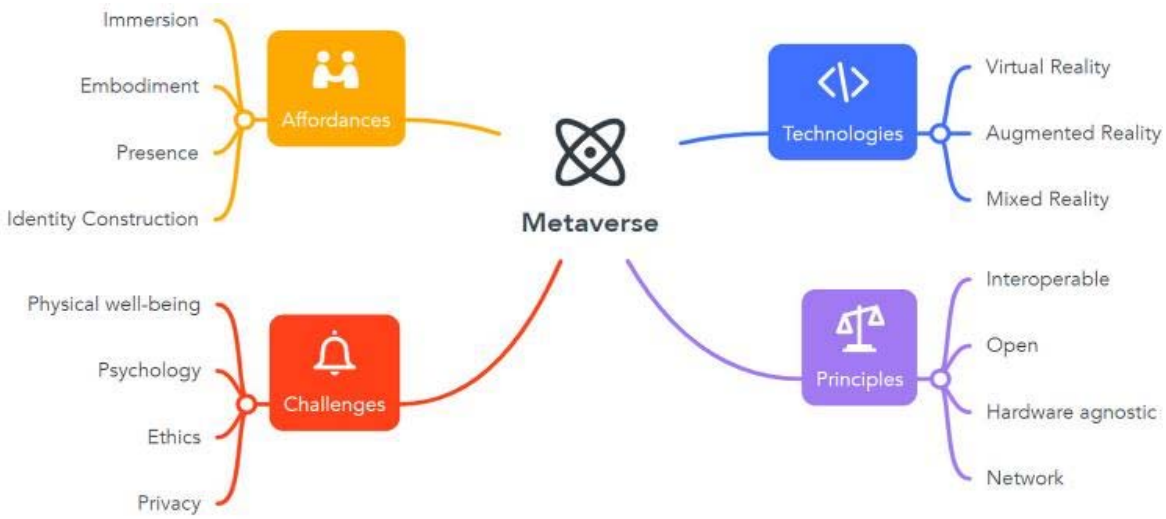


Figure 9: The Metaverse Concept (Source: [31], page 3)

Online learning may be done more interactively thanks to the virtual world idea espoused by Metaverse. The learning environment at school or college is not compromised by the support offered by Metaverse for online learning. Online learning can be done more interactively with the virtual world idea suggested by Metaverse [31]. The world of education will unavoidably need to get ready to embrace this technology as a result of the Metaverse being developed by powerful technology businesses. The atmosphere will undoubtedly be more comfortable and enjoyable in the virtual/Metaverse world where school buildings with all the amenities can be built, but the relationship between teachers and students in the real world may suffer because they only interact with each other in the Metaverse in the form of their respective avatars, whereas they hardly or never interact in the real world [31]. In learning and educational situations, Metaverse offers students more immersive experiences and a more interactive learning experience.

d) Handling Copyright and Intellectual Property (IP) Violations of Learning Materials

Patents, copyrights, trademarks, and trade secrets are all considered to be part of intellectual property. With a patent, the owner has the legal authority to prevent others from "practicing" (creating, utilizing, and commercializing) an invention. New, practical, and nonobvious inventions that fall under the categories of methods, machines, manufacture, and composition of matter are eligible for patent protection. Thus, the outcomes of academic research can take many different forms, including technologies, chemicals, biological materials, instruments and methods for conducting study, production processes, and software. Trademarks, service marks, certification markings (which, for example, indicate testing by an independent laboratory), and collective marks are the many types of marks used to distinguish goods and services in the marketplace (identifying membership in an organization, such as real estate agents). Original works of authorship preserved in any physical form are protected under copyright. When a work satisfies these legal standards, copyright becomes its property; there is no longer a need for an application or registration procedure. Literature and other printed materials, architectural or engineering drawings, circuit diagrams, lectures and other instructional materials, musical or dramatic compositions, motion pictures, sound recordings, choreography, computer software and databases, as well as paintings and sculptures, are examples of subject matter that is eligible for copyright protection. According to [33], intellectual property in universities includes developed theories, laws, mathematical formulas, and symbols; Published print and electronic books, journals, and articles; discoveries and innovations resulting from scientific research, statistical information and reports, and art prints and drawings. Patents, trademarks, breeder's rights, copyrights, and industrial design rights are all examples of intellectual property rights.

One component of access to knowledge is access to educational resources. There is little question that access to educational resources is a key component of the success of any educational system and that education is a cornerstone of social and economic growth. Any set of policy solutions that deal with the issue of access to learning materials in southern Africa will have to take the informal economy into account in order to be comprehensive, despite the fact that it may be challenging for policy-making structures to overcome the naturalization of simplistic polarities like "piracy" on the one hand and the "formal economy" on the other. It is presumable that a student's ability to persevere through the learning process depends on the caliber and accessibility of the learning materials. People who work on academic, instructional, or artistic projects create a wide range of copyright-eligible items that they would want to guard from unlawful use. Books, articles, monographs, bibliographies, lecture notes and handouts, musical compositions and recordings, visual arts like paintings and pictures, films, and audiovisual works, as well as computer programs, are just a few examples of these. The copyright of a work that is created by a member of the faculty, staff, or a student is theirs to keep. Even while the College might offer some assistance in the form of resources like buildings, supplies, gear, or staff, it is proper for each individual to own the copyright to such works. The College may use, reproduce, and modify any copyrighted work that was initially created with the express intent of making it available to people other than, or in addition to, the original creator for use in teaching, administration, or other College activities. It is understood, however, that the individual will grant a perpetual, worldwide, royalty-free license allowing the College to do so. Even if the person who designed the curriculum or programs has left the College, the College will have access to these materials for free. It is the individual's responsibility to make sure that any additional authors of works with multiple authors are made aware of this policy and give their consent for the license to be granted to the College in cases where one or more of the authors are not affiliated with the College and are not covered by this policy.

It is possible to start learning and producing information as soon as possible. Students can acquire new knowledge and create it as soon as possible without any additional restrictions that might pose a barrier, such as classroom partitions and time constraints. In order to experience the true freedom of learning, which must be enjoyable for them, students will have a class that is as diverse as this world and more time to spend researching the knowledge they wish to acquire. Ultimately, there will be more and expanding

learning resources. The use of technology will inevitably lead to the development of new knowledge and technologies. The more knowledge sources we have access to, including sources of information that may be used to advance our abilities, will result in the creation of learning resources that are more diverse. Schools are not just structures anymore. There will be many virtual schools that do not require significant amounts of land and buildings to construct an educational institution and the existence of the Metaverse will bring about changes to the physical form of educational institutions in the globe. The majority of educational institutions are out of reach due to distance, travel time, and prohibitive expenses.

Online learning has replaced the traditional face-to-face classroom setting for instruction. Because of the limited resources available to schools that demand teachers and students to teach both in social media groups and in class, several schools provide daily instruction through online learning programs. Poor learning performance is a result of this, especially when there is a literacy gap between teachers and students. Because no technology can completely replace the function of the teacher in student-centered learning, the Metaverse will have an impact on the educational landscape. Teachers should interact with students in person rather than online. Other than teaching and learning activities, the Metaverse can be used for administrative tasks like managing teachers, finances, supervision, promotion files, and so forth. Whether these tasks can ultimately be implemented in our nation is still up in the air, and it is obvious that for the time being, all of them are still confined to wishful thinking. Negative effects, like the loss of social warmth because they do not directly engage with people, will be felt if all educational activities are conducted digitally. Because education is merely a formality, educators do not have a direct relationship with their students.

Since the 1980s, tensions around ownership of the results of faculty research have been quietly rising, but they have gotten worse over the past three years. Ownership of patentable discoveries has always been a contentious issue, but recently, a number of colleges have unequivocally declared that they are the rightful proprietors of academic research results. Additionally, universities are becoming more interested in designating faculty intellectual property to be subject to copyright. This is most obviously seen in the requests that faculty members transfer ownership of online courses and other teaching resources to their schools. Because it directly affects the university's essential principles, such as academic freedom, scholarship, research, shared governance, and the dissemination of knowledge, the management of innovations, patents, and other types of intellectual property in a university context calls for specific direction. These guiding principles set university activity apart from that of government and business, and they serve as a foundation for the case for public funding of research and the university's role as an independent contributor to both policy and business. The administration and negotiation of faculty-generated intellectual property can be difficult and have serious repercussions for those directly involved.

The disadvantages of the Metaverse are-

1. Metaverse requires a high level of technology consumption due to the sophisticated and high-quality graphics it produces.
2. It is quite expensive to gain access to technologies that enable Metaverse.
3. Due to the Metaverse's unbounded nature, there is the potential for social and cultural development.
4. Relevance and metaverse are still struggling with the question of whether communication and action in the virtual world are necessary or not.

e) Cybersecurity-Compliant Hadoop Architecture Framework for Metaverse Online Education Value Chain

[3] explained how the framework of bitcoin and blockchain technology addresses cyber concerns and adds value to the financial services sector and education value chain in the following way:

- *Minimal Transaction Fees:* Peer-to-peer crypto-currency transfers necessitate no centralized intermediaries, therefore transaction fees are negligible, and decentralized systems do not impose fees for currency conversion.
- *Accessibility:* By their very nature, cryptocurrencies are not subject to a country's exchange rates, interest rates, transaction fees, or other levies.
- *Instant Payment:* Peer-to-peer transactions make Instant Payments possible.
- *Improved security provided by Blockchain technology*: Blockchain technology offers greater security than centralized financial systems, which makes it very difficult for hackers to compromise.
- *Transparency in the transactions.*
- *Decentralization framework* supporting stakeholder governance by giving people, rather than centralized authorities, the power to make decisions.
- *Immutability:* The blockchain's general ledger's immutability makes it impossible for internal players to change data for their own gain.

The Big Data Analytics Framework that is suggested for implementation in a Hadoop-Metaverse system is represented on Figure 10 below from the conceptual framework perspective of this research article.

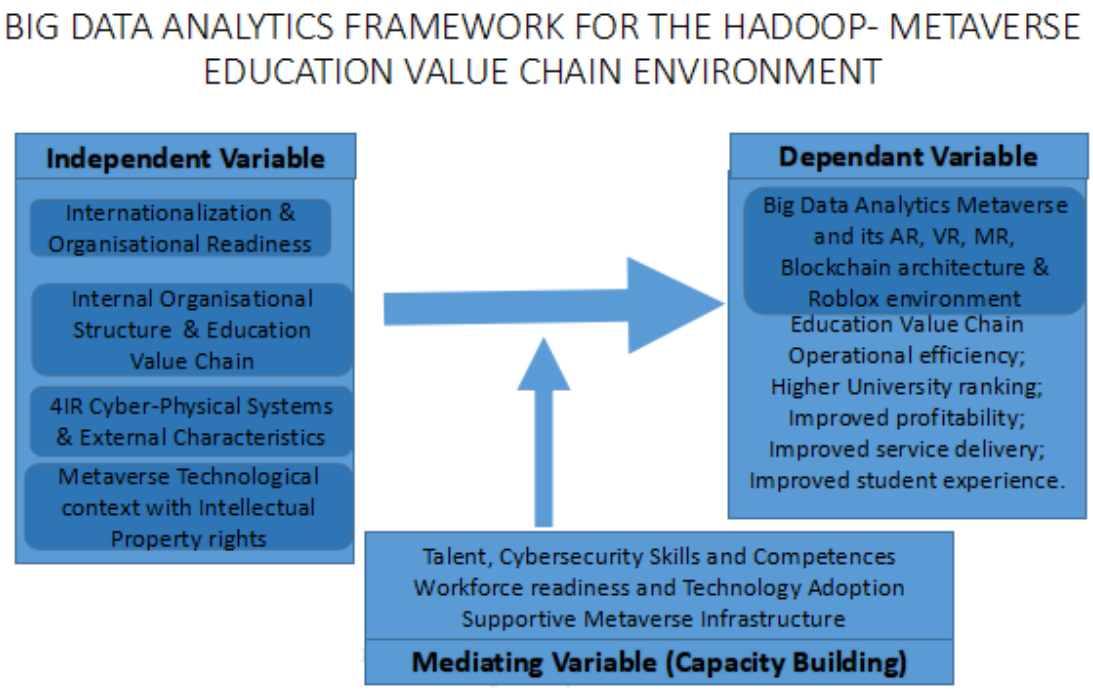


Figure 10: Big Data Analytics Framework for the Hadoop-Metaverse Environment

The sixth generation (6G) of mobile communication, which follows and improves on the fourth and fifth generations (4G and 5G), is a cutting-edge technology that combines sensing, storage, communication, control, and computational capability. Speed and latency will be the most noticeabe differences between 6G and 5G. A major advantage of 6G is that it facilitates instant communication in phones, computers, wearable devices, robotics, and more. Every time mobile communication technology is updated and iterated, its different performance indicators outperform the last generation by a factor of 10 to 100. Edge intelligence powered by 6G enables the Internet of Everything and allows people, devices, and the cloud to be connected at any time and from any location [51]. Smart service applications for next-generation wireless networks are transforming our way of life and enhancing it. The effective integration and collaboration of AI technology and 6G mobile communication technology resulted in the creation of the 6G-enabled edge AI paradigm [51]. Edge AI benefits from decreased latency, a more reliable network connection, and a more secure network design thanks to 6G mobile communication technologies. The benefits of reduced latency, computing offload, and high performance come with 6G edge intelligence. The immersive and real-time physical-virtual world interaction offered by the Metaverse technical layer is a feature of the Metaverse architecture shown on Figure 11. The Metaverse is low bandwidth, low latency, provides ubiquitous access, and is reliable for consumers thanks to the enabling technologies.

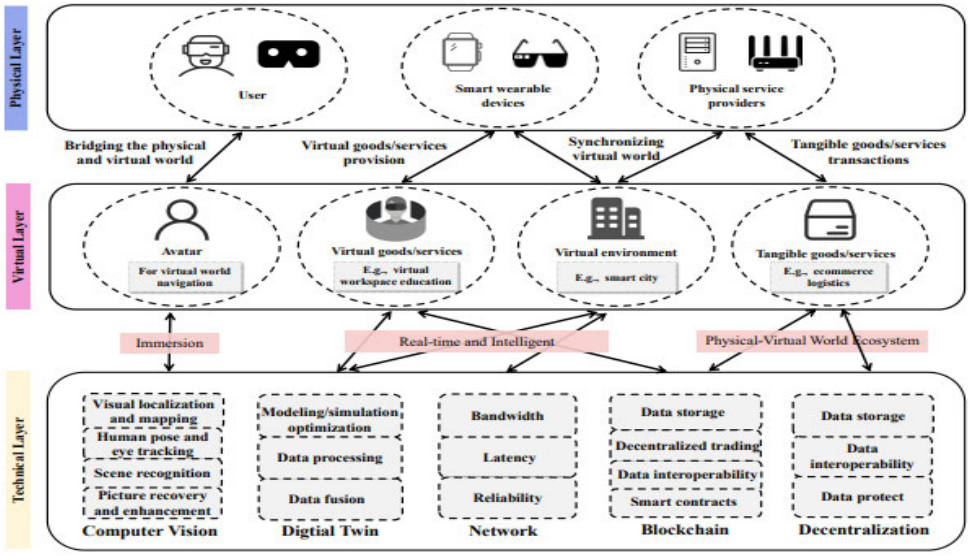


Figure 11: Metaverse Architecture with Immersive and Real-Time Physical-Virtual World (Source: [51])

The Cybersecurity model for the Cybersecurity model for a Roblox-based Metaverse architecture framework is illustrated on Figure 12.

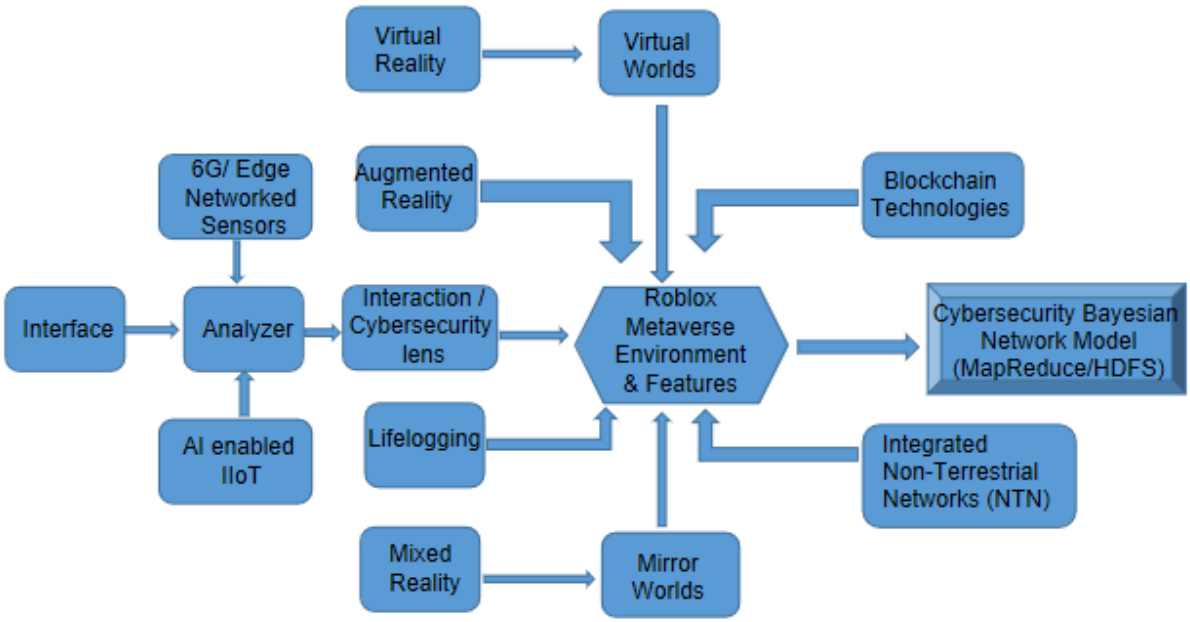


Figure 12: Cybersecurity Model for a Roblox-Based Metaverse Architecture Framework

f) Summary Architecture Framework

The effects of internationalization, international integration, or globalization as well as the COVID-19 health emergency have caused a shift from the traditional/simulated education paradigm to zero and one as well as introduced and innovated significant changes to the teaching and learning process. Virtual reality (VR), immersive virtual reality (IVR), and augmented reality (AR) are the only three harmful tendencies in the field of education at the moment as a result of the tremendous technological transformation that humanity is undergoing [32]. In order for kids to study and engage in the new technological field in which they are born, we must first construct transformative educational settings in addition to implementing innovative emerging technologies in education. Virtual reality (VR) is seen as a philosophical, scientific, and technological turning point in the digital age. IVR can enhance the transformation of the educational process [32]. Immersive virtual reality presents a significant

short-term challenge to educational institutions as a learning tool. IVR is becoming more affordable and accessible. Roblox and other immersive learning tools make it possible to identify devices, thus it is crucial in education to take the teaching and learning process to a new level by honing and developing abilities in online and offline (synchronous and asynchronous) training. IVR facilitates the creation of simulations in which the teaching is done, with a focus on teaching and learning in the context of educational technology.

The Metaverse is a three-dimensional, real-time immersive simulation medium, and its ecology is well suited to supporting audiovisual notifications, creating an amazing setup in training or teaching environments. Nevertheless, it is challenging for different network users to participate in or even use three-dimensional world technology in the teaching/learning process due to a lack of knowledge and competence. Most importantly, making full use of the metaverse's capabilities and applying these capabilities to the digital environment "requires training in specific skills specific to the virtual world. Digital skills are what this entails. The knowledge, skills, abilities, attitudes, and tactics needed to use internet technology and the Internet are collectively referred to as "digital competencies."Every field of work or education can benefit from the immersive, multisensory 3D environment that Metaverse offers teachers.

The Cybersecurity model for a Roblox-based Metaverse architecture framework shown on Figure 12 is a Bayesian Network. Bayesian Networks (BNs) are directed acyclic graphs that have an associated probability distribution function and these graphical probabilistic models are used for multivariate analysis [3]. These BNs allow us to reason from evidence to hypotheses with regards to cybsecurity issues.

$$P(x) = {}^{n}\prod_{i=1} p(x_i|\Psi_i)$$

V. Conclusion

The Metaverse is a virtual iteration of the Internet as a single, universal, immersive virtual world made possible by the use of virtual reality and augmented reality headsets in futuristic and science fiction. Roblox is an open-source platform that can be used for online education to enable interactive 3D virtual environments in physical and online classrooms, with some basic cybersecurity mechanisms. In essence, Metaverse is a combination of virtual reality, augmented reality, mixed reality, blockchain, web3, cryptocurrencies, social media, etc. Metaverse provides users with a multilingual experience, which is a key requirement for successful internationalization that breaks down language barriers and enables easier and more affordable exchange programs. The metaverse has many advantages in science that outweigh disadvantages such as physical limitations when working with VR and AR. Although there are many different types of E Learning environments, metaverse based systems can also be used to provide safe and efficient environments for education and business by utilizing virtual reality technologies and continuously researching and attempting to expand learning experiences. The Metaverse roadmap, according to???, is divided into four sections: augmented reality, life logging, mirror worlds, and virtual worlds. Our ability to trust the technology that underpins virtual experiences is severely compromised as a result. Cyber security is a technique for defending against online attacks on programs, networks, and systems. The key focus of cyber security is the defense of programs, networks, and systems against harmful digital attacks. The Cyber security model for a Roblox-based Metaverse architecture framework developed is a Bayesian Network, which is a directed acyclic graph that has an associated probability distribution function which can be used for multivariate analysis. Systematic literature review of Metaverse, Virtual Reality and Augmented Reality Augmented reality was conducted. The systematic review work highlighted the Metaverse elements, digital currencies, AI applications in the virtual world, and blockchain-empowered technologies to discuss how blockchain and AI fuse with the Metaverse. Between augmented reality and virtual reality, mixed reality provides an improved version of augmented reality. The use of the metaverse in Software Engineering Education enables experiences that effectively teach software processes, allowing the student to take on the lead roles in software projects. Students do this using techniques of specific development process models, navigating in different environments, communicating with other avatars, and interacting with and viewing Unified Modeling Language diagrams in the same way that they are seen in real-world software projects.

References Références Referencias

1. De Wit, H., Hunter F., Howard L., Egron-Polak E. (Eds.) (2015) *"Internationalisation of Higher Education"*, European Parliament, Brussels: EU. Taken from http://www.europarl.europa.eu/RegData.etudes/STUD/2015/540370/IPOL_STU (2015) 540370_EN.pdf on September 25, 2016; Print ISBN 978-92-823-7847-2, DOI: 10.2861/6854, QA-02-15-573-EN-C PDF ISBN 978-92-823-7846-5, DOI: 10.2861/444393 QA-02-15-573-EN-N; http://www.europarl.europa.eu /studies.
2. Dahan, N. A.; Al-Razgan, M.; Al-Laith, A.; Alsoufifi, M.A.; Al-Asaly, M.S.; Alfakih, T., (2022, *"Metaverse Framework: A Case Study on E-Learning Environment (ELEM)"*, *Electronics* 2022, *11*, 1616. https:// doi.org/10.3390/electronics11101616.
3. Kabanda, G., (2021), "*Cybersecurity Risk Management Plan for a Blockchain Technology Application*

Model", ACM Transactions on Engineering and Computer Science, April, 2021, Volume 2, Issue 1, https://gnoscience.com/uploads/journals/articles/634258716714.pdf, Gnoscience Group, (https://gnoscience.com/journals/3), Hindenburgstr 24, Erlangen, 91054, Germany.

4. Fernandes, F., and Werner, C., (2022)., *"A Systematic Literature Review of the Metaverse for Software Engineering Education: Overview, Challenges and Opportunities"*, PRESENCE Journal, 13th September, 2022, Universidade Federal do Rio de Janeiro, Brazil.
5. Yung, R., and Khoo-Lattimore, C., (2019), *"New realities: a systematic literature review on virtual reality and augmented reality in tourism research"*, Current Issues in Tourism, 22:17, 2056-2081, https://doi.org/10.1080/13683500.2017.1417359; available online: https://www. tandfonline.com/doi/10.1080/13683500.2017.1417359; Griffith Research Online: https://research-repository.griffith.edu.au; ISSN: 1368-3500 (Print) 1747-7603 (Online) Journal homepage: https://www.tandfonline.com/loi/rcit20.
6. Kim, D., and Im, T., (2022), *"A Systematic Review of Virtual Reality-Based Education Research Using Latent Dirichlet Allocation: Focus on Topic Modeling Technique"*, August 2022, Hindawi Mobile Information Systems, Volume 2022, Article ID 1201852, 17 pages; https://doi.org/10.1155/2022/1201852, Kongju National University, Kongju, Republic of Korea.
7. Dwivedi, Y. K., Hughes, L., Baabdullah, A. M, et al, (2022), *"Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy",* International Journal of Information Management, Published by Elsevier Ltd, www.elsevier.com/locate/ijinfomgt;https://doi.org/10.1016/j.ijinfomgt.2022.102542.
8. Zahiroh, M.Y., (2020), *"Cybersecurity Awareness and Digital Skills on Readiness For Change in Digital Banking"*, Li Falah-Jurnal Studi Ekonomi Dan Bisnis Islam (Journal of Islamic Economics and Business Studies), Volume 4 (No.2, 2019), pages 53-73, P-ISSN: 2541-6545, E-ISSN: 2549-6085.
9. Mpofu, N., and Chikati, R. (2013). Digital Divide and The Education Value Chain. *International Journal Of Scientific & Technology Research Volume 2, Issue 10, October 2013*
10. Ernst and Young, (2015). *Cybersecurity and the Internet of Things*
11. Global Information Assurance Certification, (2022), https://www.giac.org/workforce-development/government/niceframework/
12. National Institute of Standards and Technology, (2022). https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center.
13. National Initiative for Cybersecurity Careers and Studies, 2022. https://niccs.cisa.gov/workforce-development/nice-framework.
14. Roblox (2022), https://corp.roblox.com/
15. Bailenson, J. N., (2018), *Experience on Demand (2018): What Virtual Reality Is, How It Works, and What It Can Do,* NewYork, NY: W. W. Norton; 2018.
16. Meier, C., Saorín, J., de León, A. B., and Cobos, A. G. (2020). Using the Roblox video game engine for creating virtual tours and learning about the sculptural heritage. International Journal of Emerging Technologies in Learning (iJET), 15 (20), 268–280. https://doi.org/10.3991/ijet.v15i20.16535.
17. Pericles, R., (2022), "*Metaverse or Simulacra? Roblox, Minecraft, Meta and the turn to virtual reality for education, socialisation and work"*, Interactive Learning Environments, 30:1, 1-3, DOI: 10.1080/ 10494820.2022.2022899.
18. Sadiya, S., (2022), "Humans Emerging beyond Universe with Metaverse, is it possible? How?", International Journal for Research in Applied Science & Engineering Technology (IJRASET), DOI: https://doi.org/10.22214/ijraset.2022.40044
19. Maloney, D., and Freeman, G., (2020). *Falling asleep together: What makes activities in social virtual reality meaningful to users.* In In proceedings of the annual symposium on computer-human interaction in play (pp. 510–521). https://dl.acm.org/doi/10.1145/3410404.3414266.
20. Hutson, J., (2022), *Social Virtual Reality: Neurodivergence and Inclusivity in the Metaverse,* Societies 2022, 12, 102. https://doi.org/10.3390/soc12040102.
21. Cummings, J. J., and Bailenson, J. N., (2016). How immersive is enough? A meta-analysis of the effect of immersive technology on user presence. Media Psychology, 19 (2), 272–309. https://doi.org/10.1080/15213269.2015.1015740.
22. Coban, M., Bolat, Y. I., and Goksu, I., (2022). *The potential of immersive virtual reality to enhance learning: A meta-analysis,* Educ. Res. Rev., 2022, 36, 100452.
23. Gaggioli, A., (2018), *Virtually social,* Cyberpsychology, Behavior, and Social Networking, 21 (5), 338–339. https://doi.org/10.1089/cyber.2018.29112.csi.
24. Hussein, M.; Nätterdal, C (2015). The Benefits of Virtual Reality in Education. A Comparison Study. Bachelor's Thesis, University of Gothenburg, Göteborg, Sweden, 2015.
25. Saunders, M., Lewis, P., & Thornhill, A. (2009). Research methods for business students. Pearson education.
26. Tayler, W. B., & Bloomfield, R. J. (2011). Norms, conformity, and controls. Journal of Accounting Research, 49 (3), 753-790.
27. Jebreen, I. (2012). Using inductive approach as research strategy in requirements engineering

International Journal of Computer and Information Technology, (2), 162-173.
28. Nanda, S., Rivas, A., Trochim, W., & Deshler, J. (2000). Emphasis on validation in research: A meta-analysis. Scientometrics, 48 (1), 45-64.
29. Soiferman, L. K. (2010). Compare and Contrast Inductive and Deductive Research Approaches. Online Submission. https://eric.ed.gov/? id=ED542066.
30. Yu, J.-E., (2022), *"Exploration of Educational Possibilities by Four Metaverse Types in Physical Education"*, *Technologies* 2022, *10*, 104, https://doi.org / 10.3390/ technologies10050104 .
31. Fitrial, T. N., Simbolon, N. E., and Afdaleni, (2022), *"Possibility of Metaverse in Education: Opportunity and Threat",* SOSMANIORA (Jurnal Ilmu Sosial dan Humaniora), Vol. 1 No. 3 (September 2022), pages 366 – 376; https://journal.literasisains.id/index.php/sosmaniora; DOI: 10.55123/sosmaniora. v1i3.821; e-ISSN 2829-2340| p-ISSN 2829-2359.
32. Barráez-Herrera, D.P., (2022), *"Metaverse in a virtual education context"*, Metaverse 2022; 3(1): 9 pages; Asia Pacific Academy of Science Pte. Ltd., Creative Commons Attribution License (https://creativecommons.org/licenses/by/4.0/).
33. Philips, C.A., and Chinda, C.I, (2017),*"Lecturers' Perception of Intellectual Property Rights in Universities in Rivers State"*, International Journal of Human Resource Studies, ISSN 2162-3058, 2017, Vol. 7, No. 1,Macrothink Institute.
34. Dean, J., & Ghemawat, S. (2008). MapReduce: simplified data processing on large clusters. *Communications of the ACM*, *51* (1), 107-113.
35. Chowdhury, B., Rabl, T., Saadatpanah, P., Du, J., & Jacobsen, H. A. (2013). A bigbench implementation in the hadoop ecosystem. In Advancing big data benchmarks (pp. 3-18). Springer, Cham.
36. George, M. M., & Rasmi, P. S. (2022, January). Performance Comparison of Apache Hadoop and Apache Spark for COVID-19 data sets. In *2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 1659-1665). IEEE.
37. Akhtar, N., Parwej, F., & Perwej, Y. (2017). A perusal of big data classification and hadoop technology. *International Transaction of Electrical and Computer Engineers System (ITECES), USA*, *4* (1), 26-38.
38. Bobade, V. B. (2016). Survey paper on big data and Hadoop. *Int. Res. J. Eng. Technol*, *3* (1), 861-863.
39. Agrawal, S. (2011). The Next Generation of Apache Hadoop MapReduce. Apache Hadoop Summit India.
40. Borthakur, D. (2010). HDFS architecture. *Document on Hadoop Wiki. URL http://hadoop. apache.org/common/docs/r0*, *20*.
41. Vyas, A., & Ram, S. (2017). Comparative study of MapReduce frameworks in big data analytics. *Int J Mod Comput Sci*, *5*, 5-13.
42. Shvachko, K., Kuang, H., Radia, S., & Chansler, R. (2010, May). The hadoop distributed file system. In *2010 IEEE 26th symposium on mass storage systems and technologies (MSST)* (pp. 1-10). IEEE.
43. Rabl, T., Frank, M., Danisch, M., Gowda, B., & Jacobsen, H. A. (2014, August). Towards a complete BigBench implementation. In Workshop on Big Data Benchmarks (pp. 3-11). Springer, Cham.
44. Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, *50*, 102407.
45. Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials*, *18* (3), 2084-2123.
46. Hussein, A. F., ArunKumar, N., Ramirez-Gonzalez, G., Abdulhay, E., Tavares, J. M. R., & de Albuquerque, V. H. C. (2018). A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform. Cognitive Systems Research, 52, 1-11.
47. Maksymyuk, T., Gazda, J., Han, L., & Jo, M. (2019, July). Blockchain-based intelligent network management for 5G and beyond. In *2019 3rd International Conference on Advanced Information and Communications Technologies (AICT)* (pp. 36-39). IEEE.
48. Mohamed, N., & Al-Jaroodi, J. (2019, January). Applying blockchain in industry 4.0 applications. In *2019 IEEE 9th annual computing and communication workshop and conference (CCWC)* (pp. 0852-0858). IEEE.
49. Tiscini, R., Testarmata, S., Ciaburri, M., & Ferrari, E. (2020). The blockchain as a sustainable business model innovation. *Management Decision*.
50. Kramer, M. P., Bitsch, L., & Hanf, J. (2021). Blockchain and its impacts on agri-food supply chain network management. *Sustainability*, *13* (4), 2168.
51. Chang, L., Zhang, Z., Li, P., Xi, S., Guo, W., Shen, Y., ... & Wu, Y. (2022). 6 G-enabled Edge AI for Metaverse: Challenges, Methods, and Future Research Directions. *arXiv preprint arXiv: 220406192*.

This page is intentionally left blank

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 23 Issue 1 Version 1.0 Year 2022
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Digital Forensics: Techniques and Tools for Cybercrime Investigations

By Madhav Vedpathak & Aarti Kashid

Abstract- Digital forensics is a crucial aspect of modern-day investigations, particularly those involving cyber crimes. With the increasing prevalence of digital devices, the amount of electronic evidence available for investigation has also grown significantly. Therefore, it is essential to have the necessary techniques and tools to extract and analyse digital evidence accurately and efficiently. This paper aims to provide an overview of digital forensics and highlight some of the most popular techniques and tools used in the field.

Keywords: *digital evidence, cybercrime, computer crimes, electronic fraud, recovery and preservation of electronic data, analysis of electronic data, disk imaging, file carving, network forensics, memory analysis, mobile forensics, digital forensics tools, en case, forensic toolkit (FTK), sleuth kit, encryption, anti-forensic techniques, cloud-based storage.*

GJCST-E Classification: *LCC Code: HV8079.2-8109.5*

Strictly as per the compliance and regulations of:

Digital Forensics: Techniques and Tools for Cybercrime Investigations

Madhav Vedpathak [α] & Aarti Kashid [σ]

Abstract- **Digital forensics is a crucial aspect of modern-day investigations, particularly those involving cyber crimes. With the increasing prevalence of digital devices, the amount of electronic evidence available for investigation has also grown significantly. Therefore, it is essential to have the necessary techniques and tools to extract and analyse digital evidence accurately and efficiently. This paper aims to provide an overview of digital forensics and highlight some of the most popular techniques and tools used in the field.**

Keywords: digital evidence, cybercrime, computer crimes, electronic fraud, recovery and preservation of electronic data, analysis of electronic data, disk imaging, file carving, network forensics, memory analysis, mobile forensics, digital forensics tools, en case, forensic toolkit (FTK), sleuth kit, encryption, anti-forensic techniques, cloud-based storage.

I. Introduction

Digital forensics is a branch of forensic science that involves the recovery, preservation, and analysis of electronic data. Digital forensics is essential in investigating cybercrimes, computer crimes, and electronic fraud. With the widespread use of digital devices in everyday life, digital forensics has become an essential tool for law enforcement agencies, corporations, and government agencies. The objective of this paper is to provide a comprehensive overview of digital forensics, including its history, techniques, tools, and challenges.

II. History of Digital Forensics

The history of digital forensics can be traced back to the 1970s when computer forensics began. In the early days of computer forensics, the focus was on recovering data from computer hard drives. However, with the advent of the internet and the proliferation of digital devices, digital forensics has expanded to include the recovery and analysis of data from a wide range of devices, including smartphones, tablets, and cloud-based storage.

III. Digital Forensics Objectives

The primary objective of digital forensics is the identification, preservation, extraction, interpretation, and documentation of electronic evidence. Digital forensics is typically used to support criminal investigations, litigation, and other legal proceedings. However, digital forensics is also used in non-criminal cases, such as data breach investigations, corporate investigations, and employee misconduct investigations.

IV. Digital Forensics Techniques

Digital forensics employs a wide range of techniques to extract and analyze electronic evidence. The Disk Imaging: Disk imaging is the process of creating a bit-by-bit copy of a digital device's hard drive. The purpose of disk imaging is to preserve the integrity of the data and prevent any changes to the original data. Disk imaging is essential in any digital forensic investigation, as it provides a reliable and accurate copy of the original data.

1. *File Carving:* File carving is the process of extracting deleted files from a digital device. This technique involves searching for deleted files based on specific file signatures and recovering them. File carving is essential in cases where files have been intentionally or unintentionally deleted, as it allows investigators to recover valuable evidence.
2. *Network Forensics:* Network forensics involves the analysis of network traffic to identify and gather evidence related to cybercrime the capture and analysis of network packets to identify the source and destination of data, the type of data transmitted, and any anomalies in the traffic. Network forensics is used in cases such as data breaches, network intrusions, and malware attacks.
3. *Memory Analysis:* Memory analysis is the process of analyzing a digital device's volatile memory to identify and gather evidence related to cybercrime. Volatile memory includes data stored in RAM, which is lost when a device is turned off or restarted. Memory analysis involves capturing the memory image of a running system and analyzing it to identify running processes, network connections, and any malicious code present in the memory.
4. *Mobile Forensics:* Mobile forensics involves the recovery and analysis of data from mobile devices, such as smartphones and tablets. Mobile forensics includes techniques such as logical and physical extraction, file carving, and analysis of app data, call logs, and messaging data. Mobile forensics is

Author α σ: Guide: Prof. Salunkhe A. A (HOD of Computer Department) Rajgad Dnyanpeeth Technical Campus Polytechnic, Gat No. 237, Pune Bangalore Highway, Dhangawadi, Tal. Bhor, Dist - Pune.
e-mail: themadhavvedpathak@gmail.com

such as smartphones and tablets. Mobile forensics includes techniques such as logical and physical extraction, file carving, and analysis of app data, call logs, and messaging data. Mobile forensics is essential in cases where mobile devices are involved in criminal activities, such as drug trafficking, terrorism, and child exploitation.

V. Digital Forensics Tools

Digital forensics tools are software applications that are used to assist in digital forensic investigations. Digital forensics tools are designed to assist in disk imaging, file carving, network analysis, and memory analysis. Some of the commonly used digital forensics tools include:

1. *EnCase:* EnCase is a commercial digital forensic tool that is used for disk imaging, file carving, and memory analysis. EnCase has a user-friendly interface and provides a wide range of features for digital forensic investigations.
2. *Forensic Toolkit (FTK):* FTK is a commercial digital forensic tool that is used for disk imaging, file carving, and mobile forensics. FTK provides advanced search and analysis capabilities and is widely used in law enforcement agencies and government agencies.
3. *Sleuth Kit:* Sleuth Kit is an open-source digital forensic tool that is used for disk imaging and file carving. Sleuth Kit provides a command-line interface and can be used on a wide range of operating systems.

VI. Challenges in Digital Forensics

Digital forensics faces several challenges, including the following:

1. *Encryption:* Encryption makes it challenging to extract and analyze electronic evidence. Encryption is commonly used to protect data, and without the proper decryption keys, investigators cannot access the data.
2. *Anti-Forensic Techniques:* Anti-forensic techniques are used to hide or destroy electronic evidence. Anti-forensic techniques include file wiping, encryption, and data hiding.
3. *Complexity:* Digital devices are becoming increasingly complex, making it challenging to extract and analyze electronic evidence. The use of cloud-based storage, virtual machines, and encrypted communication channels makes it difficult for investigators to gather electronic evidence.

VII. Conclusion

Digital forensics is an essential tool for investigating cybercrime, computer crimes, and electronic fraud. Digital forensics techniques, tools, and challenges are constantly evolving, and investigators need to stay up to date with the latest developments to conduct effective digital forensic investigations. Digital forensics is critical in maintaining the integrity of digital data and ensuring that justice is served in criminal and civil cases. digital data and ensuring that justice is served in criminal and civil cases.

References Références Referencias

1. Casey, E., & Carrier, B. (Eds.). (2014). Handbook of digital forensics and investigation. Academic Press.
2. Nelson, B., Phillips, A., & Steuart, C. (2018). Guide to computer forensics and investigations. Cengage Learning.
3. "Computer Forensics: Investigating Data and Image Files" by EC-Council.
4. "Challenges in Digital Forensic Investigations of Cybercrime in India" by Geeta Sharma and B. B. Gupta.

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 23 Issue 1 Version 1.0 Year 2022
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Cybersecurity and Cyber Defence: Nationwide Level Strategic Method

By Shyam Meshram & Saurabh Mittal
Patil University

Abstract- Data, working knowledge (OT), and an extensive range of other practices, tools, and concepts are all comprised under the canopy term of cybersecurity. The aggressive use of info skill to bout opponents is a characteristic eye of cyberse-curity. Clienteles and security doctors are misinformed and the significant changes between these sentences are hidden by the use of the term ”cybersecurity” as a key challenge and a substitute for info security or IT security. The period ”cybersecurity” should only be used to mention to security practices related to self-justifying actions involving or relying on info skill and/or working knowledge surroundings and schemes, according to the orientation of security leaders. In this paper, we define ”cyberse-curity” and thoughtful how info security, working skill security (OTS), IT security, and other related punishments and practices, such as cyber protection, are connected to each additional and how they are practically in agreement with the nationwide cybersecurity plan, whether it be present or deliberate.

Keywords: Action plan, cyberattack; cybercrime; cyber defence; cyber operations; cybersecurity; national cybersecurity strategy; people-centric security.

GJCST-E Classification: LCC Code: QA76.9.A25

Strictly as per the compliance and regulations of:

Cybersecurity and Cyber Defence: Nationwide Level Strategic Method

Shyam Meshram [α] & Saurabh Mittal [σ]

Abstract- Data, working knowledge (OT), and an extensive range of other practices, tools, and concepts are all comprised under the canopy term of cybersecurity. The aggressive use of info skill to bout opponents is a characteristic eye of cyberse-curity. Clienteles and security doctors are misinformed and the significant changes between these sentences are hidden by the use of the term "cybersecurity" as a key challenge and a substitute for info security or IT security. The period "cybersecurity" should only be used to mention to security practices related to self-justifying actions involving or relying on info skill and/or working knowledge surroundings and schemes, according to the orientation of security leaders. In this paper, we define "cyberse-curity" and thoughtful how info security, working skill security (OTS), IT security, and other related punishments and practices, such as cyber protection, are connected to each additional and how they are practically in agreement with the nationwide cybersecurity plan, whether it be present or deliberate. The Nationwide Cybersecurity Plan of the State of Croatia and its Act Strategy is obtainable and expounded upon in the case education providing as an instance. The main formats of the plan are to classify organizational issues with implementation and to upsurge consciousness of the implication of this problematic in growth.

Keywords: *Action plan, cyberattack; cybercrime; cyber defence; cyber operations; cybersecurity; national cybersecurity strategy; people-centric security.*

I. Introduction

Armed organizations have been using cybersecurity tech-niques for more than ten years. The phrase has been used in many different contexts in new years, numerous of which bear slight or no relation to the phrase's unique sense. The misappropriation of the term confuses the rank of the proce-dures that syndicate info security, working skill (OT) safety, and IT safety procedures related to numerical possessions to form the cybersecurity discipline. Cyber defense examines the numerous threats that could exist for the given setting with a sympathizer of the particular setting. The strategies obligatory to protect against malicious attacks or intimidations are then industrialized and applied with its help. Cyber resistance includes a wide range of varied doings for both the defense of the board object and for the rapid reply to a danger scenery.

Author α σ: Ajeenkya D.Y. Patil university Pune, Maharashtra, India.
e-mails: shyam.meshram@adypu.edu.in, mittal.saurabhin2512@gmail.com

These might include creation the setting fewest inviting to possible assailants, meaningful where subtle data and critical sites are, putt preemptive events in place to make bouts costly, having the aptitude to notice bouts, and having response and reply competences. In order to determine the routes and regions that attackers might use, cyber defense also performs technical analysis [1].

II. Review of Previous Work

Similar to how military skill has travelled into noncom-batant businesses, military jargon has entered a non-military contexts. Similar changes have been experienced by additional terms, such as progressive tenacious danger [2]. A change in terminology has been frequently advantageous because it improves the level of specificity in discussions of technological operations. But when a term's distinctive meaning is lost or diminished during the transition to a new context, its usefulness is diminished.

a) Cybersecurity

Meaning: Cybersecurity is the ascendency, growth, organi-zation and usage of data safety, OT safety, and IT security tools and methods for attaining controlling obedience, defensive possessions and conciliatory the possessions of opponents [2]. The authors mentioned above claim that cybersecurity.

1. Is a subset of the performs found in information safety, operational safety, offensive safety, and IT safety;
2. Employs the gears and methods of info security, working security, and IT safety to reduce weaknesses, preserve system honesty, restrict access to authorized users, and protect possessions;
3. Comprises the growth and usage of aggressive IT- or OT-based bouts in contradiction of opponents, and (4) ropes info pledge objects (for example, paper documents).
4. Supports information pledge goals in a digital setting, but excludes analogue media security But, in the similar period, cyber security is not
    1. Just used as a substitute for info safety, OT security, or IT safety; and
    2. Used to protect an enterprise from criminal activity.

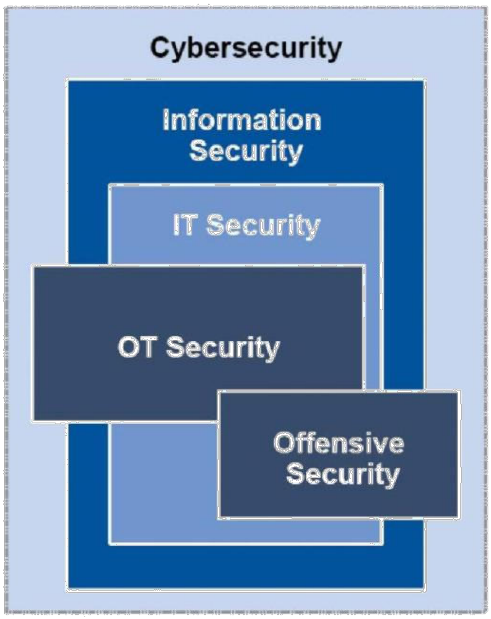


Figure 1: Components of Cybersecurity

3. Cyber warfare - although the term's definition is still debatable, it is generally agreed that "cyber warfare" mentions to the application of cybersecurity tools to combat situations. This is a complex area, and information warfare and physical attacks on infrastructure (such as the destruction of property and machinery) should not be confused with one another.
4. Cyberterrorism refers to the usage cybersecurity practices as a component of a guerilla movement or action, much like cyber warfare does.
5. Cybercrime. The term "cybercrime" simply mentions to criminal attacks that use IT infrastructure. Cybersecurity is unrelated to it.

Suitable usages of "cybersecurity" [2] would be the resulting:

1. The section increased its investment in cybersecurity in reply threat, danger valuations to enable the discount of weaknesses and enhanced competences for attacks
2. Integration of OT and IT security programmed inside the cybersecurity team allows for more comprehensive replies to intimidations.
3. A variety of cybersecurity strategies are used by the "" group Anonymous to further its goals (use of offensive capabilities).

However, there are some instances where the term "cyberse-curity" is used improperly:

1. The stock's cybersecurity plan recommends the use of whole drive encryption to reduce laptop theft. (This paragraph outlines a fundamental IT security action.)
2. The cybersecurity policy requires all CAM schemes on the shop floor to use strong passwords. This explains a Cyber defense

Despite their widespread use in the television and in na-tionwide and global organizational statements, there are no universal definitions for terms used in the cyberspace. Instead, they are unspoken to nasty dissimilar belongings by dissimilar states and governments [3]. Though, [1] delivers the follow-ing meaning and additional clarification of the term "cyber defense": A processed net protection mechanism known as "cyber defense" comprises reply to threats, dangerous sub-structure defense, and info pledge for businesses, governments, and other possible nets. To safeguard that no substructure or data is cooperating, cyber protection emphases on stopping, detection, and quickly replying to attacks or intimidations. Cy-ber defense is crucial for the majority of entities in instruction to protect subtle info and possessions due to the upsurge in the capacity and difficulty of cyber attacks. The much-needed pledge to carry out procedures and actions without worrying about intimidations is provided by cyber defense. It assists in improving the most efficient use of resources and security strategy. Cyber protection, also assistances in enhancing the efficiency of security expenditures and resources, chiefly in sensitive areas. The United States (US) Section of Protection (DoD) has clear a new idea, Active Cyber Defense (ACD), as DoD's coordinated, real-time competence to uncover, notice, analyses, and alleviate intimidations and susceptibilities [4]. This was done in response to the need to hurry discovery of and response to hateful net actors.

III. Cyber Operations

Cyber processes include a wide range of tasks including cyber organization, cyber attack, misuse, and cyber defense. These actions are by their very nature preventative, protective, and recuperative. Here, we'll talk about ACD as a branch of cyber defense that emphases on integrating and automating a variety of services and devices to carry out reply movements in a timely manner.

A CD is made up of a number of rational purposes that capture information from enterprise-level building to working realization with the main goal of becoming a functioning constituent of the Ministry of Defense's cyber processes to aid in defending the republic from adversaries with a focus on the internet. The essential to be safe, which comprises the ideas of , defensive, aggressive, and defensive amongst the war-fighter areas of land, sea, air, space, and cyber, is one of the many requirements of war-fighter processes. Cyber is both a standalone domain with specific requirements for cyber defense and a mixing competence in the other areas [8]. Proactive, active, and regenerative are three complementary types of cyber defense. "Proactive" activities, maintain peak performance for mission functions and harden the cyber envi-ronment. "Active" activities "stop" or "limit" adversarial cyber action's harm in a time that is relevant to cyberspace. After a successful cyberattack, "reactive" activities bring efficiency or competence back. A shared outline of mechanization that comprises ACD as a subsection of combined cyber defense unites these categories to form a continuum of cybersecurity activities that take place continuously and concurrently on the nets. This article focuses on ACD [8].

Cyber defense also includes making actuarial-style predictions of the future and using non-real-time big-data analytics to discover tendencies in past information sources. Physical proximity and time are required for attacks in non-cyber domains to be carried out. Anyone with a Net joining is a possible member in this global fight space, making cyber sole in that there is no requirement for physical proximity to carry out a bat and that an attack can be carried out in a significantly shorter amount of time. By mixing numerous responses to deliver reply actions in cyber-relevant period, ACD addresses the significantly decreased time needed for a successful attack. The term "cyber-relevant time," which accommodates the demands of the battle space, is intentionally ambiguous.

The cyber-relevant period ranges from moments to mi-croseconds if the battleground is a Dominant Dispensation Unit (CPU) and Random Access Memory (RAM), and the fighters are competing package requests. Cyber relevant time ranges from mass to seconds if the fight interplanetary is amid two computers that are bodily near to one another. Cyber-relevant time is instants in a battle interplanetary amid two computers on conflicting flanks of the planet interacts via cable links. Cyber pertinent time ranges from instants to minutes with live operators and the delays brought on by reasoning dispensation, keystrokes, and mouse clicks. As the adversary gets smarter and faster, the requirements for ACD rise [8]. Decision support algorithms used in the ACD sense-making process may be influenced by these analytics, which may be fed data from the ACD monitoring activity. These past and upcoming analytics, however, fall outdoor the purview of real-time dispensation and, consequently, fall outdoor the purview of ACD.

IV. Basic Notions

In instruction to efficiently address the security intimidations in modern cyberspace, the Plan aims to attain a stable and synchronized reply from various organizations on behalf of all social subdivisions. The Plan acknowledges the standards that must be endangered, the appropriate organizations, and the steps necessary to implement such protection in a system-atic way. The Strategy is a declaration of the stakeholders' commitment to acting in their individual spheres of influence, collaborating with one another, and exchanging the essential data. It is a declaration of their willingness to last their own improvement and growth so that Croatian Internet will be structured, accessible, open, and secure. The approach to cyberspace is envisioned in the plan and act plan for its application as the society's virtual measurement. The aim of the Strategy and its implementation through the use of the events outlined in the Act plan is thus reliable with the European Union's Cybersecurity Plan [13] and is focused on achieving the highest level of capability and organization amongst all facets of our civilization in order to effectively implement the law and protect self-governing values in the virtual, or cyber, measurement of today's civilization. Only a common, effectively coordinated strategy involving a wide range of various institutions accountable for various sectors can accomplish such a goal. This is due to the very compli-cated field of cyber security, which now encompasses all facets of society and far surpasses the technical field from which it originally emerged with the fast growth of the Net and related info and message skills.

Therefore, the important problem in cyber security is one group, which is solved in the Plan by better and more real communication between all societal sections, making the most of the already-existing forms and their lawful obligations. Smearing the events outlined in the Action plan for each separate, impartial of the Plan should help achieve the doc-umented goals in various areas of cyber security. The plan will be implemented in large part within the outline of the existing coffers of the forms capable for the activities in a given amount and the forms that will also be complicated, according to the description of the

events obtainable in the Act plan for the application of the plan. The additional worth of these existing funds and other capitals is attained through structural events for better coordination and coordination in the work of numerous forms on related activities, a more effective information exchange, and, generally, through the interaction of various organizations and civilization subdivisions that have up until now not been adequately linked and synchronized when it originates to the doings connected to cyberspace. Adopting the Plan and Action Plan and implementing a methodical and all-encompassing method for cyber security are intended to accomplish an amount of goals that are crucial for the advancement of the whole civilization, in specific:

1. A methodical approach to the request and growth of the nationwide lawful outline version for the new, cyber measurement of the civilization.
2. Putting into action initiatives and strategies to increase the safety, dependability, and resilience of cyberspace;
3. establishing a more effective information-sharing system to guarantee an advanced standard of overall care in cyberspace.
4. Increasing the security consciousness of all internet users.
5. Promoting the creation of synchronized educational au-tomatic. Encourage research and growth, chiefly in the field of e-services.
6. A methodical strategy for international cyber security cooperation. The practice of method selected to define the Strategy's fillings was founded on identifying the over-all objectives of the Plan, the societal subdivisions it enclosed, and the fundamental values of method to the Strategy's application. At this stage of the information society's development, Croatia is divided into societal segments considered to be most important for cyber security. The following are the cyber security domains that were chosen:
7. Public communications infrastructure, e-government substructure, and electric financial facilities are further broken down into electric message and information substructure and services.
8. Critical infrastructure for communication and informa-tion, cybercrime management.

The Strategy not only acknowledges the cyber security areas, but also their relationships with one another, safeguarding synchronized preparation of all cooperative doings and capitals in the aforementioned cyber security parts. The following connections between the various aspects of fake security have been chosen:

1. Data security.
2. Coordinating practical efforts to address computer secu-rity incidents.
3. Collaboration on a global scale.
4. Cybersecurity education, research, development, and awareness-building. The Plan is based on the current laws and obligations, but it acknowledges the need for some laws to be changed through the application of the Action Plan's events and synchronized with the acknowl-edged supplies of the civilization's virtual measurement, which has previously become an essential component of all citizens' personal and expert lives as well as their daily activities.

Adopting the Strategy won't immediately address all the issues that have arisen and accumulated as a result of the rapid globalization of society and technological advancement over the past 20 years, issues that are now present in every aspect of our society.

Presenting long-term and methodical care for all upcoming tests in the society's virtual measurement through the Strategy is unquestionably the first step to a methodical and permanent development of the present national in the field of cyber security. This is crucial to the society's continued development.

V. General Goals of the Strategy

Submission and improvement of the nationwide legal outline using a systematic approach, custody in mind the coordination with global duties and trends in worldwide cyber security, to account for the new, cyber measurement of civilization; pur-suing actions and events to strengthen cyberspace's security, pliability, and dependability that must be taken to safeguard the accessibility, integrity, and privacy of the various groups of info used in cyberspace, both by the breadwinners of numerous electric and substructure services and by the users, i.e., all legal objects and people whose info schemes are linked to Internet; founding a device for info sharing that is more effective and required for a advanced equal of overall safety in cyberspace, wherein each investor is required to ensure the application of passable and consistent values of information defense, particularly with regard to certain groups of information; raising security awareness among all internet users using a plan that takes into account the unique characteristics of the community and secluded sectors, as well as those of individ-uals and legal entities, and that incorporates the outline of the essential instructive components into regular and additional school activities as well as the planning and execution of various creativities aimed at humanizing the over-all public about specific present issues in this part; encouraging the creation of unified educational programmed in colleges and universities through beleaguered and specialized sequences, by fusing the moot, public, and business sectors; fostering the growth of e-services by establishing the necessary minimal security standards and increasing user trust in e-services; encouraging

coordinated efforts between the academic, commercial, and public sectors by stimulating research and development; a methodical approach to international cooperation that enables effective knowledge transfer and synchronized info distribution among the various national establishments, organizations, and societal sectors that are competent, with the goal of identifying and developing competences for successful engagement in commercial doings in a global setting.

VI. Sectors of the Civilization and Forms of Cooperation of Cybersecurity Stakeholders

The scope of this Strategy was defined by defining the subdivisions of civilization and what they mean for the drives of this Plan, as well as the ways in which the stakeholders in cyber security cooperate. Following are the subdivisions of civilization and their meanings for the Plan:

1. The public sector, which includes a variety of competent authorities that are Strategy stakeholders, other state es-tablishments, bodies of local and local self-government units, lawful objects with community establishments and organizations that represent Internet users in a variety of ways, and entities required to implement Strategy-related measures.
2. The academic sector, working closely with the state es-tablishments, who are the Strategy's investors, and other educational organizations from the public and financial subdivisions, who in numerous ways represent operators of cyberspace and objects required to implement the Strategy's regulations.
3. The financial subdivision in close coordination with the pertinent state and controlling bodies that are the Strat-egy's investors, particularly the legal entities subject to special rules pertaining to dangerous substructures and defense, as well as all other legal objects and commercial objects on behalf of the users of cyberspace in various ways and objects required to implement the Strategy's events, with all of those lawful and commercial entities' unique characteristics.
4. The general public, which includes all operators of message and information skills. The level of security in cyberspace has a variety of effects on the populace. It also refers to people whose data are in cyberspace, but who do not actively use it.

The following are the types of stakeholder collaboration in cyber security that the Strategy envisions:

1. Intergovernmental coordination.
2. Cross-country collaboration between the community, moot, and business subdivisions.
3. Discussion with absorbed parties, and communication with the populace.
4. Global collaboration among those involved in cyberse-curity.

According to competencies, capabilities, and objectives as well as the functionaries expounded cyber security parts outlined in the Plan, all of these forms of collaboration are carried out in a systematic and synchronized way.

VII. Analysis and Results of Measures Application

The treated data are related to 77 measures (33 area-level events and 44 link-level area-level measures) registered with the Act Plan, which support a total of 35 specific goals and 8 over-all formats in the Plan developed in 5 areas-level and 4 link-level cyber security initiatives. Teamwork is the connection between actions taken to achieve both specific and general formats. For the strategy Plan and Act Plan's approach and drafting, as well as for some of the region's nations, a reference model has been created The strategy was methodical, clear, and all-inclusive. Analysis of a worldwide movement involving the hateful code behind Wanna Cry was also done in terms of approximations, i.e., lessened injury and learned educations.

The journalism arrangement allows for four degree interpre-tations on the rank of application: Fully applied/applied, ap-plied/carried out, applied/applied to a lesser grade/not started, and all events of the Act Plan have clear application indicators. Out of the 30 pertinent cyber security organizations in the Republic of Croatia, data from the accompanying reports of individual measures, along with analyses conducted in specific areas and the connections between those areas and those clear in the Policy's objectives and Action Plan application, have been processed. The consequences are as shadows:

a) For the Following Areas

1. Community Electric Transportations (3 Events): The Action Plan identified three Measures based on the Strategy's three goals. Application pointers include two short-term events with a 12-month limit for applica-tion (since the Strategy's adoption) and one long-term amount.
2. Electric organization (8 measures): The plan has three objects, and the act strategy has eight events that are both consecutive and reliant on, have real implemen-tation pointers that are descriptive, and have deadlines for application. The 2016 report does not include any information on how the measures were put into action. The main issue is the lack of adequate coordination between information technology development strategies and projects and security supplies.
3. Electric monetary facilities (4 measures): In this priority area, the Plan has established two planned goals, and Act Plan 4 assesses the precise

application deadlines and indicators that have already been met. The reports succumbed have demonstrated that while the events are being applied, they are not yet completely realized. 33 measures are present in all areas.

b) For regional links

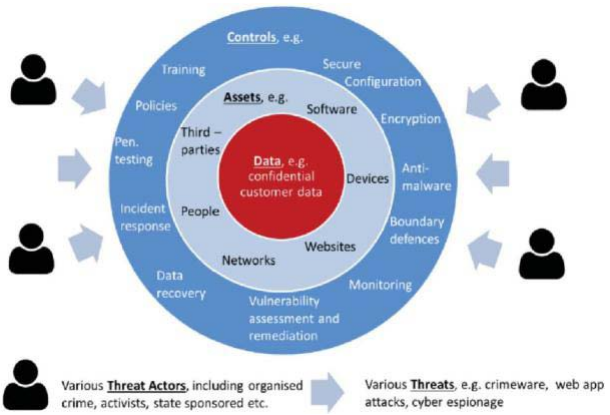
1. Information Defense (6 measures): The Plan has rec-ognized five objects, and the Act Strategy calls for six actions, with one action being implemented continuously for four actions for 12 or 24 months after the Strategy's adoption or the start of implementation, and one action's implementation being contingent upon the acceptance of EU orders.
2. Practical Organization in Computer Security Events (5 Measures): The Plan outlines three goals, and the Act Strategy for achieving these objectives includes five measures, one of which must be put into action 12 months after the Strategy's adoption while the other four must be continued unceasingly.
3. Global Co-operation (6 Measures): The Plan has set six objects, and the Act Plan calls for six actions to achieve these objectives. These actions must be implemented consistently and in a way that promotes success.
4. Teaching, Research, Growth, and Improvement of Cyber Security (27 Measures): The Plan outlines three objects, and the Act Strategy contain 27 measures to help achieve these objectives. Of these measures, three have imple-mentation deadlines in 2017-2018, two have deadlines of 6 or 12 months from the acceptance of the Plan, and the residual 22 should be approved out unceasingly.

The need for much healthier, exercise of lecturers at various heights and types of teaching, as well as much greater con-sistency in cyber security, is a major problem. There are 44 measures in all of the links. Total, there are 77 measures. By implementing the Act Plan events that provision the exact and overall objects of the Plan, it can be inferred from the results above that the Strategy 2016 was realized in agreement with the capabilities or appointment of all the investors designated by the Manager and the Assembly.

c) Cyber Defense

Despite their widespread use in the television and in na-tionwide and global organizational statements, there are no universal definitions for terms used in the cyberspace. Instead, they are unspoken to nasty dissimilar belongings by dissimilar states and governments [3]. Though, [1] delivers the following meaning and additional clarification of the term "cyber de-fense": A processer net protection mechanism known as "cyber defense" comprises reply to threats, dangerous substructure defense, and info pledge for businesses, governments, and other possible nets.

To safeguard that no substructure or data is cooperated, cyber protection emphases on stopping, detection, and quickly replying to attacks or intimidations. Cyber defense is crucial for the majority of entities in instruction to protect subtle info and possessions due to the upsurge in the capacity and difficulty of cyberattacks. The much-needed pledge to carry out procedures and actions without worrying about intimidations is provided by cyber defense. It assists in improving the most efficient use of resources and security strategy. Cyber protection also assistances in enhancing the efficiency of security expenditures and resources, chiefly in sensitive areas. The United States (US) Section of Protection (DoD) has clear a new idea, Active Cyber Defense (ACD), as DoD's coordinated, real-time competence to uncover, notice, analyses, and alleviate intimidations and susceptibilities [4]. This was done in response to the need to hurry discovery of and response to hateful net actors.



d) People-Centric Security

A plan that offers another to traditional information security practices is called "people-centric security" (PCS). PCS seeks to raid a balance amid employee agility and risk discount. It is a calculated method of information security that places less emphasis on limiting, preventative security measures and more on personal responsibility and trust. The old-style control-centric method to info security is flattering more and more impracticable in environments where technology, business, and risk are evolving quickly and becoming ever more complex.

Security directors in companies with the right ethos should look into whether some or all of PCS's ideas and precepts can be applied to their security plans. Such a study ought to point out instances in which a trust-based, cost-effective security strategy will be made possible by a more people-centric approach [5].

PCS is founded on a number of fundamental principles as well as on an individual's rights and associated obligations. The underlying idea behind PCS

is that workers have sure human rights. These, however, are connected to particular duties. These human rights and duties are founded on the sympathetic that, if a being bombs to achieve his or her obligations or bombs to act in a way that compliments the human rights of his or her classmates and other investors in the initiative, that person will face consequences.

1. This agreement of rights and obligations fosters a sense of codependency among employees, taking advantage of the social capital already present within the company.
2. According to PCS principles, transparent preventive controls, as opposed to intrusive preventative controls, should be prioritized over detectable and reactive con-trols.
3. PCS favors maximizing a trust environment in which personal initiative and autonomy are promoted.
4. PCS requires executive awareness and support, as well as an open, trust-based business ethos.
5. According to PCS principles, people must have the necessary information to comprehend their rights, obli-gations, and related choices.

On the other pointer, PCS is not

1. A spare for shared intelligence, defense in complexity security,
2. A loosening of safety supplies or social values,
3. Individuality organization, not exactly concentrating on an individual's digital identity,
4. Targeted at employees of the enterprise rather than all individuals, and
5. (Almost) security consciousness and exercise [3].

e) Methodology

Illustrates important cyber security elements and connec-tions:

1. Data are stowed, treated, and connected with, by, or to Possessions such as package, nets, plans, sites, persons, and 3rd gatherings
2. Information is stowed, treated, and connected with, by, or to Assets, in the majority of bags intimate data, such as client records or other valued info.
3. Danger Performers, including organized corruption bands, campaigners, and nation conditions, will use Intimidations to access Data, usually through or by targeting Possessions.
4. Threat-resistance controls are frequently practically to Possessions and sporadically straight to Data.
5. Approximately panels, like mobile device encoding, guard against particular threats, like the loss or robbery of moveable plans, whereas other panels, like package patching, guard in contradiction of a variety of intimi-dations, like somewhere, web app bouts, cyber spying, etc.
6. Intimidations will try to take advantage of Controls' flaws (or vulnerabilities) to access Data.
7. The group will be able to protect itself in contradiction of the Threat if the appropriate Panels are practical to the appropriate Possessions and they are applied efficiently compared to the equal of Danger. If this is not the circumstance, there will be a data opening.

VIII. Cybersecurity Strategy, Cyber Operations and Security Risk Management

The price of launching an attack simultaneously decreases while the cost of defensive cyber constructions and the rewards from fruitful bouts both continue to increase [6]. According to the traditional armed definition, "strategy" is the use of a country's entire force structure through extensive, long-term preparation and growth in order to guarantee safety or conquest. That strategy was successful in old-style wars against old-style colossal foes. The Merriam-Webster meaning of the plan as "an adaptation or complex of adaptations (as of behavior, metabolism, or structure) that serves or appears to serve an important function in achieving evolutionary success" is more pertinent for today's biosphere of unequal fighting and fast evolving intimidations. Receiving to inferior levels of susceptibility is the key to increasing cybersecurity. Even though threat awareness is crucial, all attacks are made more challenging by reducing vulnerabilities [7].

Cybersecurity risk management: Ashley Madison, the US Workplace of Workers Organization, and JP Morgan Chase are just a few examples of companies that have experienced cyber security breaches that have shown the threat is real and present. Admiral Mike Rodgers, director of the Nationwide Security Activity and commander of the United States Fake Knowledge, was enthused to say that "It's not a matter of if you will be penetrated, but when." [9].

As a result, it is crucial for businesses to accurately assess their current state of cyber security and, where essential, take quick corrective action to address flaws. Governments won't be able to achieve cyber security dangers and will nearly surely experience at opening if there is insufficient visibility into the status of their cyber security.

The term "visibility of cyber security status" refers to having the full picture and capacities to respond to the following queries:

1. What are the present slow heights of enterprise-wide cyber security danger due to the numerous threats we face?
2. Can we tolerate these cyber security dangers?
3. If not, what is our ordered, justifiable strategy for reducing these dangers to manageable levels?
4. Who is in charge and by when?

It is essential to be able to amount the state of cyber security because management is impossible without measurement. Data analytics and security event and event management (SIEM) tools can give helpful hints network compromises that have already occurred or could happen in the future, but these are only partial perspectives, not the capacities of our overall risk status. Threat intellect services work similarly in that they can spot data losses and give useful hints about current or upcoming attacks, but once more, these are not evaluations of our level of risk. Individual results from acquiescence organi-zation, vulnerability organization, penetration challenging, and reviews can all be characterized in the same way.

It is likely to reply to proceed and make decisions rapidly when there is surely in our cybersecurity risk capacities, for example:

1. Being able to classify dangers that we are not ready to stand and having a strong and ordered risk-based action strategy for the switch developments required to decrease these dangers to a satisfactory equal.
2. To gain a deeper comprehension of how threat intellect, SIEM productions, and data analytics can be used to enable quicker, more precise responses.
3. To create defenses for investments in cyber security products and facilities based on risk. But because of the extremely high threat level and the rapid rate of alteration in both the danger and switch sceneries, we must be able to regularly update our assessment of our level of cyber security. As part of planning and budgeting, cybersecurity risk management used to be an annual process, but it is now a vital real-time organizer in the fight against cyberattacks [9].

When people, events, skill, or additional elements of the cyber security danger organization scheme are lacking, insufficient, or malfunction in some method, a cyber security breach con-sequence. Therefore, we must comprehend all of the crucial elements and how they interact.

This does not imply that your risk organization system must store information about each end opinion and the current state of each susceptibility on the net, as there are other gears that can do that; however, the danger organization system must be aware that every endpoint on the network has been recognized and that all dangerous vulnerabilities are being spoken as soon as they are discovered.

a) Cyberattack model (intrusion Kill Chain

A suitable attack model must be used in order to counter a cyberattack. An attack's current state and potential future states can be identified using a boat perfect. A bout perfect is a hypothesis-based perfect that will be used to forecast potential attacker actions. Our attack model is primarily based on the Lockheed-Martin Interruption Kill Chain (IKC) [10] model. IKC is a seven-stage model that an attacker must inevitably use to plan and execute an interruption. The IKC phases are shown as follows in Figure 3: [11]

1. Information gathering - gathering details about the tar-ge, such as the technologies it uses and any potential security holes.
2. Weaponization is the process of creating hateful code to exploit found weaknesses and combined it with un-known deliverable cargos like pdfs, docs, and pets.
3. Distribution: Moving the weaponized cargo to the in-tended location.
4. Misuse is the usage of security flaws to run hateful code.
5. Connection – In order for the adversary to uphold its perseverance in the beleaguered setting, Remote Access Trojans (RAT) are typically installed. Attackers may need to execute one or more IKCs to get around various self-justifying panels in order to defeat most advanced defense systems.

Cyber resiliency situational consciousness: The success of cyber resiliency is a consequence of prompt and syn-chronized movements resulting from an efficient execution procedure. Defenders in a hardy scheme must be able to recognize the movements of assailants, decipher their sense, and respond in a way that will minimize the effects of these movements and enable a speedy recovery of any assets that were harmed.

The side with information dominance has the best chance of winning, just like in any conflict. SA is the key to achieving information dominance (and denying it to the enemy). The following are the main points of SA's response to the question of which data:

Control and direction (C2). An adversary needs a channel of communication to manage its malware and carry out their operations. As a result, a C2 server connection is required. Actions. In the final stage of the kill chain, the opponent ac-complishes its goals by carrying out acts like data . Protectors can be sure that the opposition has advanced to this stage after completing earlier ones [11].

IX. National Cybersecurity Strategy and Action plan

Like the phone system was a period ago, the Internet is now unquestionably a necessary communications infrastructure. However, the Internet's development and technological foun-dations are very distinct from those of telecommunications or any other infrastructure.

As a result, distinct strategies are needed to guarantee dependable and secure facilities in cyberspace as opposed to on the outdated telecom nets, and distinct processes also need to be followed when developing public policy. Instead of adopting

strategies that only encourage higher spending or visibility, Gartner advises that nationwide cybersecurity rule takes a more pragmatic method of encouraging advanced heights of security in the Internet. The administration has a role to play, but attempting to increase cyberspace security through rule will be more like attempting to address global heating than it will be like to address policies pertaining to the banking, banking industry, or the automobile industry [7].

A countrywide cybersecurity plan should, in accordance with [7], make use of the government's resources to advance the normal security procedures used by businesses, adminis-tration entities, and individuals in their everyday use of the internet. Define the present areas of weakness, use influence close those gaps, evaluate development, and recurrence are the objectives of such a strategy. The government shouldn't try to switch the level of safety on the Net or pass laws requiring fixes as part of a nationwide cybersecurity strategy. The spread of cybersecurity is a problem that will only worsen as technology advances.

Similar to a storm readiness plan, which orders reshap-ing constructions or erecting advanced levees instead of the placement of more aquatic devices, the cybersecurity strategy should therefore place a greater emphasis on removing or protecting susceptibilities that enable bouts than on journalism attacks.

a) Case Study

The Nationwide Cyber Security Plan [12] is an article that the Republic of Croatia means to use to begin preparing the most crucial actions for safeguarding all users of contempo-rary electric services, including those in the community and commercial sectors as well as the over-all public.

b) Principles

Internet, substructure, and users under Croatian authority are all covered by the complete nature of the method to cyber security (citizenship, registration, domain, address); combining efforts from various cyber security fields, as well as their connection and supplementation, to make the internet a safer place; proactive approach involving ongoing activity and mea-sure adjustment and appropriate periodic strategic framework adaptation;

Strengthening resiliency, dependability, and adaptability through the application of universal standards for the defense of privacy and the privacy, honesty, and obtainability of sure groups of info, as well as through compliance with the relevant obligations related to these issues, including the application of suitable guarantee and authorization of various kin Application of fundamental principles as the cornerstone of contemporary society's organization in cyberspace, the virtual facet of so-ciety: application of the law to safeguard people's rights and freedoms, particularly privacy, property rights, and all other fundamental aspects of a modern, organized society;

creating a unified legal framework through coordinated efforts from all societal sectors, that is, the forms and lawful objects involved in this Plan; request of the subsidiarity code finished a methodically developed transmission of decision-making and reporting authority on cyber security matters to the suitable expert whose expertise is neighboring to the issue being determined in parts significant for cyber security, from group finished organization and collaboration to the practical subjects of replying to processer intimidations to specific message and info substructure;

By applying the proportionality principle, each area's costs and level of protection will rise in direct proportion to the risks it faces and its capacity to mitigate those risks.

c) Cybersecurity Areas

At the time the Strategy was being written, Croatia's top needs were evaluated, and these needs led to the definition of the cyber security areas. These areas cover security measures for the message and info substructure and facilities, including community electric communications, e-Government, and elec-tric monetary facilities, which are the substructure of major strategic importance for the whole society. Another crucial part of cyber security is the defense of vital information and communication infrastructure. It might exist in all three of the aforementioned infrastructure areas, but those characteristics are very different, so it's important to establish the standards for identifying them.

Although cybercrime has existed in civilization for a very long time and takes many dissimilar forms, at the current stage of the growth of the virtual measurement of society, it represents a continuous and a rising threat to the growth and financial wealth of every contemporary state. Because of this, combating cybercrime is also regarded as a priority in the arena of cyber security, and setting strategic objectives is essential to stepping up efforts to do so in the near future.

The component of the defense plan that falls under the purview of the office responsible for defense-related matters is the part of cyber defense. It will be the focus of separate discussion and action, carried out with the aid of all pertinent factors resulting from this Plan. and additional cyber-related nationwide security subjects are handled by a minor amount of the security and intellect system's competent bodies and need a distinct strategy, which will also make use of all the necessary components resulting from this Plan.

In instruction to classify the unique objectives intended to achieve developments in each separate area and the events required for attaining the of the Plan, cyber security parts are analyzed in relative to the

over-all gamuts of the Plan. The specific goals and actions that will be additional developed by the Act Plan for the Plan's application are chosen in consideration of the identified societal sectors and how the cyber security field affects each one, as well as the ways in which the various cyber security stakeholders cooperate with one another. The development of the cyber security areas adheres to the principles outlined in the Strategy.

It makes sense to assume that the susceptibility of geospatial information will eventually make it a target for actual bodily attacks on the data's objects.

X. Implementation of the Tactic

The defined, planned goals are elaborated on the active plan for the application of the plan, lengthways with the relevant establishments and a schedule of limits for their application. It also identifies the application measures required to attain those formats. The action plan for the strategy's application enables systematic oversight of the plan's implementation and acts as a mechanism for controlling whether a particular measure has been fully applied and has achieved the wanted consequence or whether it needs to be redefined in light of the new supplies.

It is essential to found a scheme of incessant nursing of the application of the Plan and Act plan in instruction to ascertain in due period, whether the Plan is producing the wanted con-sequences, that is, whether the clear goals are being achieved and the recognized events are applied within the deliberate time frame, and to also establish a device for coordinating all the capable administration forms in developing the suitable rules and replies to threats.

The Nationwide Cyber Security Council1 (hereafter "the National Council") will be established by the Administration of the Republic of Croatia with the aim of studying and refining the application of the Strategy and Act Plan for its application.

XI. Conclusion on Consequences

The majority of the organizations fulfilled their obligations and gave the Council the necessary information for analysis as part of the separate Action Plan events for which the Assembly demanded the completion of the procedure.

There have been some developments since the Act Plan's application got underway in 2016 among the 30 joint in-stitutions that make up the diverse stakeholder profiles in cybernetic security. Every institution and stakeholder have acknowledged and connected initiatives within their purview to the conceptual thematic measures of the Act Plan. A few managers in the measures' application have completed their tasks. For admission the application of events in the area of critical message and info organizations, it is essential for whole the application of activities and, if essential, to change the legal outline in the area of nationwide dangerous substructure before continuing with the application of national events in this area.

Cybersecurity needs to be much more consistent, and lec-turers at all educational levels and types need better training. Because of this, the effectiveness of the cybernetic security teaching programmed being run in the Republic of Croatia is in doubt.

All nationwide teaching programmed in this area must be developed with the Strategy and Action Plan's emphasis on developing cybersecurity as their framework, and the Council should participate in the Republic of Croatia's optional process for the pertinent office and other forms regarding curriculum improvement and the enhancement of all types and heights of teaching in the area of cybernetic safety and protection.

XII. Conclusion and Future Effort

The administration must play a significant part in encourag-ing advancement of cybersecurity. The high-leverage part of enhancing cybersecurity is reducing vulnerabilities. A strategy that focuses on operations is required. Many government orga-nizations serve as excellent examples of how to enforce current laws. The relationships and connections between numerous actors at various levels of hierarchy are a contributing factor to the limitations of the national cybersecurity strategy. Infor-mation and communication technologies have seen the most dynamic and all-encompassing technological development of any field. The fast growth and introduction of new facilities and crops have always been prioritized, while security-related anxieties have characteristically had little influence on the extensive adoption of new skills.

Modern information systems have very short life cycles from the time of their planning, introduction, and use for the time they are removed from use, which frequently makes systematic testing them impossible. Instead, testing is most frequently practical as an exclusion, in specifically specified bags. The majority of commercial products have security fea-tures that protect user data confidentiality and confidentiality, but because users typically have little information on the skill they use and it is practiced in such a method that it is very difficult to approximation these security features, many of these products are sold commercially. The users' boldness towards message and information skill as a result is largely based on unreasoning sureness.

Technology in the areas of communication and information is pervasive in contemporary societies. Nowadays, text, image, and sound are transmitted between people using a variety of technologies, with the growing Internet of Things (IoT) tendency. While a sure type of message and information orga-nization's deviation from normal operation may go ignored, the indecorous operation of additional systems may have

severe repercussions on the state's ability to function. These consequences can include loss of life, health problems, signifi-cant material damage, environmental pollution, and disruption of other functions that are crucial to the society's ability to function as a whole.

A variety of factors, including human mistake, malicious action, technological error, and organizational oversight, have contributed to deviations in the proper operation of message and info skills from the time of their inception up until the present.

The development of the Internet and the linking of numerous information and communication systems used by the commu-nity, moot, and commercial subdivisions as well as individuals shaped the modern Internet, which is made up of this inter-connected infrastructure as well as users communicating more and more with one another using an increasing number of dissimilar facilities, some brand-new and some more old-style but in a new, computer-generated way.

Nonconformities in how these unified systems or their components should function are no lengthier just practical issues; they pose a threat to worldwide security. The term "cyber security" refers to a variety of actions and policies that modern societies use to combat them. In light of the susceptibility of geospatial information, it may ultimately be rational to anticipate bouts that have a bodily impact on the data's.

References Références Referencias

1. Cyber Defense. https://www.techopedia.com/definition/6705/cyber-defense. Accessed 2017-02-10.
2. A. Walls, Perkins E, Weiss J. Definition: "Cybersecur¬ity", G00252816. Gartner Inc.; 2013.
3. NATO Cyber Cooperative Cyber Defence Center of Excellence Tallin Estonia. https://ccdcoe.org/cyber-defi nitions.html. Accessed 2017-02-10.
4. United States Department of Defense. Strategy for operating in cy-berspace. Department of Defense; 2011.
5. Scholtz T. Definition: "People-Centric Security", G00250121. Gartner Inc.; 2013.
6. Infosecurity. http://infosecurityinc.net/wp-content/uploads/2011/07/Consult-Cyber-1Cyber-Threats¬Diminishing-Attack-Costs-galncreasing-Complexity4. jpg. Accessed 2016-11-15.
7. Pescatore J. Toward a national cybersecurity strategy, G00167598. Gartner Inc.; 2009.
8. Herring MJ, Willett KD. Active cyber defense: a vision for real-time cyber defense. J Inform Warfare. 2014;13 (2):46–55.
9. Marvell S. The real and present threat of a cyber breach demands real-time risk management. Acuity Risk Management; 2015.
10. Hutchins EM, Cloppert MJ, Amin RM. Intelligence-driven computer network defense informed by analysis of adversary campaigns and in-trusion kill chains. 6th Annual International Conference on Information War¬fare and Security; 2011.
11. Yano ET, Gustavsson PM, A hlfeldt R. A framework to support the development of cyber resiliency with situa¬tional awareness capability. 20th ICCRTS Proceedings: C2, Cyber, and Trust. International Com-mand and Control Institute; pp. 1–11, 2011.
12. Government of the Republic of Croatia. The national cyber security strategy and action plan for the imple¬mentation of the strategy. Official Gazette; 108/2015, 2015.
13. European Commission, Cybersecurity strategy of the European Union: an open, safe and secure cyberspace, Brussels, 7.2.2013, JOIN 1 final, 2013.

Global Journals Guidelines Handbook 2023

www.GlobalJournals.org

Memberships

Fellows/Associates of Computer Science Research Council

FCSRC/ACSRC Memberships

Introduction

FCSRC/ACSRC is the most prestigious membership of Global Journals accredited by Open Association of Research Society, U.S.A (OARS). The credentials of Fellow and Associate designations signify that the researcher has gained the knowledge of the fundamental and high-level concepts, and is a subject matter expert, proficient in an expertise course covering the professional code of conduct, and follows recognized standards of practice. The credentials are designated only to the researchers, scientists, and professionals that have been selected by a rigorous process by our Editorial Board and Management Board.

Associates of FCSRC/ACSRC are scientists and researchers from around the world are working on projects/researches that have huge potentials. Members support Global Journals' mission to advance technology for humanity and the profession.

FCSRC

Fellow of Computer Science Research Council

FELLOW OF COMPUTER SCIENCE RESEARCH COUNCIL is the most prestigious membership of Global Journals. It is an award and membership granted to individuals that the Open Association of Research Society judges to have made a 'substantial contribution to the improvement of computer science, technology, and electronics engineering.

The primary objective is to recognize the leaders in research and scientific fields of the current era with a global perspective and to create a channel between them and other researchers for better exposure and knowledge sharing. Members are most eminent scientists, engineers, and technologists from all across the world. Fellows are elected for life through a peer review process on the basis of excellence in the respective domain. There is no limit on the number of new nominations made in any year. Each year, the Open Association of Research Society elect up to 12 new Fellow Members.

Benefit

To the institution

Get letter of appreciation

Global Journals sends a letter of appreciation of author to the Dean or CEO of the University or Company of which author is a part, signed by editor in chief or chief author.

Exclusive Network

Get access to a closed network

A FCSRC member gets access to a closed network of Tier 1 researchers and scientists with direct communication channel through our website. Fellows can reach out to other members or researchers directly.They should also be open to reaching out by other.

Career | Credibility | Exclusive | Reputation

Certificate

Certificate, LoR and Laser-Momento

Fellows receive a printed copy of a certificate signed by our Chief Author that may be used for academic purposes and a personal recommendation letter to the dean of member's university.

Career | Credibility | Exclusive | Reputation

Designation

Get honored title of membership

Fellows can use the honored title of membership. The “FCSRC” is an honored title which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., FCSRC or William Walldroff, M.S., FCSRC.

Career | Credibility | Exclusive | Reputation

Recognition on the Platform

Better visibility and citation

All the Fellow members of FCSRC get a badge of "Leading Member of Global Journals" on the Research Community that distinguishes them from others. Additionally, the profile is also partially maintained by our team for better visibility and citation. All fellows get a dedicated page on the website with their biography.

Career | Credibility | Reputation

Future Work

Get discounts on the future publications

Fellows receive discounts on future publications with Global Journals up to 60%. Through our recommendation programs, members also receive discounts on publications made with OARS affiliated organizations.

Career | Financial

GJ Account

Unlimited forward of Emails

Fellows get secure and fast GJ work emails with unlimited forward of emails that they may use them as their primary email. For example, john [AT] globaljournals [DOT] org.

Career | Credibility | Reputation

Premium Tools

Access to all the premium tools

To take future researches to the zenith, fellows receive access to all the premium tools that Global Journals have to offer along with the partnership with some of the best marketing leading tools out there.

Financial

Conferences & Events

Organize seminar/conference

Fellows are authorized to organize symposium/seminar/conference on behalf of Global Journal Incorporation (USA). They can also participate in the same organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent. Additionally, they get free research conferences (and others) alerts.

Career | Credibility | Financial

Early Invitations

Early invitations to all the symposiums, seminars, conferences

All fellows receive the early invitations to all the symposiums, seminars, conferences and webinars hosted by Global Journals in their subject.

Exclusive

Publishing Articles & Books

Earn 60% of sales proceeds

Fellows can publish articles (limited) without any fees. Also, they can earn up to 70% of sales proceeds from the sale of reference/review books/literature/publishing of research paper. The FCSRC member can decide its price and we can help in making the right decision.

Exclusive | Financial

Reviewers

Get a remuneration of 15% of author fees

Fellow members are eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get a remuneration of 15% of author fees, taken from the author of a respective paper.

Financial

Access to Editorial Board

Become a member of the Editorial Board

Fellows may join as a member of the Editorial Board of Global Journals Incorporation (USA) after successful completion of three years as Fellow and as Peer Reviewer. Additionally, Fellows get a chance to nominate other members for Editorial Board.

Career | Credibility | Exclusive | Reputation

And Much More

Get access to scientific museums and observatories across the globe

All members get access to 5 selected scientific museums and observatories across the globe. All researches published with Global Journals will be kept under deep archival facilities across regions for future protections and disaster recovery. They get 10 GB free secure cloud access for storing research files.

ASSOCIATE OF COMPUTER SCIENCE RESEARCH COUNCIL

ASSOCIATE OF COMPUTER SCIENCE RESEARCH COUNCIL is the membership of Global Journals awarded to individuals that the Open Association of Research Society judges to have made a 'substantial contribution to the improvement of computer science, technology, and electronics engineering.

The primary objective is to recognize the leaders in research and scientific fields of the current era with a global perspective and to create a channel between them and other researchers for better exposure and knowledge sharing. Members are most eminent scientists, engineers, and technologists from all across the world. Associate membership can later be promoted to Fellow Membership. Associates are elected for life through a peer review process on the basis of excellence in the respective domain. There is no limit on the number of new nominations made in any year. Each year, the Open Association of Research Society elect up to 12 new Associate Members.

Benefit

To the institution

Get letter of appreciation

Global Journals sends a letter of appreciation of author to the Dean or CEO of the University or Company of which author is a part, signed by editor in chief or chief author.

Exclusive Network

Get access to a closed network

A ACSRC member gets access to a closed network of Tier 2 researchers and scientists with direct communication channel through our website. Associates can reach out to other members or researchers directly.They should also be open to reaching out by other.

Career | Credibility | Exclusive | Reputation

Certificate

Certificate, LoR and Laser-Momento

Associates receive a printed copy of a certificate signed by our Chief Author that may be used for academic purposes and a personal recommendation letter to the dean of member's university.

Career | Credibility | Exclusive | Reputation

Designation

Get honored title of membership

Associates can use the honored title of membership. The “ACSRC” is an honored title which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., ACSRC or William Walldroff, M.S., ACSRC.

Career | Credibility | Exclusive | Reputation

Recognition on the Platform

Better visibility and citation

All the Associate members of ACSRC get a badge of "Leading Member of Global Journals" on the Research Community that distinguishes them from others. Additionally, the profile is also partially maintained by our team for better visibility and citation.

Career | Credibility | Reputation

Future Work

Get discounts on the future publications

Associates receive discounts on future publications with Global Journals up to 30%. Through our recommendation programs, members also receive discounts on publications made with OARS affiliated organizations.

Career | Financial

GJ Account

Unlimited forward of Emails

Associates get secure and fast GJ work emails with 5GB forward of emails that they may use them as their primary email. For example, john [AT] globaljournals [DOT] org.

Career | Credibility | Reputation

Premium Tools

Access to all the premium tools

To take future researches to the zenith, associates receive access to all the premium tools that Global Journals have to offer along with the partnership with some of the best marketing leading tools out there.

Financial

Conferences & Events

Organize seminar/conference

Associates are authorized to organize symposium/seminar/conference on behalf of Global Journal Incorporation (USA). They can also participate in the same organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent. Additionally, they get free research conferences (and others) alerts.

Career | Credibility | Financial

Early Invitations

Early invitations to all the symposiums, seminars, conferences

All associates receive the early invitations to all the symposiums, seminars, conferences and webinars hosted by Global Journals in their subject.

Exclusive

Publishing Articles & Books

Earn 30-40% of sales proceeds

Associates can publish articles (limited) without any fees. Also, they can earn up to 30-40% of sales proceeds from the sale of reference/review books/literature/publishing of research paper.

Exclusive | Financial

Reviewers

Get a remuneration of 15% of author fees

Associate members are eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get a remuneration of 15% of author fees, taken from the author of a respective paper.

Financial

And Much More

Get access to scientific museums and observatories across the globe

All members get access to 2 selected scientific museums and observatories across the globe. All researches published with Global Journals will be kept under deep archival facilities across regions for future protections and disaster recovery. They get 5 GB free secure cloud access for storing research files.

Associate	Fellow	Research Group	Basic
$4800 **lifetime designation**	$6800 **lifetime designation**	$12500.00 **organizational**	APC **per article**
Certificate, LoR and Momento **2** discounted publishing/year **Gradation** of Research **10** research contacts/day **1 GB** Cloud Storage **GJ** Community Access	**Certificate,** LoR and Momento **Unlimited** discounted publishing/year **Gradation** of Research **Unlimited** research contacts/day **5 GB** Cloud Storage **Online Presense** Assistance **GJ** Community Access	**Certificates,** LoRs and Momentos **Unlimited** free publishing/year **Gradation** of Research **Unlimited** research contacts/day **Unlimited** Cloud Storage **Online Presense** Assistance **GJ** Community Access	**GJ** Community Access

Preferred Author Guidelines

We accept the manuscript submissions in any standard (generic) format.

We typeset manuscripts using advanced typesetting tools like Adobe In Design, CorelDraw, TeXnicCenter, and TeXStudio. We usually recommend authors submit their research using any standard format they are comfortable with, and let Global Journals do the rest.

Alternatively, you can download our basic template from https://globaljournals.org/Template.zip

Authors should submit their complete paper/article, including text illustrations, graphics, conclusions, artwork, and tables. Authors who are not able to submit manuscript using the form above can email the manuscript department at submit@globaljournals.org or get in touch with chiefeditor@globaljournals.org if they wish to send the abstract before submission.

Before and during Submission

Authors must ensure the information provided during the submission of a paper is authentic. Please go through the following checklist before submitting:

1. Authors must go through the complete author guideline and understand and *agree to Global Journals' ethics and code of conduct,* along with author responsibilities.
2. Authors must accept the privacy policy, terms, and conditions of Global Journals.
3. Ensure corresponding author's email address and postal address are accurate and reachable.
4. Manuscript to be submitted must include keywords, an abstract, a paper title, co-author(s') names and details (email address, name, phone number, and institution), figures and illustrations in vector format including appropriate captions, tables, including titles and footnotes, a conclusion, results, acknowledgments and references.
5. Authors should submit paper in a ZIP archive if any supplementary files are required along with the paper.
6. Proper permissions must be acquired for the use of any copyrighted material.
7. Manuscript submitted *must not have been submitted or published elsewhere* and all authors must be aware of the submission.

Declaration of Conflicts of Interest

It is required for authors to declare all financial, institutional, and personal relationships with other individuals and organizations that could influence (bias) their research.

Policy on Plagiarism

Plagiarism is not acceptable in Global Journals submissions at all.

Plagiarized content will not be considered for publication. We reserve the right to inform authors' institutions about plagiarism detected either before or after publication. If plagiarism is identified, we will follow COPE guidelines:

Authors are solely responsible for all the plagiarism that is found. The author must not fabricate, falsify or plagiarize existing research data. The following, if copied, will be considered plagiarism:

- Words (language)
- Ideas
- Findings
- Writings
- Diagrams
- Graphs
- Illustrations
- Lectures

- Printed material
- Graphic representations
- Computer programs
- Electronic material
- Any other original work

Authorship Policies

Global Journals follows the definition of authorship set up by the Open Association of Research Society, USA. According to its guidelines, authorship criteria must be based on:

1. Substantial contributions to the conception and acquisition of data, analysis, and interpretation of findings.
2. Drafting the paper and revising it critically regarding important academic content.
3. Final approval of the version of the paper to be published.

Changes in Authorship

The corresponding author should mention the name and complete details of all co-authors during submission and in manuscript. We support addition, rearrangement, manipulation, and deletions in authors list till the early view publication of the journal. We expect that corresponding author will notify all co-authors of submission. We follow COPE guidelines for changes in authorship.

Copyright

During submission of the manuscript, the author is confirming an exclusive license agreement with Global Journals which gives Global Journals the authority to reproduce, reuse, and republish authors' research. We also believe in flexible copyright terms where copyright may remain with authors/employers/institutions as well. Contact your editor after acceptance to choose your copyright policy. You may follow this form for copyright transfers.

Appealing Decisions

Unless specified in the notification, the Editorial Board's decision on publication of the paper is final and cannot be appealed before making the major change in the manuscript.

Acknowledgments

Contributors to the research other than authors credited should be mentioned in Acknowledgments. The source of funding for the research can be included. Suppliers of resources may be mentioned along with their addresses.

Declaration of funding sources

Global Journals is in partnership with various universities, laboratories, and other institutions worldwide in the research domain. Authors are requested to disclose their source of funding during every stage of their research, such as making analysis, performing laboratory operations, computing data, and using institutional resources, from writing an article to its submission. This will also help authors to get reimbursements by requesting an open access publication letter from Global Journals and submitting to the respective funding source.

Preparing your Manuscript

Authors can submit papers and articles in an acceptable file format: MS Word (doc, docx), LaTeX (.tex, .zip or .rar including all of your files), Adobe PDF (.pdf), rich text format (.rtf), simple text document (.txt), Open Document Text (.odt), and Apple Pages (.pages). Our professional layout editors will format the entire paper according to our official guidelines. This is one of the highlights of publishing with Global Journals—authors should not be concerned about the formatting of their paper. Global Journals accepts articles and manuscripts in every major language, be it Spanish, Chinese, Japanese, Portuguese, Russian, French, German, Dutch, Italian, Greek, or any other national language, but the title, subtitle, and abstract should be in English. This will facilitate indexing and the pre-peer review process.

The following is the official style and template developed for publication of a research paper. Authors are not required to follow this style during the submission of the paper. It is just for reference purposes.

Manuscript Style Instruction (Optional)

- Microsoft Word Document Setting Instructions.
- Font type of all text should be Swis721 Lt BT.
- Page size: 8.27" x 11'", left margin: 0.65, right margin: 0.65, bottom margin: 0.75.
- Paper title should be in one column of font size 24.
- Author name in font size of 11 in one column.
- Abstract: font size 9 with the word "Abstract" in bold italics.
- Main text: font size 10 with two justified columns.
- Two columns with equal column width of 3.38 and spacing of 0.2.
- First character must be three lines drop-capped.
- The paragraph before spacing of 1 pt and after of 0 pt.
- Line spacing of 1 pt.
- Large images must be in one column.
- The names of first main headings (Heading 1) must be in Roman font, capital letters, and font size of 10.
- The names of second main headings (Heading 2) must not include numbers and must be in italics with a font size of 10.

Structure and Format of Manuscript

The recommended size of an original research paper is under 15,000 words and review papers under 7,000 words. Research articles should be less than 10,000 words. Research papers are usually longer than review papers. Review papers are reports of significant research (typically less than 7,000 words, including tables, figures, and references)

A research paper must include:

a) A title which should be relevant to the theme of the paper.
b) A summary, known as an abstract (less than 150 words), containing the major results and conclusions.
c) Up to 10 keywords that precisely identify the paper's subject, purpose, and focus.
d) An introduction, giving fundamental background objectives.
e) Resources and techniques with sufficient complete experimental details (wherever possible by reference) to permit repetition, sources of information must be given, and numerical methods must be specified by reference.
f) Results which should be presented concisely by well-designed tables and figures.
g) Suitable statistical data should also be given.
h) All data must have been gathered with attention to numerical detail in the planning stage.

Design has been recognized to be essential to experiments for a considerable time, and the editor has decided that any paper that appears not to have adequate numerical treatments of the data will be returned unrefereed.

i) Discussion should cover implications and consequences and not just recapitulate the results; conclusions should also be summarized.
j) There should be brief acknowledgments.
k) There ought to be references in the conventional format. Global Journals recommends APA format.

Authors should carefully consider the preparation of papers to ensure that they communicate effectively. Papers are much more likely to be accepted if they are carefully designed and laid out, contain few or no errors, are summarizing, and follow instructions. They will also be published with much fewer delays than those that require much technical and editorial correction.

The Editorial Board reserves the right to make literary corrections and suggestions to improve brevity.

Format Structure

It is necessary that authors take care in submitting a manuscript that is written in simple language and adheres to published guidelines.

All manuscripts submitted to Global Journals should include:

Title

The title page must carry an informative title that reflects the content, a running title (less than 45 characters together with spaces), names of the authors and co-authors, and the place(s) where the work was carried out.

Author details

The full postal address of any related author(s) must be specified.

Abstract

The abstract is the foundation of the research paper. It should be clear and concise and must contain the objective of the paper and inferences drawn. It is advised to not include big mathematical equations or complicated jargon.

Many researchers searching for information online will use search engines such as Google, Yahoo or others. By optimizing your paper for search engines, you will amplify the chance of someone finding it. In turn, this will make it more likely to be viewed and cited in further works. Global Journals has compiled these guidelines to facilitate you to maximize the web-friendliness of the most public part of your paper.

Keywords

A major lynchpin of research work for the writing of research papers is the keyword search, which one will employ to find both library and internet resources. Up to eleven keywords or very brief phrases have to be given to help data retrieval, mining, and indexing.

One must be persistent and creative in using keywords. An effective keyword search requires a strategy: planning of a list of possible keywords and phrases to try.

Choice of the main keywords is the first tool of writing a research paper. Research paper writing is an art. Keyword search should be as strategic as possible.

One should start brainstorming lists of potential keywords before even beginning searching. Think about the most important concepts related to research work. Ask, “What words would a source have to include to be truly valuable in a research paper?” Then consider synonyms for the important words.

It may take the discovery of only one important paper to steer in the right keyword direction because, in most databases, the keywords under which a research paper is abstracted are listed with the paper.

Numerical Methods

Numerical methods used should be transparent and, where appropriate, supported by references.

Abbreviations

Authors must list all the abbreviations used in the paper at the end of the paper or in a separate table before using them.

Formulas and equations

Authors are advised to submit any mathematical equation using either MathJax, KaTeX, or LaTeX, or in a very high-quality image.

Tables, Figures, and Figure Legends

Tables: Tables should be cautiously designed, uncrowned, and include only essential data. Each must have an Arabic number, e.g., Table 4, a self-explanatory caption, and be on a separate sheet. Authors must submit tables in an editable format and not as images. References to these tables (if any) must be mentioned accurately.

Figures

Figures are supposed to be submitted as separate files. Always include a citation in the text for each figure using Arabic numbers, e.g., Fig. 4. Artwork must be submitted online in vector electronic form or by emailing it.

Preparation of Eletronic Figures for Publication

Although low-quality images are sufficient for review purposes, print publication requires high-quality images to prevent the final product being blurred or fuzzy. Submit (possibly by e-mail) EPS (line art) or TIFF (halftone/ photographs) files only. MS PowerPoint and Word Graphics are unsuitable for printed pictures. Avoid using pixel-oriented software. Scans (TIFF only) should have a resolution of at least 350 dpi (halftone) or 700 to 1100 dpi (line drawings). Please give the data for figures in black and white or submit a Color Work Agreement form. EPS files must be saved with fonts embedded (and with a TIFF preview, if possible).

For scanned images, the scanning resolution at final image size ought to be as follows to ensure good reproduction: line art: >650 dpi; halftones (including gel photographs): >350 dpi; figures containing both halftone and line images: >650 dpi.

Color charges: Authors are advised to pay the full cost for the reproduction of their color artwork. Hence, please note that if there is color artwork in your manuscript when it is accepted for publication, we would require you to complete and return a Color Work Agreement form before your paper can be published. Also, you can email your editor to remove the color fee after acceptance of the paper.

Tips for writing a good quality Computer Science Research Paper

Techniques for writing a good quality computer science research paper:

1. Choosing the topic: In most cases, the topic is selected by the interests of the author, but it can also be suggested by the guides. You can have several topics, and then judge which you are most comfortable with. This may be done by asking several questions of yourself, like "Will I be able to carry out a search in this area? Will I find all necessary resources to accomplish the search? Will I be able to find all information in this field area?" If the answer to this type of question is "yes," then you ought to choose that topic. In most cases, you may have to conduct surveys and visit several places. Also, you might have to do a lot of work to find all the rises and falls of the various data on that subject. Sometimes, detailed information plays a vital role, instead of short information. Evaluators are human: The first thing to remember is that evaluators are also human beings. They are not only meant for rejecting a paper. They are here to evaluate your paper. So present your best aspect.

2. Think like evaluators: If you are in confusion or getting demotivated because your paper may not be accepted by the evaluators, then think, and try to evaluate your paper like an evaluator. Try to understand what an evaluator wants in your research paper, and you will automatically have your answer. Make blueprints of paper: The outline is the plan or framework that will help you to arrange your thoughts. It will make your paper logical. But remember that all points of your outline must be related to the topic you have chosen.

3. Ask your guides: If you are having any difficulty with your research, then do not hesitate to share your difficulty with your guide (if you have one). They will surely help you out and resolve your doubts. If you can't clarify what exactly you require for your work, then ask your supervisor to help you with an alternative. He or she might also provide you with a list of essential readings.

4. Use of computer is recommended: As you are doing research in the field of computer science then this point is quite obvious. Use right software: Always use good quality software packages. If you are not capable of judging good software, then you can lose the quality of your paper unknowingly. There are various programs available to help you which you can get through the internet.

5. Use the internet for help: An excellent start for your paper is using Google. It is a wondrous search engine, where you can have your doubts resolved. You may also read some answers for the frequent question of how to write your research paper or find a model research paper. You can download books from the internet. If you have all the required books, place importance on reading, selecting, and analyzing the specified information. Then sketch out your research paper. Use big pictures: You may use encyclopedias like Wikipedia to get pictures with the best resolution. At Global Journals, you should strictly follow here.

6. Bookmarks are useful: When you read any book or magazine, you generally use bookmarks, right? It is a good habit which helps to not lose your continuity. You should always use bookmarks while searching on the internet also, which will make your search easier.

7. Revise what you wrote: When you write anything, always read it, summarize it, and then finalize it.

8. Make every effort: Make every effort to mention what you are going to write in your paper. That means always have a good start. Try to mention everything in the introduction—what is the need for a particular research paper. Polish your work with good writing skills and always give an evaluator what he wants. Make backups: When you are going to do any important thing like making a research paper, you should always have backup copies of it either on your computer or on paper. This protects you from losing any portion of your important data.

9. Produce good diagrams of your own: Always try to include good charts or diagrams in your paper to improve quality. Using several unnecessary diagrams will degrade the quality of your paper by creating a hodgepodge. So always try to include diagrams which were made by you to improve the readability of your paper. Use of direct quotes: When you do research relevant to literature, history, or current affairs, then use of quotes becomes essential, but if the study is relevant to science, use of quotes is not preferable.

10.Use proper verb tense: Use proper verb tenses in your paper. Use past tense to present those events that have happened. Use present tense to indicate events that are going on. Use future tense to indicate events that will happen in the future. Use of wrong tenses will confuse the evaluator. Avoid sentences that are incomplete.

11. Pick a good study spot: Always try to pick a spot for your research which is quiet. Not every spot is good for studying.

12. Know what you know: Always try to know what you know by making objectives, otherwise you will be confused and unable to achieve your target.

13. Use good grammar: Always use good grammar and words that will have a positive impact on the evaluator; use of good vocabulary does not mean using tough words which the evaluator has to find in a dictionary. Do not fragment sentences. Eliminate one-word sentences. Do not ever use a big word when a smaller one would suffice.

Verbs have to be in agreement with their subjects. In a research paper, do not start sentences with conjunctions or finish them with prepositions. When writing formally, it is advisable to never split an infinitive because someone will (wrongly) complain. Avoid clichés like a disease. Always shun irritating alliteration. Use language which is simple and straightforward. Put together a neat summary.

14. Arrangement of information: Each section of the main body should start with an opening sentence, and there should be a changeover at the end of the section. Give only valid and powerful arguments for your topic. You may also maintain your arguments with records.

15. Never start at the last minute: Always allow enough time for research work. Leaving everything to the last minute will degrade your paper and spoil your work.

16. Multitasking in research is not good: Doing several things at the same time is a bad habit in the case of research activity. Research is an area where everything has a particular time slot. Divide your research work into parts, and do a particular part in a particular time slot.

17. Never copy others' work: Never copy others' work and give it your name because if the evaluator has seen it anywhere, you will be in trouble. Take proper rest and food: No matter how many hours you spend on your research activity, if you are not taking care of your health, then all your efforts will have been in vain. For quality research, take proper rest and food.

18. Go to seminars: Attend seminars if the topic is relevant to your research area. Utilize all your resources.

19. Refresh your mind after intervals: Try to give your mind a rest by listening to soft music or sleeping in intervals. This will also improve your memory. Acquire colleagues: Always try to acquire colleagues. No matter how sharp you are, if you acquire colleagues, they can give you ideas which will be helpful to your research.

20. Think technically: Always think technically. If anything happens, search for its reasons, benefits, and demerits. Think and then print: When you go to print your paper, check that tables are not split, headings are not detached from their descriptions, and page sequence is maintained.

21. Adding unnecessary information: Do not add unnecessary information like "I have used MS Excel to draw graphs." Irrelevant and inappropriate material is superfluous. Foreign terminology and phrases are not apropos. One should never take a broad view. Analogy is like feathers on a snake. Use words properly, regardless of how others use them. Remove quotations. Puns are for kids, not grunt readers. Never oversimplify: When adding material to your research paper, never go for oversimplification; this will definitely irritate the evaluator. Be specific. Never use rhythmic redundancies. Contractions shouldn't be used in a research paper. Comparisons are as terrible as clichés. Give up ampersands, abbreviations, and so on. Remove commas that are not necessary. Parenthetical words should be between brackets or commas. Understatement is always the best way to put forward earth-shaking thoughts. Give a detailed literary review.

22. Report concluded results: Use concluded results. From raw data, filter the results, and then conclude your studies based on measurements and observations taken. An appropriate number of decimal places should be used. Parenthetical remarks are prohibited here. Proofread carefully at the final stage. At the end, give an outline to your arguments. Spot perspectives of further study of the subject. Justify your conclusion at the bottom sufficiently, which will probably include examples.

23. Upon conclusion: Once you have concluded your research, the next most important step is to present your findings. Presentation is extremely important as it is the definite medium though which your research is going to be in print for the rest of the crowd. Care should be taken to categorize your thoughts well and present them in a logical and neat manner. A good quality research paper format is essential because it serves to highlight your research paper and bring to light all necessary aspects of your research.

Informal Guidelines of Research Paper Writing

Key points to remember:

- Submit all work in its final form.
- Write your paper in the form which is presented in the guidelines using the template.
- Please note the criteria peer reviewers will use for grading the final paper.

Final points:

One purpose of organizing a research paper is to let people interpret your efforts selectively. The journal requires the following sections, submitted in the order listed, with each section starting on a new page:

The introduction: This will be compiled from reference matter and reflect the design processes or outline of basis that directed you to make a study. As you carry out the process of study, the method and process section will be constructed like that. The results segment will show related statistics in nearly sequential order and direct reviewers to similar intellectual paths throughout the data that you gathered to carry out your study.

The discussion section:

This will provide understanding of the data and projections as to the implications of the results. The use of good quality references throughout the paper will give the effort trustworthiness by representing an alertness to prior workings.

Writing a research paper is not an easy job, no matter how trouble-free the actual research or concept. Practice, excellent preparation, and controlled record-keeping are the only means to make straightforward progression.

General style:

Specific editorial column necessities for compliance of a manuscript will always take over from directions in these general guidelines.

To make a paper clear: Adhere to recommended page limits.

Mistakes to avoid:

- Insertion of a title at the foot of a page with subsequent text on the next page.
- Separating a table, chart, or figure—confine each to a single page.
- Submitting a manuscript with pages out of sequence.
- In every section of your document, use standard writing style, including articles ("a" and "the").
- Keep paying attention to the topic of the paper.
- Use paragraphs to split each significant point (excluding the abstract).
- Align the primary line of each section.
- Present your points in sound order.
- Use present tense to report well-accepted matters.
- Use past tense to describe specific results.
- Do not use familiar wording; don't address the reviewer directly. Don't use slang or superlatives.
- Avoid use of extra pictures—include only those figures essential to presenting results.

Title page:

Choose a revealing title. It should be short and include the name(s) and address(es) of all authors. It should not have acronyms or abbreviations or exceed two printed lines.

Abstract: This summary should be two hundred words or less. It should clearly and briefly explain the key findings reported in the manuscript and must have precise statistics. It should not have acronyms or abbreviations. It should be logical in itself. Do not cite references at this point.

An abstract is a brief, distinct paragraph summary of finished work or work in development. In a minute or less, a reviewer can be taught the foundation behind the study, common approaches to the problem, relevant results, and significant conclusions or new questions.

Write your summary when your paper is completed because how can you write the summary of anything which is not yet written? Wealth of terminology is very essential in abstract. Use comprehensive sentences, and do not sacrifice readability for brevity; you can maintain it succinctly by phrasing sentences so that they provide more than a lone rationale. The author can at this moment go straight to shortening the outcome. Sum up the study with the subsequent elements in any summary. Try to limit the initial two items to no more than one line each.

Reason for writing the article—theory, overall issue, purpose.

- Fundamental goal.
- To-the-point depiction of the research.
- Consequences, including definite statistics—if the consequences are quantitative in nature, account for this; results of any numerical analysis should be reported. Significant conclusions or questions that emerge from the research.

Approach:

- Single section and succinct.
- An outline of the job done is always written in past tense.
- Concentrate on shortening results—limit background information to a verdict or two.
- Exact spelling, clarity of sentences and phrases, and appropriate reporting of quantities (proper units, important statistics) are just as significant in an abstract as they are anywhere else.

Introduction:

The introduction should "introduce" the manuscript. The reviewer should be presented with sufficient background information to be capable of comprehending and calculating the purpose of your study without having to refer to other works. The basis for the study should be offered. Give the most important references, but avoid making a comprehensive appraisal of the topic. Describe the problem visibly. If the problem is not acknowledged in a logical, reasonable way, the reviewer will give no attention to your results. Speak in common terms about techniques used to explain the problem, if needed, but do not present any particulars about the protocols here.

The following approach can create a valuable beginning:

- Explain the value (significance) of the study.
- Defend the model—why did you employ this particular system or method? What is its compensation? Remark upon its appropriateness from an abstract point of view as well as pointing out sensible reasons for using it.
- Present a justification. State your particular theory(-ies) or aim(s), and describe the logic that led you to choose them.
- Briefly explain the study's tentative purpose and how it meets the declared objectives.

Approach:

Use past tense except for when referring to recognized facts. After all, the manuscript will be submitted after the entire job is done. Sort out your thoughts; manufacture one key point for every section. If you make the four points listed above, you will need at least four paragraphs. Present surrounding information only when it is necessary to support a situation. The reviewer does not desire to read everything you know about a topic. Shape the theory specifically—do not take a broad view.

As always, give awareness to spelling, simplicity, and correctness of sentences and phrases.

Procedures (methods and materials):

This part is supposed to be the easiest to carve if you have good skills. A soundly written procedures segment allows a capable scientist to replicate your results. Present precise information about your supplies. The suppliers and clarity of reagents can be helpful bits of information. Present methods in sequential order, but linked methodologies can be grouped as a segment. Be concise when relating the protocols. Attempt to give the least amount of information that would permit another capable scientist to replicate your outcome, but be cautious that vital information is integrated. The use of subheadings is suggested and ought to be synchronized with the results section.

When a technique is used that has been well-described in another section, mention the specific item describing the way, but draw the basic principle while stating the situation. The purpose is to show all particular resources and broad procedures so that another person may use some or all of the methods in one more study or referee the scientific value of your work. It is not to be a step-by-step report of the whole thing you did, nor is a methods section a set of orders.

Materials:

Materials may be reported in part of a section or else they may be recognized along with your measures.

Methods:

- Report the method and not the particulars of each process that engaged the same methodology.
- Describe the method entirely.
- To be succinct, present methods under headings dedicated to specific dealings or groups of measures.
- Simplify—detail how procedures were completed, not how they were performed on a particular day.
- If well-known procedures were used, account for the procedure by name, possibly with a reference, and that's all.

Approach:

It is embarrassing to use vigorous voice when documenting methods without using first person, which would focus the reviewer's interest on the researcher rather than the job. As a result, when writing up the methods, most authors use third person passive voice.

Use standard style in this and every other part of the paper—avoid familiar lists, and use full sentences.

What to keep away from:

- Resources and methods are not a set of information.
- Skip all descriptive information and surroundings—save it for the argument.
- Leave out information that is immaterial to a third party.

Results:

The principle of a results segment is to present and demonstrate your conclusion. Create this part as entirely objective details of the outcome, and save all understanding for the discussion.

The page length of this segment is set by the sum and types of data to be reported. Use statistics and tables, if suitable, to present consequences most efficiently.

You must clearly differentiate material which would usually be incorporated in a study editorial from any unprocessed data or additional appendix matter that would not be available. In fact, such matters should not be submitted at all except if requested by the instructor.

Content:

- Sum up your conclusions in text and demonstrate them, if suitable, with figures and tables.
- In the manuscript, explain each of your consequences, and point the reader to remarks that are most appropriate.
- Present a background, such as by describing the question that was addressed by creation of an exacting study.
- Explain results of control experiments and give remarks that are not accessible in a prescribed figure or table, if appropriate.
- Examine your data, then prepare the analyzed (transformed) data in the form of a figure (graph), table, or manuscript.

What to stay away from:

- Do not discuss or infer your outcome, report surrounding information, or try to explain anything.
- Do not include raw data or intermediate calculations in a research manuscript.
- Do not present similar data more than once.
- A manuscript should complement any figures or tables, not duplicate information.
- Never confuse figures with tables—there is a difference.

Approach:

As always, use past tense when you submit your results, and put the whole thing in a reasonable order.

Put figures and tables, appropriately numbered, in order at the end of the report.

If you desire, you may place your figures and tables properly within the text of your results section.

Figures and tables:

If you put figures and tables at the end of some details, make certain that they are visibly distinguished from any attached appendix materials, such as raw facts. Whatever the position, each table must be titled, numbered one after the other, and include a heading. All figures and tables must be divided from the text.

Discussion:

The discussion is expected to be the trickiest segment to write. A lot of papers submitted to the journal are discarded based on problems with the discussion. There is no rule for how long an argument should be.

Position your understanding of the outcome visibly to lead the reviewer through your conclusions, and then finish the paper with a summing up of the implications of the study. The purpose here is to offer an understanding of your results and support all of your conclusions, using facts from your research and generally accepted information, if suitable. The implication of results should be fully described.

Infer your data in the conversation in suitable depth. This means that when you clarify an observable fact, you must explain mechanisms that may account for the observation. If your results vary from your prospect, make clear why that may have happened. If your results agree, then explain the theory that the proof supported. It is never suitable to just state that the data approved the prospect, and let it drop at that. Make a decision as to whether each premise is supported or discarded or if you cannot make a conclusion with assurance. Do not just dismiss a study or part of a study as "uncertain."

Research papers are not acknowledged if the work is imperfect. Draw what conclusions you can based upon the results that you have, and take care of the study as a finished work.

- You may propose future guidelines, such as how an experiment might be personalized to accomplish a new idea.
- Give details of all of your remarks as much as possible, focusing on mechanisms.
- Make a decision as to whether the tentative design sufficiently addressed the theory and whether or not it was correctly restricted. Try to present substitute explanations if they are sensible alternatives.
- One piece of research will not counter an overall question, so maintain the large picture in mind. Where do you go next? The best studies unlock new avenues of study. What questions remain?
- Recommendations for detailed papers will offer supplementary suggestions.

Approach:

When you refer to information, differentiate data generated by your own studies from other available information. Present work done by specific persons (including you) in past tense.

Describe generally acknowledged facts and main beliefs in present tense.

The Administration Rules

Administration Rules to Be Strictly Followed before Submitting Your Research Paper to Global Journals Inc.

Please read the following rules and regulations carefully before submitting your research paper to Global Journals Inc. to avoid rejection.

Segment draft and final research paper: You have to strictly follow the template of a research paper, failing which your paper may get rejected. You are expected to write each part of the paper wholly on your own. The peer reviewers need to identify your own perspective of the concepts in your own terms. Please do not extract straight from any other source, and do not rephrase someone else's analysis. Do not allow anyone else to proofread your manuscript.

Written material: You may discuss this with your guides and key sources. Do not copy anyone else's paper, even if this is only imitation, otherwise it will be rejected on the grounds of plagiarism, which is illegal. Various methods to avoid plagiarism are strictly applied by us to every paper, and, if found guilty, you may be blacklisted, which could affect your career adversely. To guard yourself and others from possible illegal use, please do not permit anyone to use or even read your paper and file.

Criterion for Grading a Research Paper (Compilation) by Global Journals Inc. (US)

Please note that following table is only a Grading of "Paper Compilation" and not on "Performed/Stated Research" whose grading solely depends on Individual Assigned Peer Reviewer and Editorial Board Member. These can be available only on request and after decision of Paper. This report will be the property of Global Journals Inc. (US).

Topics	Grades		
	A-B	**C-D**	**E-F**
Abstract	Clear and concise with appropriate content, Correct format. 200 words or below	Unclear summary and no specific data, Incorrect form Above 200 words	No specific data with ambiguous information Above 250 words
Introduction	Containing all background details with clear goal and appropriate details, flow specification, no grammar and spelling mistake, well organized sentence and paragraph, reference cited	Unclear and confusing data, appropriate format, grammar and spelling errors with unorganized matter	Out of place depth and content, hazy format
Methods and Procedures	Clear and to the point with well arranged paragraph, precision and accuracy of facts and figures, well organized subheads	Difficult to comprehend with embarrassed text, too much explanation but completed	Incorrect and unorganized structure with hazy meaning
Result	Well organized, Clear and specific, Correct units with precision, correct data, well structuring of paragraph, no grammar and spelling mistake	Complete and embarrassed text, difficult to comprehend	Irregular format with wrong facts and figures
Discussion	Well organized, meaningful specification, sound conclusion, logical and concise explanation, highly structured paragraph reference cited	Wordy, unclear conclusion, spurious	Conclusion is not cited, unorganized, difficult to comprehend
References	Complete and correct format, well organized	Beside the point, Incomplete	Wrong format and structuring

Index

save our planet

Global Journal of Computer Science and Technology

Visit us on the Web at www.GlobalJournals.org | www.ComputerResearch.org
or email us at helpdesk@globaljournals.org

ISSN 9754350