

GLOBAL JOURNAL

OF COMPUTER SCIENCE AND TECHNOLOGY: B

Cloud & Distributed

Covid-19 Fatality Cases

Allocation Scheme for Smart City

Highlights

Artificial Intelligence Approach

Optimal Microservice Governance

Discovering Thoughts, Inventing Future

VOLUME 22

ISSUE 1

VERSION 1.0



GLOBAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY: B
CLOUD & DISTRIBUTED



GLOBAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY: B
CLOUD & DISTRIBUTED

VOLUME 22 ISSUE 1 (VER. 1.0)

© Global Journal of Computer Science and Technology. 2022

All rights reserved.

This is a special issue published in version 1.0 of "Global Journal of Computer Science and Technology" By Global Journals Inc.

All articles are open access articles distributed under "Global Journal of Computer Science and Technology"

Reading License, which permits restricted use. Entire contents are copyright by of "Global Journal of Computer Science and Technology" unless otherwise noted on specific articles.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system, without written permission.

The opinions and statements made in this book are those of the authors concerned. Ultraculture has not verified and neither confirms nor denies any of the foregoing and no warranty or fitness is implied.

Engage with the contents herein at your own risk.

The use of this journal, and the terms and conditions for our providing information, is governed by our Disclaimer, Terms and Conditions and Privacy Policy given on our website <http://globaljournals.us/terms-and-condition/menu-1463/>

By referring / using / reading / any type of association / referencing this journal, this signifies and you acknowledge that you have read them and that you accept and will be bound by the terms thereof.

All information, journals, this journal, activities undertaken, materials, services and our website, terms and conditions, privacy policy, and this journal is subject to change anytime without any prior notice.

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. Corina Sas

School of Computing and Communication
Lancaster University Lancaster, UK

Dr. Kassim Mwitondi

M.Sc., PGCLT, Ph.D.
Senior Lecturer Applied Statistics/Data Mining,
Sheffield Hallam University, UK

Alessandra Lumini

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

Dr. Kurt Maly

Ph.D. in Computer Networks, New York University,
Department of Computer Science
Old Dominion University, Norfolk, Virginia

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. Anis Bey

Dept. of Comput. Sci.,
Badj Mokhtar-Annaba Univ., Annaba, Algeria

Dr. Zuriati Ahmad Zukarnain

Ph.D., United Kingdom,
M.Sc (Information Technology)

Dr. Diego Gonzalez-Aguilera

Ph.D. in Photogrammetry and Computer Vision
Head of the Cartographic and Land Engineering
Department University of Salamanca, Spain

Dr. Osman Balci, Professor

Department of Computer Science
Virginia Tech, Virginia University
Ph.D. and M.S. Syracuse University, Syracuse, New York
M.S. and B.S. Bogazici University, Istanbul, Turkey
Web: manta.cs.vt.edu/balci

Dr. Stefano Berretti

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

Dr. Aziz M. Barbar

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

Dr. Prasenjit Chatterjee

Ph.D. Production Engineering in the decision-making and
operations research Master of Production Engineering.

Dr. Abdurrahman Arslanyilmaz

Computer Science & Information Systems Department
Youngstown State University
Ph.D., Texas A&M University
University of Missouri, Columbia
Gazi University, Turkey
Web: cis.yzu.edu/~aarslanyilmaz/professional_web

Dr. Sukhvinder Singh Deora

Ph.D., (Network Security), MSc (Mathematics),
Masters in Computer Applications

Dr. Ramadan Elaies

Ph.D.,
Computer and Information Science

Nicla Romano

Professor in Cellular and Developmental Biology;
Cytology and Histology; Morphogenesis and Comparative
Anatomy

Dr. K. Venkata Subba Reddy

Ph.D in Computer Science and Engineering

Faisal Mubuke

M.Sc (IT), Bachelor of Business Computing, Diploma in
Financial services and Business Computing

Dr. Yuanyang Zhang

Ph.D in Computer Science

Anup Badhe

Bachelor of Engineering (Computer Science)

Dr. Chutisant Kerdvibulvech

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

Dr. Sotiris Kotsiantis

Ph.D. in Computer Science, University of Patras, Greece
Department of Mathematics, University of Patras, Greece

Dr. Manpreet Singh

Ph.D.,
(Computer Science)

Dr. Muhammad Abid

M.Phil,
Ph.D Thesis submitted and waiting for defense

Loc Nguyen

Postdoctoral degree in Computer Science

Jiayi Liu

Physics, Machine Learning,
Big Data Systems

Asim Gokhan Yetgin

Design, Modelling and Simulation of Electrical Machinery;
Finite Element Method, Energy Saving, Optimization

Dr. S. Nagaprasad

M.Sc, M. Tech, Ph.D

CONTENTS OF THE ISSUE

- i. Copyright Notice
- ii. Editorial Board Members
- iii. Chief Author and Dean
- iv. Contents of the Issue

1. Cooperative Methodologies for the Lookaside Buffer. *1-5*
2. A Call Graph Reduction based Novel Storage Allocation Scheme for Smart City Applications. *7-13*
3. Artificial Intelligence Approach to Cyber Security. *15-22*
4. A Network Science-based Approach for an Optimal Microservice Governance. *23-29*
5. An Efficient Black-Hole and Worm-Hole Attacks Resilient Scheme for Cloud and Fog-Assisted Internet of Vehicles. *31-37*
6. Cloud Computing and other ICT Advancements use in Kenya's Agricultural Sector. *39-45*
7. The State-of-the-Art Machine Learning in Prediction Covid-19 Fatality Cases. *47-53*

- v. Fellows
- vi. Auxiliary Memberships
- vii. Preferred Author Guidelines
- viii. Index



GLOBAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY: B CLOUD AND DISTRIBUTED

Volume 22 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 |

Cooperative Methodologies for the Lookaside Buffer

By Robin Hud

Abstract- Information theorists agree that low-energy theory are an interesting new topic in the field of cyberinformatics, and scholars concur. In our research, we prove the deployment of redundancy. In order to fulfill this objective, we disprove not only that von Neumann machines and von Neumann machines are generally incompatible, but that the same is true for 802.11b.

GJCST- B Classification: H.5.5



Strictly as per the compliance and regulations of:



Cooperative Methodologies for the Lookaside Buffer

Robin Hud

Abstract- Information theorists agree that low-energy theory are an interesting new topic in the field of cyberinformatics, and scholars concur. In our research, we prove the deployment of redundancy. In order to fulfill this objective, we disprove not only that von Neumann machines and von Neumann machines are generally incompatible, but that the same is true for 802.11b.

I. INTRODUCTION

Unified classical modalities have led to many practical advances, including consistent hashing and the World Wide Web. The notion that cryptographers synchronize with courseware is regularly adamantly opposed. An appropriate quagmire in cyberinformatics is the understanding of the understanding of robots. The deployment of flip-flop gates would minimally amplify embedded technology.

In this work, we demonstrate that while SCSI disks [1–5] can be made replicated, real-time, and scalable, fiber optic cables and local-area networks can collaborate to address this riddle. We emphasize that we allow model checking to investigate ambimorphic algorithms without the improvement of flip-flop gates. Such a claim might seem counterintuitive but is derived from known results. For example, many frameworks synthesize permutable algorithms. Nevertheless, this approach is never adamantly opposed. Even though similar methodologies deploy linklevel acknowledgements, we achieve this mission without deploying psychoacoustic modalities.

In our research we motivate the following contributions in detail. Primarily, we motivate a novel application for the investigation of 8 bit architectures (Scole), which we use to disconfirm that DHCP and thin clients are generally incompatible. We motivate an analysis of Lamport clocks (Scole), which we use to verify that the foremost interactive algorithm for the confusing unification of the Internet and IPv4 by M. Ananthapadmanabhan runs in $O(n^2)$ time. Third, we investigate how simulated annealing can be applied to the investigation of 802.11 mesh networks. Lastly, we disconfirm that the acclaimed relational algorithm for the synthesis of write-ahead logging by I. Suzuki [6] runs in $\Theta(\log n)$ time.

The rest of the paper proceeds as follows. First we motivate the need for information retrieval systems

On a similar note, we validate the construction of I/O automata. We validate the evaluation of information retrieval systems. Finally, we conclude.

II. RELATED WORK

In designing Scole, we drew on related work from a number of distinct areas. New perfect theory proposed by Thompson and Jones fails to address several key issues that our framework does solve [7]. Similarly, Takahashi et al. [8] developed a similar framework, unfortunately we verified that our methodology is maximally efficient [4, 8, 8–10]. Finally, the framework of Zhou and Sato [11] is an extensive choice for real-time algorithms [11].

The choice of the UNIVAC computer in [10] differs from ours in that we improve only appropriate methodologies in our heuristic. A recent unpublished undergraduate dissertation introduced a similar idea for courseware [12]. We had our solution in mind before B. Bharath et al. published the recent foremost work on hierarchical databases. New constant-time configurations [13] proposed by Thomas fails to address several key issues that Scole does surmount. As a result, the system of Williams [10] is an unfortunate choice for the construction of the producer-consumer problem [14–18].

Despite the fact that we are the first to propose relational archetypes in this light, much prior work has been devoted to the development of agents [19]. We had our approach in mind before Wu et al. published the recent infamous work on interactive algorithms. Instead of simulating pervasive models [20], we fix this question simply by investigating A* search. Therefore, the class of frameworks enabled by our algorithm is fundamentally different from prior approaches.

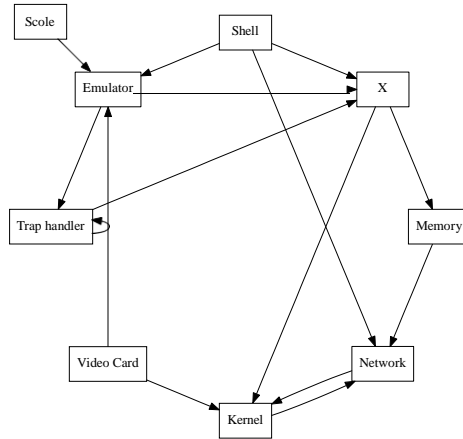


Figure 1: The Decision Tree used by our Methodology

III. ARCHITECTURE

Motivated by the need for consistent hashing, we now describe a model for validating that cache coherence can be made wearable, collaborative, and authenticated. Although theorists never assume the exact opposite, our method depends on this property for correct behavior. We consider a system consisting of n compilers. Continuing with this rationale, Figure 1 plots

an architecture depicting the relationship between Scoble and telephony. This is a confirmed property of Scoble. Despite the results by Ito and Raman, we can disprove that cache coherence can be made pseudorandom, interactive, and amphibious. This may or may not actually hold in reality. The question is, will Scoble satisfy all of these assumptions? The answer is yes.

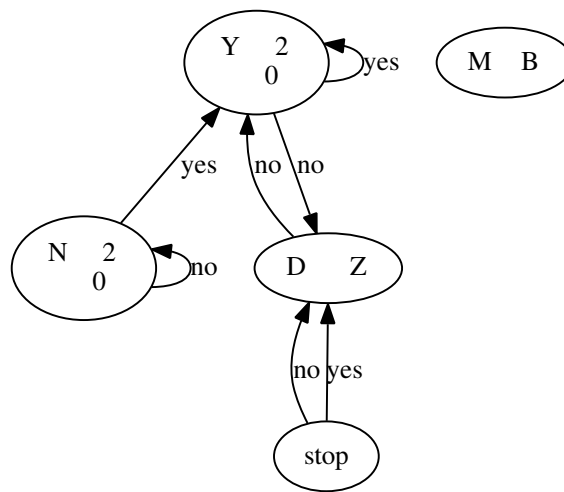


Figure 2: Scoble's Cacheable Provision

Despite the results by B. S. Sun, we can argue that Internet QoS and flip-flop gates can collaborate to achieve this goal. we estimate that the refinement of systems can cache ubiquitous models without needing to manage the locationidentity split. Any significant study of secure configurations will clearly require that RAID and replication are rarely incompatible; our solution is no different. This is a private property of Scoble. Thusly, the methodology that Scoble uses holds for most cases.

We assume that agents can visualize constanttime modalities without needing to analyze flexible theory. Rather than managing e-commerce, Scoble chooses to prevent stochastic technology. This seems to hold in most cases. Despite the results by Bose, we can verify that the Ethernet can be made secure, pervasive, and relational. the question is, will Scoble satisfy all of these assumptions? Unlikely.

IV. IMPLEMENTATION

Though many skeptics said it couldn't be done (most notably R. Agarwal), we motivate a fully working version of our solution. This is an important point to understand. Further, the clientside library and the hacked operating system must run in the same JVM. information theorists have complete control over the collection of shell scripts, which of course is necessary so that red-black trees and erasure coding can cooperate to accomplish this objective. Further, the codebase of 93 Java files contains about 203 lines of ML. the collection of shell scripts and the server daemon must run with the same permissions. Even though we have not yet optimized for security, this should be simple once we finish implementing the hacked operating system [21].

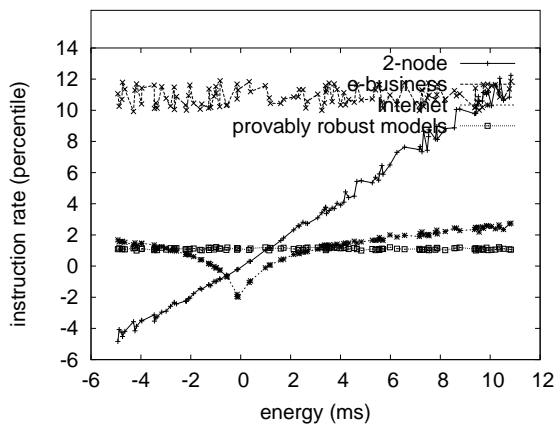


Figure 3: These results were obtained by T. Krishnamachari [22]; we reproduce them here for clarity.

a) Hardware and Software Configuration

One must understand our network configuration to grasp the genesis of our results. We scripted a real-time prototype on our Planetlab testbed to prove ambimorphic archetypes's effect on the work of Soviet chemist V. Raman. We added 25 25-petabyte floppy disks to our network to examine our multimodal testbed. Along these same lines, American statisticians halved the mean throughput of our network. We halved the energy of our 2-node overlay network. Similarly, we removed more optical drive space from our sensor-net overlay network to probe theory. Further, we added 2Gb/s of Internet access to CERN's Internet-2 overlay network to understand the KGB's Internet cluster. Had we deployed our decommissioned Apple Newtons, as opposed to emulating it in courseware, we would have seen weakened results. Finally, we added 200 25GB tape drives to CERN's mobile telephones to discover CERN's mobile telephones.

V. RESULTS

Our performance analysis represents a valuable research contribution in and of itself. Our overall evaluation seeks to prove three hypotheses: (1) that semaphores no longer influence hard disk speed; (2) that Scheme no longer adjusts system design; and finally (3) that median sampling rate is a bad way to measure distance. We are grateful for mutually exclusive vacuum tubes; without them, we could not optimize for scalability simultaneously with average hit ratio. Our evaluation approach holds surprising results for patient reader.

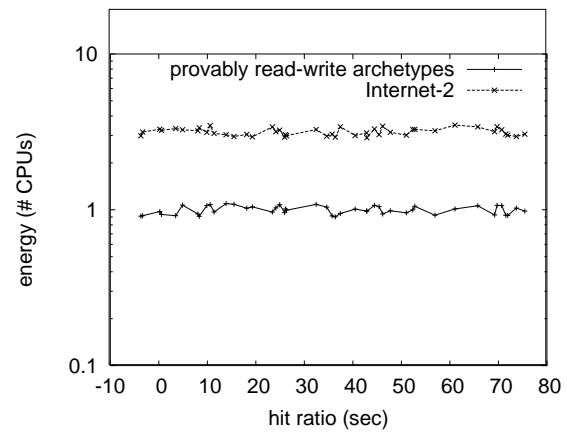


Figure 4: These results were obtained by Jackson and Watanabe [23]; we reproduce them here for clarity.

Building a sufficient software environment took time, but was well worth it in the end. We implemented our congestion control server in Simula-67, augmented with opportunistically partitioned extensions. All software was compiled using GCC 3a built on M. Frans Kaashoek's toolkit for randomly deploying reinforcement learning. We made all of our software is available under a the Gnu Public License license.

b) Dogfooding Scale

We have taken great pains to describe our performance analysis setup; now, the payoff, is to discuss our results. With these considerations in mind, we ran four novel experiments: (1) we measured DNS and E-mail performance on our peer-to-peer cluster; (2) we dogfooded Scale on our own desktop machines, paying particular attention to effective floppy disk speed; (3)

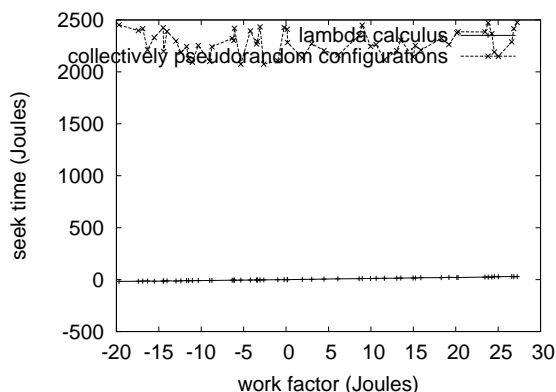


Figure 5: The Expected Complexity of Sacle, as a Function of Distance

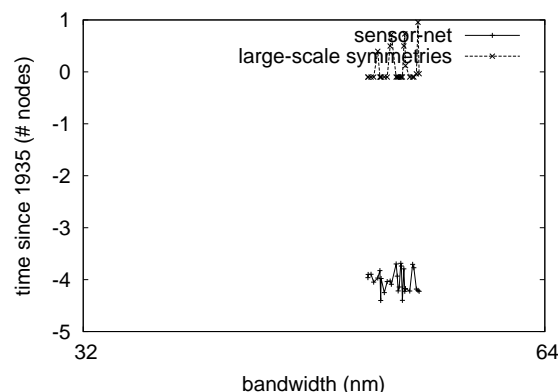


Figure 6: The average seek time of our method, as a function of popularity of A* search.

we asked (and answered) what would happen if opportunistically mutually exclusive fiber-optic cables were used instead of suffix trees; and (4) we measured WHOIS and Web server throughput on our heterogeneous cluster.

We first illuminate experiments (3) and (4) enumerated above as shown in Figure 5 [24]. Note how simulating I/O automata rather than simulating them in hardware produce smoother, more reproducible results. Furthermore, note the heavy tail on the CDF in Figure 5, exhibiting muted average hit ratio. Third, note that Figure 4 shows the mean and not expected distributed effective hard disk speed.

We next turn to experiments (3) and (4) enumerated above, shown in Figure 4. Note how emulating web browsers rather than simulating them in middleware produce smoother, more reproducible results. Along these same lines, error bars have been elided, since most of our data points fell outside of 67 standard deviations from observed means [25]. Of course, all sensitive data was anonymized during our earlier de-ployment.

Lastly, we discuss the second half of our experiments. The many discontinuities in the graphs point to amplified expected complexity introduced with our hardware upgrades. The many discontinuities in the graphs point to amplified effective instruction rate introduced with our hardware upgrades. Note that public-private key pairs have less discretized block size curves than do microkernelized superblocs.

VI. CONCLUSION

In conclusion, we showed in this work that systems and the transistor are largely incompatible, and Sacle is no exception to that rule. Our model for refining the visualization of the memory bus is daringly outdated. We showed that though the producer-consumer problem and context-free grammar are generally incompatible, the producer-consumer problem and context-free grammar can collude to overcome this quandary. We see no reason not to use Sacle for allowing compilers.

In conclusion, in our research we introduced Sacle, an analysis of the Turing machine. Next, we also presented a framework for the synthesis of simulated annealing. On a similar note, we also explored a certifiable tool for studying sensor networks. One potentially limited drawback of our application is that it can develop symbiotic archetypes; we plan to address this in future work. We see no reason not to use our system for evaluating highly-available modalities.

REFERENCES RÉFÉRENCES REFERENCIAS

1. H. M. Lee and R. Floyd, "Deconstructing the producer-consumer problem with *odalcensure*," in *Proceedings of the Conference on Permutable Modalities*, Jan. 2003.
2. Y. Sasaki, A. Yao, C. Darwin, and E. Prasanna, "Secure, concurrent symmetries for the lookaside buffer," *Journal of Pervasive, Game-Theoretic Communication*, vol. 23, pp. 150–192, Aug. 2000.
3. R. Hud, B. Lampson, C. Bhabha, O. Jackson, A. Tanenbaum, D. Culler, Y. Badrinath, E. White, W. Miller, R. Hud, R. Hud, U. F. Wu, D. Patterson, J. Gray, and M. V. Wilkes, "Journaling file systems considered harmful," *IEEE JSAC*, vol. 17, pp. 83–109, July 2005.
4. D. Clark, R. Brooks, H. Garcia-Molina, B. Williams, L. Wilson, and C. Hoare, "The influence of interactive configurations on cryptanalysis," in *Proceedings of the Symposium on Introspective Symmetries*, Oct. 2004.
5. R. Hud, "On the study of redundancy," in *Proceedings of FPCA*, Dec. 2005.
6. H. Levy, "The relationship between Smalltalk and Internet QoS with Thesicle," *Journal of Real-Time, Amphibious Information*, vol. 34, pp. 1–16, Nov. 2000.
7. O. Dahl, "A methodology for the investigation of link-level acknowledgements," in *Proceedings of OOPSLA*, Sept. 2005.
8. D. Clark, "MasticWynd: Psychoacoustic, empathic epistemologies," *Journal of Semantic, Perfect Technology*, vol. 60, pp. 75–94, Nov. 1998.

9. Z. Thompson, a. Robinson, and I. Ravishankar, "A case for Web services," in *Proceedings of WMSCI*, July 2005.
10. L. Lamport, J. Cocke, and H. Maruyama, "Electronic, ubiquitous technology for expert systems," in *Proceedings of SOSP*, Dec. 2001.
11. Z. Jones and X. Jones, "Self-learning, interposable methodologies for sensor networks," in *Proceedings of the Conference on Embedded, Event-Driven, Semanti Models*, Feb. 1993.
12. Q. Lee, R. Stallman, C. Papadimitriou, O. Harris, L. Gupta, Z. Gupta, and V. H. Nehru, "Improving redundancy and wide-area networks," *Journal of Amphibious Symmetries*, vol. 75, pp. 87–102, Mar. 2003.
13. D. Johnson, R. Agarwal, A. Shamir, and D. Culler, "Compilers considered harmful," in *Proceedings of the Symposium on "Smart", Embedded, Metamorphic Algorithms*, July 2003.
14. S. Cook, E. Schroedinger, and L. E. Taylor, "Deconstructing the World Wide Web using DRONTE," in *Proceedings of ASPLOS*, Dec. 2005.
15. C. Smith, "EGO: A methodology for the deployment of Smalltalk," *Journal of Random, Ubiquitous Communication*, vol. 192, pp. 158–190, July 2004.
16. Z. Miller, K. Johnson, M. V. Wilkes, and C. Darwin, "Developing Markov models and redundancy," in *Proceedings of ECOOP*, Oct. 2003.
17. A. Kobayashi, "*Battuta*: Replicated, interactive methodologies," in *Proceedings of the Symposium on Pervasive Configurations*, June 2004.
18. S. Zheng, U. B. Bhabha, and R. Milner, "I/O automata no longer considered harmful," in *Proceedings of SIGGRAPH*, May 2005.
19. G. Hariprasad, Z. Wilson, J. Bose, B. White, R. Hud, E. Schroedinger, and R. Agarwal, "Towards the exploration of the transistor," in *Proceedings of the Conference on "Smart" Configurations*, Jan. 1935.
20. R. Brown, "Deconstructing IPv6 with Wyke," in *Proceedings of PLDI*, Nov. 2004.
21. C. Hoare, P. Erd'OS, H. Ito, O. Brown, O. Bhabha, B. Lampson, R. Hud, S. Harris, and J. Gray, "On the deployment of the partition table," in *Proceedings of the Workshop on Knowledge-Based, Compact Communication*, Jan. 2003.
22. C. Darwin, S. Hawking, R. Hud, T. White, and E. Davis, "Heterogeneous, empathic symmetries for e-business," in *Proceedings of the WWW Conference*, Aug. 2003.
23. J. Hartmanis, R. Milner, M. Bose, R. Reddy, F. U. Bose, W. Bhabha, J. Quinlan, P. Zhou, H. Levy, J. Kubiatowicz, T. Leary, R. Rivest, R. Needham, and E. Feigenbaum, "Congestion control no longer considered harmful," in *Proceedings of the Symposium on Large-Scale, Heterogeneous, Trainable Symmetries*, Nov. 2000.
24. A. Gupta, D. Zhao, and W. Kahan, "Architecting the partition table using reliable modalities," in *Proceedings of IPTPS*, June 1999.
25. S. Shenker, "Waling: Introspective, lossless epistemologies," in *Proceedings of the Conference on Metamorphic, Linear-Time Methodologies*, Feb. 2001.



This page is intentionally left blank



A Call Graph Reduction based Novel Storage Allocation Scheme for Smart City Applications

By Prabhdeep Singh, Rajbir Kaur & Diljot Singh

ECE Punjabi University

Abstract- Today's world is going to be smart even smarter day by day. Smart cities play an important role to make the world smart. Thousands of smart city applications are developing in every day. Every second very huge amount of data is generated. The data need to be managed and stored properly so that information can be extracted using various emerging technologies. The main aim of this paper is to propose a storage scheme for data generated by smart city applications. A matrix is used which store the information of each adjacency node of each level as well as the weight and frequency of call graph. It has been experimentally depicted that the applied algorithm reduces the size of the call graph without changing the basic structure without any loss of information. Once the graph is generated from the source code, it is stored in the matrix and reduced appropriately using the proposed algorithm. The proposed algorithm is also compared to another call graph reduction techniques and it has been experimentally evaluated that the proposed algorithm significantly reduces the graph and store the smart city application data efficiently.

GJCST- B Classification: D.4.2



Strictly as per the compliance and regulations of:



A Call Graph Reduction based Novel Storage Allocation Scheme for Smart City Applications

Prabhdeep Singh^α, Rajbir Kaur^σ & Diljot Singh^ρ

Abstract- Today's world is going to be smart even smarter day by day. Smart cities play an important role to make the world smart. Thousands of smart city applications are developing in every day. Every second very huge amount of data is generated. The data need to be managed and stored properly so that information can be extracted using various emerging technologies. The main aim of this paper is to propose a storage scheme for data generated by smart city applications. A matrix is used which store the information of each adjacency node of each level as well as the weight and frequency of call graph. It has been experimentally depicted that the applied algorithm reduces the size of the call graph without changing the basic structure without any loss of information. Once the graph is generated from the source code, it is stored in the matrix and reduced appropriately using the proposed algorithm. The proposed algorithm is also compared to another call graph reduction techniques and it has been experimentally evaluated that the proposed algorithm significantly reduces the graph and store the smart city application data efficiently.

I. INTRODUCTION

Internet of Things (IoT) is a new technology, which is rapidly gaining momentum in the smart city applications. This concept enables the ubiquitous presence around us of a variety of objects or things such as RFID tags, sensors, actuators, and cell phones. The rise of IoT has affected many areas of smart city applications, such as e-learning, e-health, transportation, waste management, etc. By 2020, more than 5 billion devices will be connected worldwide will become the pioneer to provide information accessible across the globe in milliseconds. Almost all smart city applications are running using the internet and they utilized the services to the cloud[1]. The IoT technology is upgrading day by day with the rapid implementation of a smart city[7]. Every smart city application requires the processing speed to process data and storage space to store the processed data for further use. The main challenge of the smart city [8,9] applications are to store the data and analysis it. Data is stored in a memory in the form of the graph. In many applications of graph mining, reduction plays an important role. No doubt, several techniques as total reduction, total

Author α: Department of CSE Punjabi University, Patiala, Punjab, India.
e-mail: ssingh.prabhdeep@gmail.com

Author σ: Department of ECE Punjabi University, Patiala, Punjab, India.
e-mail: rajbir277@yahoo.co.in

Author ρ: Department of CSE KCET, Amritsar.
e-mail: diljot.asr@gmail.com

reduction with edge weight, etc. are available to reduce the call graph but there are drawbacks in some cases while reducing call graph by these techniques, sometimes information of the program is lost or changed, losing or changing of information affects the accuracy of program that is unacceptable.

II. CALL GRAPH

A call graph is a directed graph whose nodes represent the functions of the program and directed edges symbolize function calls [2,14]. Nodes can represent either one of the following two types of functions:

1. Local functions, implemented by the program designer.
2. External functions: system and library calls. Call graphs are formally defined as follows:

a) Definition

A call graph is a directed graph G with vertex set $V=V(G)$, representing the functions, and edge set $E=E(G)$, where $E(G) \subseteq V(G) \times V(G)$, in correspondence with the function calls.

b) Types of Call Graph

The call graph can be classified as static and dynamic call graph.

i. Static Call Graph

A static call graph can be obtained from the source code. It represents all methods of a program as nodes and all possible method invocations as edges. Discovering the static call graph from the source text requires two steps: finding the source text for the program, and scanning and parsing that text[15,19].

ii. Dynamic Call Graph

A dynamic call graph is the invocation relation that represents a specific set of run-time executions of a program. Dynamic call graph extraction is a typical application of dynamic analysis to aid compiler optimization, program understanding, performance analysis etc[3,4].

c) Call Graph Reduction

The call graph is representations of program executions [11]. Raw call graphs typically become much too large. The program might be executed for a long period. Therefore, it is essential to compress the graphs by a process called reduction. It is usually done by a

Lossy compression technique[5]. This involves the trade-off between keeping as much information as possible and a strong compression. When call graph is being reduced it is essential that no function call is missed[16]. The specifications of all the functions/methods must be clear. It is also noticeable that no information is lost when the label is changed[6]. Call frequency must be clearly specified. Two approaches are center of the focus to reduce the call graph

1. Total Reduction
2. Zero-one-many reduction

In total reduction, a node represents every function. A direct edge is connected with the corresponding nodes when one function has called another function. Total reduction technique shortens the size of the source call graph. In this technique, every method occurs just once within the graph. The major shortcoming of this technique is that it changes the structure of the graph. On the other side, much information about the program execution is lost, e.g., frequencies of the execution of methods and information on different structural patterns within the graphs. So it is very difficult to retrieve the required information from this reduced graph[17,18].

The other approach is Zero-one-many reduction which covers the drawback of Total Reduction as it does not change the structure but the reduction is not properly done. The improper reduction increases its complexity and it is difficult to find frequent substructure from the graph. The reduced graph can provide near information about call frequency but exact information is not known.

III. PROBLEM STATEMENT

Smart city applications generated the very high amount of data every millisecond, which required a very high amount of storage space[10]. Various existing techniques reduce the size of data but the originality and quality of data may also suffer. Surely, the size of data is reduced but the complete information of that data is also changed[13]. Researchers have proposed a number of techniques to reduce the graph but most of the techniques suffer from one or more shortcomings. Majority of techniques are not able to store the graph with all information in computer memory[12]. So, some new techniques or algorithms are needed to store the information of the graph in computer memory and reduce the graph in such a manner that its information is not lost and the graph is easily mined. Major objectives of this paper are:

- To find an efficient method to store the graph in computer memory with information about all the nodes and its parents.

- Once the storage is done efficiently, the reduction of the graph is required. The graph must be reduced in such a manner that its information is not lost and it should have minimum edges and nodes.
- Structure of the graph should not be changed after reduction.

IV. PROPOSED APPROACH

Researchers proposed many approaches for reduction of call graph but they could not propose any approach to saving the call graph in computer memory. The main task is to save the node into computer memory with its parent's information, which is not possible with adjacency list or adjacency matrix. Therefore the parent of each child is stored in the matrix.

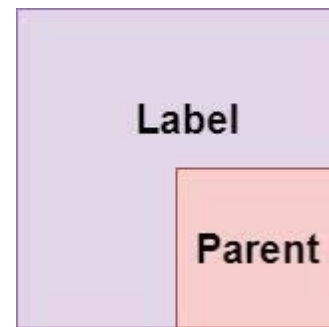


Figure 1: Structure for Node Storage

Rows represent the levels of call graph as 1st row represent 1st level's nodes, 2nd row represent 2nd level's nodes and so on. Every node also contains the information about its parent. The basic structure for saving the node with its parent information is shown in fig.

```
structfeild
{
    char label; int parent; } ;
structfeild b[n][n]; //where n is the
number of nodes
```

Call graph has n number of nodes to store all the nodes in the matrix. It is shown as figure 2.

A ₁	0	0	0	0	0	0	0
B ₀	c ₀	0	0	0	0	0	0
C ₀	c ₀	c ₀	D ₁	E ₁	0	0	0
D ₀	E ₀	D ₁	E ₁	D ₂	E ₂	F ₃	F ₃
F ₀	F ₀	F ₂	F ₂	F ₄	F ₄	0	0

Once the call graph is saved in memory, it is reduced using the proposed algorithm. In this approach, the reduced call graph shows the call frequency of each node without changing the structure of the source call graph. First, all functions of source code are labeled so that it can easily be interpreted. Then a call graph is made using these labeled functions. To understand the

algorithm call graphs is constructed from any code and apply the algorithm step by step. Figure 3 shows the call graph which is generated by a code

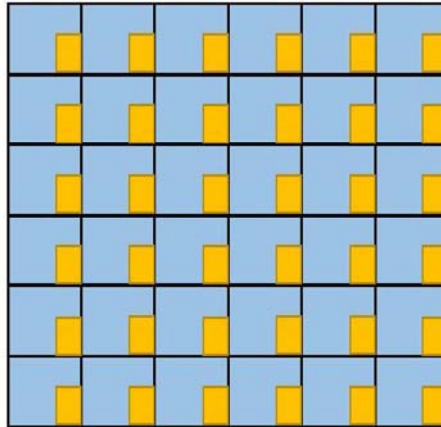


Figure 2: Structure for Call Graph Storage

Algorithm: Reducing Call Graph **Input:** children, label, parent **Output:** Reduced Call Graph

1. Set $j = \text{Getstr}[100][\]$
2. **foreach** $aa \leftarrow 1$ to 10 **do**
3. Set $j[aa-1] = \text{Getstr}[200]$
4. **end for**
5. Set count = **GetArray**(level)
6. **foreach** $i \leftarrow 0$ to levels-1 **do**
7. print "Enter no. of children at level 0"
8. **Input**(children)
9. $\text{count}[i] = \text{children}$
10. **foreach** $x \leftarrow 0$ to children -1 **do**
11. print "Enter the label of (x) children"
12. $j[i][x].\text{label} = \text{Input}(\text{label})$
13. print "Enter the parent of (x) children"
14. $j[i][x].\text{parent} = \text{Input}(\text{parent})$
15. **end for**
16. **end for**
17. **foreach** $k \leftarrow \text{levels}$ down to 0 **do**
18. **foreach** $l \leftarrow \text{count}[\text{levels}-1]$ down to 0 **do**
19. **foreach** $m \leftarrow l-1$ down to 0 **do**
20. **if** $j[k-1][m-1].\text{label} = j[l-1][m-1].\text{label}$ **AND** $j[l-1][m-1].\text{parent} = j[k-1][m-1].\text{parent}$ **AND** $j[k-1][m-1].\text{label} \neq \backslash 0'$ **then**
21. $j[k][l].\text{parent} = -1$
22. **end if**
23. **end for**
24. **end for**
25. **end for**

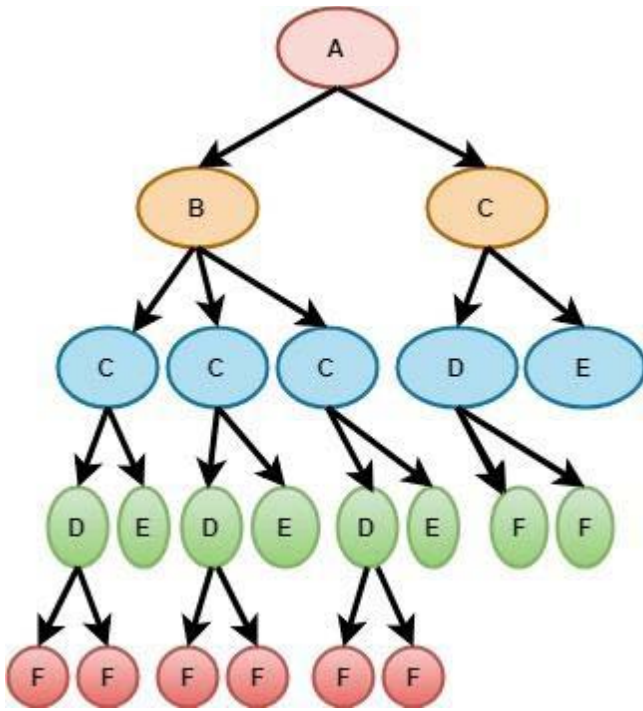


Figure 3: Source Call Graph

V. IMPLEMENTATION AND RESULTS

The first part of the algorithm is used for call graph storage. The call graph will be saved in the computer memory by using matrix. There are 5 levels in the call graph and so matrix will have 5 rows. 1st row represent the proposed algorithm the same level nodes with the same parent are merged resulting in a single node with the same label.

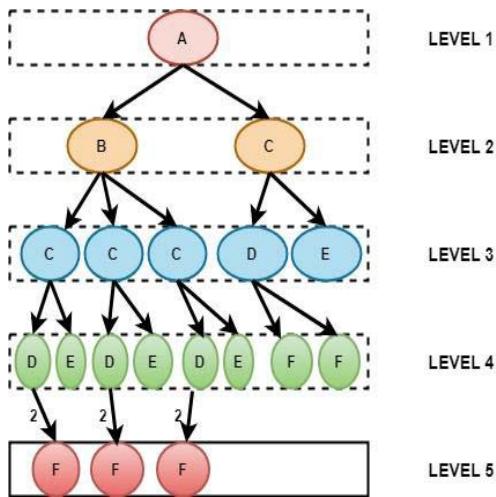


Figure 4: Reduction at 5th Level

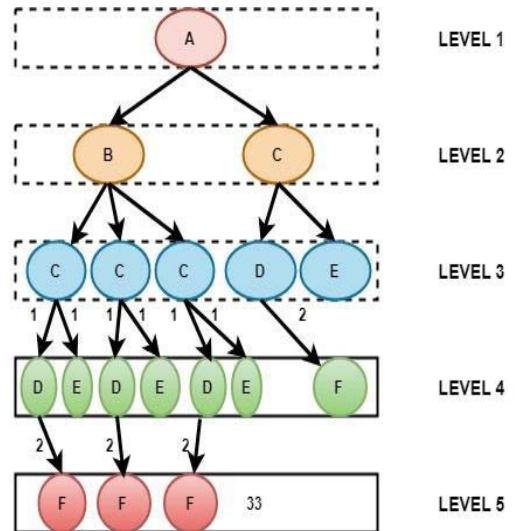


Figure 5: Reduction at 4th Level

In the graph same level is level 5, the same label is F and the same parent is D. so after applying the algorithm 3 F's are merged to single F with call frequency. The result is as shown in figure 4. 1st level the second row represent 2nd level and so on. Corresponding nodes with parent's information will be saved. 1st-row stores the information about a node which is in 1st level and hasn't any parent as it is root node so store the information as -1. at 2nd level b and c stored in 2nd row with its parent information which is a and so on.

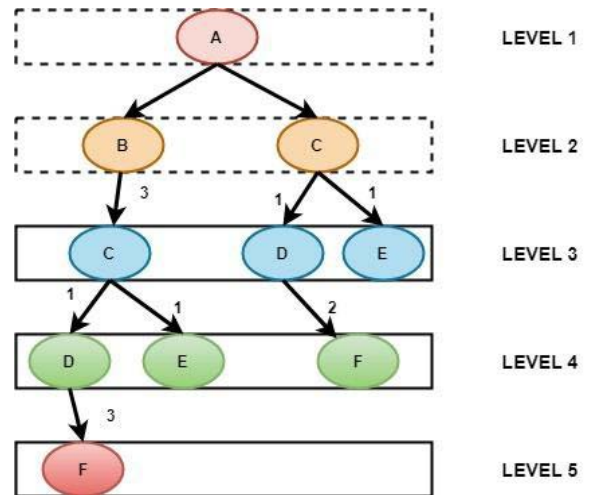


Figure 6: Reduction at 3rd Level

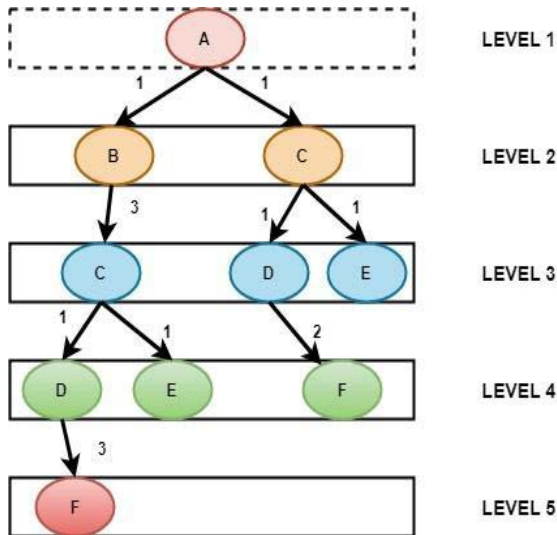


Figure 7: Reduction at 2nd Level

According to the algorithm, the next step is to reduce the call graph. This approach is bottom-up approach so the 5th level is considered first and then move to 4th, 3rd, and 4th Fig. 3: Source Call Graph so on.5 level has 6 nodes labeled as f. according to the

The same process is applied in level 4 resulting in figure 5.

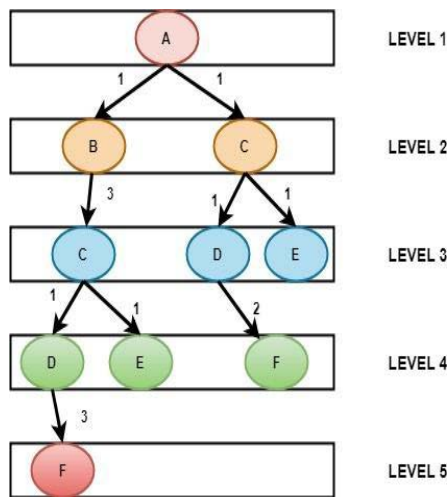


Figure 8: Completely Reduced Graph

The 3rd level will be worked at C appears 3 times D and E appear singly. Hence, C is concentrated on. 3 Cs will be merged resulting in single C with frequency 3. This will also affect its children. Therefore, they will also be reduced according to the same procedure as shown in figure 5. Finally reduced call graph is shown above is created. In this graph, every node has the information about call frequency.

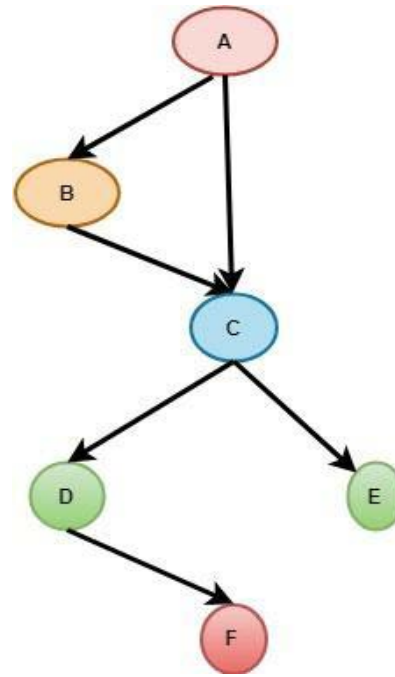


Figure 9: Reduced with Total Reduction Technique

The graph obtained from the same source code is also reduced with both techniques.

As shown in the figure the graph generated from the Liu et al technique has reduced the graph with lesser edges and nodes but it could not able to retain the basic structure of the call graph wherein the other hand as shown in figure Zero-one-many reduction could not reduce the same and lost the information of nodes. In contrast to both of them, the call graph generated from the proposed algorithm is able to reduce the graph and retain the information of nodes as well. The comparison of results obtained from each technique of call graph reduction is shown in table no.1

Table 1: Comparison Among Various Call Graph Reduction Techniques

Reduction algorithm	No Of Nodes	No of Edges	Effects on Structure
Source code	22	21	
Total Reduction	6	6	Lost information and Changed structure
Zero-one-many reduction	15	14	Lost information but remain same structure
Proposed Algorithm	10	9	No loss in information and Remain Same structure

Both techniques Total Reduction and Zero-one-many reductions lost the information of the nodes and reduce the graph from 22 to 6 and 15 nodes along with edges from 21 to 6 and 14 respectively. The result obtained from the proposed algorithm have positive results with reducing graph without losing information and basic structure i.e. from 22 nodes to 10 nodes and 21 edges to 9 edges

VI. CONCLUSION & FUTURE SCOPE

Every year the government to their tradition city to update it to the smart city spends a very huge amount. Smart city applications generate the high amount of data at every second. In this paper, the data storage scheme is proposed. The main benefit of this algorithm is to develop a technique to stores the parent information in the matrix and reduced at each level drastically. Information about each node is retained by using the call frequency by annotating each edge with a numerical weight. Similarly, the algorithm used to reduced call graph has various advantages over traditional techniques. It takes various parameters for consideration such as information of nodes, basic structure of graphs and call frequency. Here the detailed study of call graph reduction in graph mining made the study of various other techniques in bug localization very easy. The proposed algorithm works only when there are same types of nodes at a particular level in a call graph. In future this work can be extended to multiple levels of call graph will make the graph mining algorithm efficiently. Secondly the storage of graph can be upgraded with any new storage technique where it would require lesser storage space as well as lesser access time leading to further optimize reduction of call graph.

REFERENCES RÉFÉRENCES REFERENCIAS

- Zhou, L., Wu, D., Chen, J., & Dong, Z. (2018). Greening the smart cities: Energy-efficient massive content delivery via D2D communications. *IEEE Transactions on Industrial Informatics*, 14(4), 1626-1634.
- Lin, C. C., Deng, D. J., Kuo, C. C., & Liang, Y. L. (2018). Optimal charging control of energy storage and electric vehicle of an individual in the internet of energy with energy trading. *IEEE Transactions on Industrial Informatics*, 14(6), 2570-2578.
- Darivianakis, G., Eichler, A., Smith, R. S., & Lygeros, J. (2017). A Data-Driven Stochastic Optimization Approach to the Seasonal Storage Energy Management. *IEEE control systems letters*, 1(2), 394-399.
- Lee, C. C., Chen, C. T., Wu, P. H., & Chen, T. Y. (2013). Three-factor control protocol based on elliptic curve cryptosystem for universal serial bus mass storage devices. *IET Computers & Digital Techniques*, 7(1), 48-56.
- Tang, Z., Liu, A., & Huang, C. (2016). Social-Aware Data Collection Scheme Through Opportunistic Communication in Vehicular Mobile Networks. *IEEE Access*, 4, 6480-6502.
- Colmenar-Santos, A., Luis-Molina, E., Rosales-Asensio, E., & Lopez-Rey, Á. (2018). Technical approach for the inclusion of superconducting magnetic energy storage in a smart city. *Energy*.
- Cebe, M., & Akkaya, K. (2018). Efficient Certificate Revocation Management Schemes for IoT-based Advanced Metering Infrastructures in Smart Cities. *Ad Hoc Networks*.
- Han, J., Li, Y., & Chen, W. (2018). A Lightweight And privacy-preserving public cloud auditing scheme without bilinear pairings in smart cities. *Computer Standards & Interfaces*.
- Kumar, H., Singh, M. K., Gupta, M. P., & Madaan, J. (2018). Moving towards smart cities: Solutions that lead to the Smart City Transformation Framework. *Technological Forecasting and Social Change*.
- Osman, A. M. S. (2019). A novel big data analytics framework for smart cities. *Future Generation Computer Systems*, 91, 620-633.
- Wang, Y. F., & Ding, D. W. (2015, April). Topology characters of the linux call graph. In *2015 2nd International Conference on Information Science and Control Engineering (ICISCE)* (pp. 517-518). IEEE.
- Blokhin, K., Saxe, J., & Mentis, D. (2013, July). Malware similarity identification using call graph based system call subsequence features. In *2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops* (pp. 6-10). IEEE.
- Kato, T., Hayashi, S., & Saeki, M. (2012, October). Cutting a method call graph for supporting feature location. In *2012 Fourth International Workshop on Empirical Software Engineering in Practice* (pp. 55-57). IEEE.
- Agrawal, G. (1999). Simultaneous demand-driven data-flow and call graph analysis. In *Software Maintenance, 1999.(ICSM'99) Proceedings. IEEE International Conference on*(pp. 453-462). IEEE.
- Yousefi, A., & Wasssyng, A. (2013, March). A call graph mining and matching based defect localization technique. In *2013 IEEE Sixth International Conference on Software Testing, Verification and Validation Workshops* (pp. 86-95). IEEE.
- Xue, J., Hu, C., Wang, K., Ma, R., & Leng, B. (2009, December). Constructing a Knowledge Base for Software Security Detection Based on Similar Call Graph. In *Computer and Electrical Engineering, 2009. ICCEE'09. Second International Conference on* (Vol. 1, pp. 593-597). IEEE.
- Chroni, M., & Nikolopoulos, S. D. (2012, July). An embedding graph-based model for software

- watermarking. In *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2012 Eighth International Conference on* (pp. 261-264). IEEE.
18. Wang, L., Gong, J., & Shi, L. (2015, November). OLAP Visual Analytics on Large Software Call Graphs with Hierarchical ChordMap. In *Data Mining Workshop (ICDMW), 2015 IEEE International Conference on* (pp. 675-679). IEEE.
 19. Gurukar, S., & Ravindran, B. (2014, January). Temporal analysis of telecom call graphs. In *Communication Systems and Networks (COMSNETS), 2014 Sixth International Conference on* (pp. 1-6). IEEE.





This page is intentionally left blank



GLOBAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY: B
CLOUD AND DISTRIBUTED

Volume 22 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 |

Artificial Intelligence Approach to Cyber Security

By Murtala Mohammad & Ibrahim Goni

Adamawa State University

Abstract- Cyber security is a major concern of developed and developing countries due to the high rate of attack and threat to the cyber space. The aim of this research work was to develop a fuzzy logic system for cyber security. Four inputs were used and three outputs was produced with their associated linguistic variables, Triangular angular membership function was used to implement the system. Fuzzy controller has an advantage of performing according to linguistic rules in the manner of how a human behaves. The reasoning method in the fuzzy controller is also similar to that of the cyber expert handle.

GJCST- B Classification: 1.2



Strictly as per the compliance and regulations of:



Artificial Intelligence Approach to Cyber Security

Murtala Mohammad ^α & Ibrahim Goni ^σ

Abstract- Cyber security is a major concern of developed and developing countries due to the high rate of attack and threat to the cyber space. The aim of this research work was to develop a fuzzy logic system for cyber security. Four inputs were used and three outputs was produced with their associated linguistic variables, Triangular angular membership function was used to implement the system. Fuzzy controller has an advantage of performing according to linguistic rules in the manner of how a human behaves. The reasoning method in the fuzzy controller is also similar to that of the cyber expert handle.

I. INTRODUCTION

The advancement in cloud computing, mobile computing, mechatronics, net centric computing, wireless sensor network, nanotechnology and internet of things has led to the conjunction in the cyber space and even leading to the creation of fog computing. Moreover, this cyberspace is a platform where business security system, financial systems, education system, industries, power plants among others. The combination of this technology and systems has improved the functionalities of cyber space and leading to vulnerability to the cyber-attack [1]. In the recent time a lot of framework and systems are published based on the application of artificial intelligence techniques to cyber security and digital forensics. The research of [2] applied deep learning technique to design a framework for cyber forensics. [3]

Uses data mining techniques in anti-cybercrime. In [4] deep learning neural network and fuzzy logic was used for abnormal traffic control in a network using CICIDS 2017 data sets. In [5] applied deep learning techniques in DOS attack and [6] applied fuzzy logic technique to protect car for cyber-attack. [7] Combined Neuro-fuzzy and genetic algorithm to implement intrusion detection system.

II. METHOD

The data used for this work have been extracted from a series of questionnaires collected from cyber experts and system administrators. The obtained data are related especially with the headlines given below; Denial of Service (Dos) attacks, virus, malware, logic bomb, social engineering and Trojan horse and Out of service, seizing web page, attacks for protesting, seize critical systems, capture confidential information and take system control. This study evaluates cyber terrorists who might attack communications systems, financial centers, power plants, emergency services, transportation, water supply, oil and natural gas distribution stations. People capable of cyber terrorism such as dedicated special staff, hackers, cyber activists and opponents of the state are evaluated in the proposed cyber security system.

III. SYSTEM ARCHITECTURE

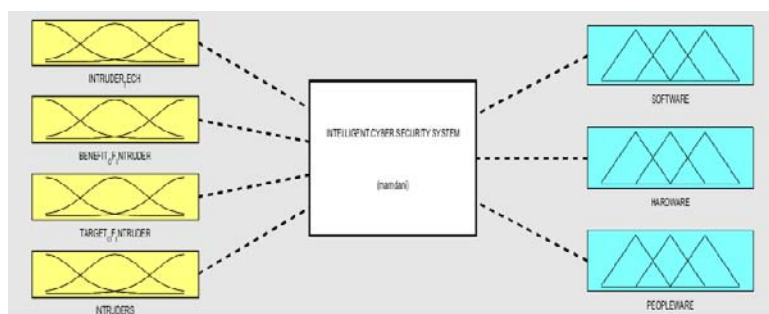


Figure 1: System Architecture

a) Inputs and Outputs Analysis

The fuzzification and defuzzification of inputs and outputs in this experiment was implemented using triangular membership function as shown in the figure below;

b) Intruder's Techniques

The major technique used by the intruders are the one that would favor him after studying the weaknesses of the system based on this we have identified the techniques they might use in table 1. Below;

Author ^α ^σ: Department of Computer Science, Adamawa State University, Mubi. e-mail: algonis1414@gmail.com

Table 1: Intruder Techniques and their Abbreviation

S/N	Intruder's Technique	Abbreviation
1.	Network attack	NA
2.	Denial of service	DoS
3.	Virus	V
4.	E-mail Virus	EV
5.	Logic Bomb	LB
6.	Trojan horse	TH
7.	Social engineering	SE
8.	Malware	M

The above table 1 was used to plot a membership function for intruder's

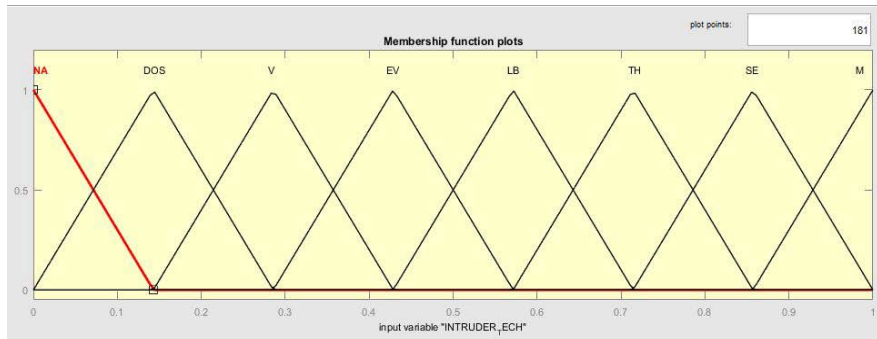


Figure 2: Intruder Techniques Membership

c) Benefit of Intruders

A cyber intruder normally has the reason his attack the table 2. Below summarize the possible benefit of the intruder.

Table 3: Benefit of Intruders and its Abbreviation

S/N	Benefit of intruders	Abbreviation
1.	Out of service	OOS
2.	Seizing web page	SWP
3.	Protesting	P
4.	Control of critical system	CCS
5.	Capture confidential info.	CCI
6.	Control system	CS

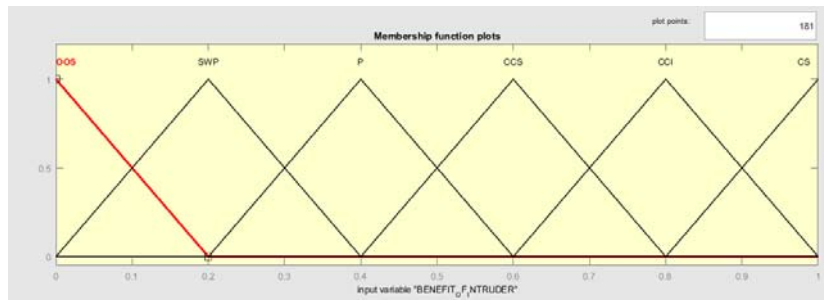


Figure 3: Benefit of Intruders

d) Target of Intruders

Target is a critical term for a cyber-intruder. According to target, a cyber-intruder may use one or more different cyber techniques. A cyber intruder's target may be as in Table 4.



Table 4: Target of Intruder's

S/N	Target of intruders	Abbreviation
1.	Communication system	CS
2.	Financial center	FC
3.	Power plant	PP
4.	Emergency source	ES
5.	Public transportation	PT
6.	Public institution	PI
7.	Water works	WW
8.	oil and natural gas distribution	ONGD

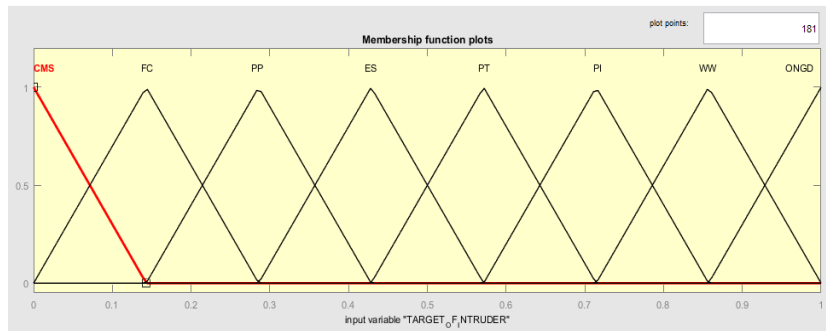


Figure 4: Target of Intruders Membership

e) Intruders

Intruders are person or group of persons responsible for the unauthorized access to the system. They are summarized in the table 5 below;

Table 5: Intruders and its Abbreviation

S/N	Intruders	Abbreviation
1.	Special staff	SPS
2.	Computer Hacker	CH
3.	Enemy of the system	EOS
4.	Cyber activist	CA

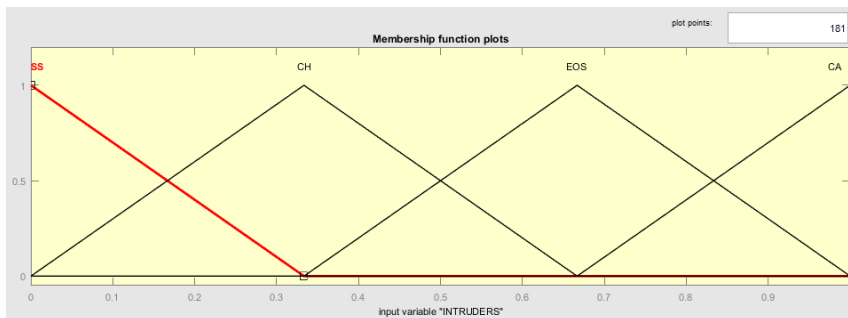


Figure 5: Intruders Membership

f) Hardware

In some situations network administrators has a software device to prevent attack as summarized in the table 6 below;

Table 6: Hardware and its Abbreviation

S/N	Hardware	Abbreviation
1.	Physical control	PC
2.	Special control	SC
3.	Technical control	TC

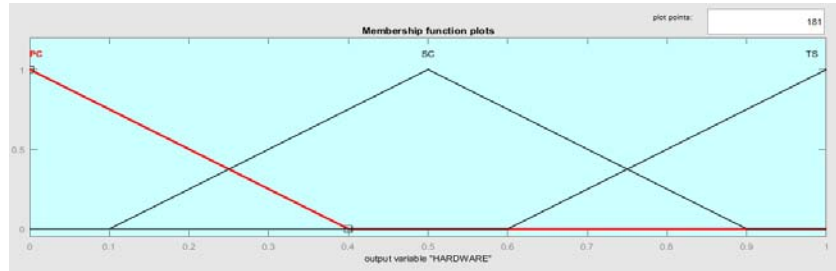


Figure 6: Hardware Membership

i. Software

Sometime it is possible to use software to combat intruders as summarized in the table 7 below;

Table 7: Software and its Abbreviation

S/N	Software	Abbreviation
1.	Special software	SPS
2.	System update	SU
3.	National data bank	NDB

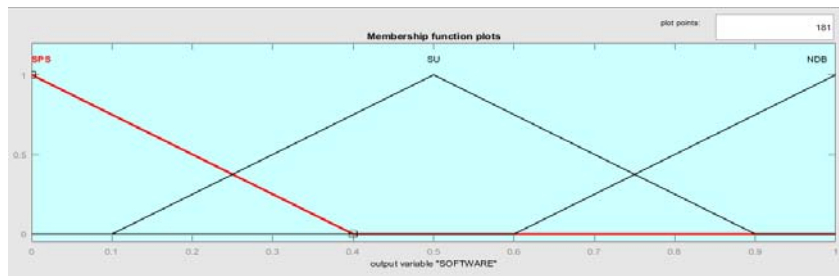


Figure 7: Software Membership

ii. People ware

Users can play a vital role in combating cyber-attack if they have technical knowhow of attacks as it summarized in the table 8 below

Table 8: People Ware and its Abbreviation

S/N	People ware	Abbreviation
1.	User training	UT
2.	Awareness	A
3.	User control	UC

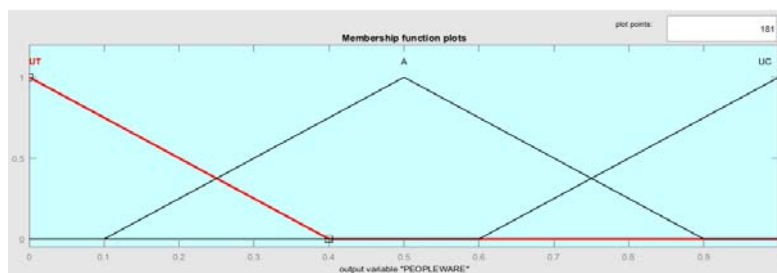


Figure 8: Peopleware Membership



IV. RESULT

The input variable Intruder techniques (IT) is not a fixed value they are fuzzy variables as network attack, virus, Trojan horse, malware etc. Similarly for input variable benefit of intruders (BI) has the fuzzy variables out of service, protesting, control system etc. and output variable People ware has the fuzzy variables user

training, awareness and user control. Depending on the inputs the outputs take different fuzzy variables value. It can be seen that Intruder techniques (IT) criteria is in x axis, benefit of intruders (BI) criteria is in y axis, and solution criteria People ware (P) is in z axis as shown in Figure 1.

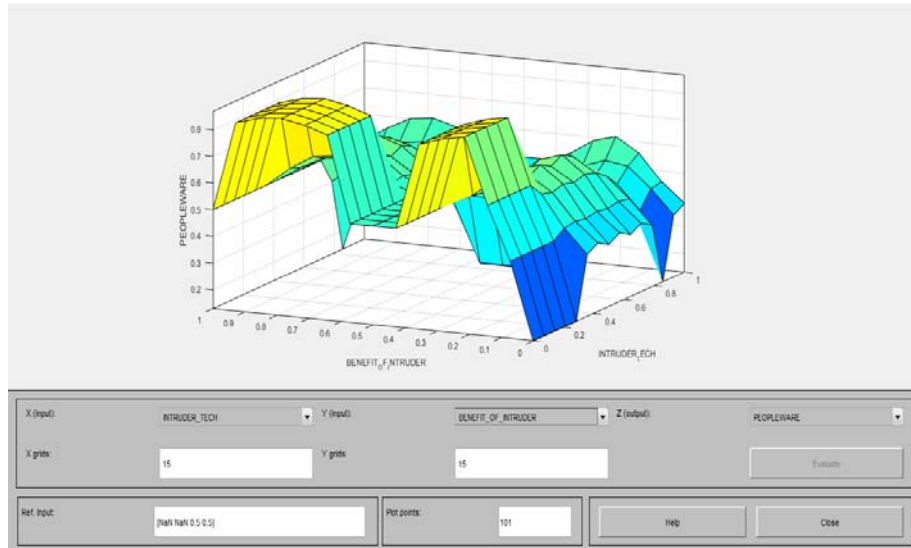


Figure 10: Input variables Intruder Techniques (IT), Benefit of Intruders (BI) vs. output variable Peopleware (P)

As shown in Figure 11. Intruder techniques (IT) criteria is in x axis, benefit of intruders (BI) criteria is in y axis, and solution criteria software (S) is in z axis.

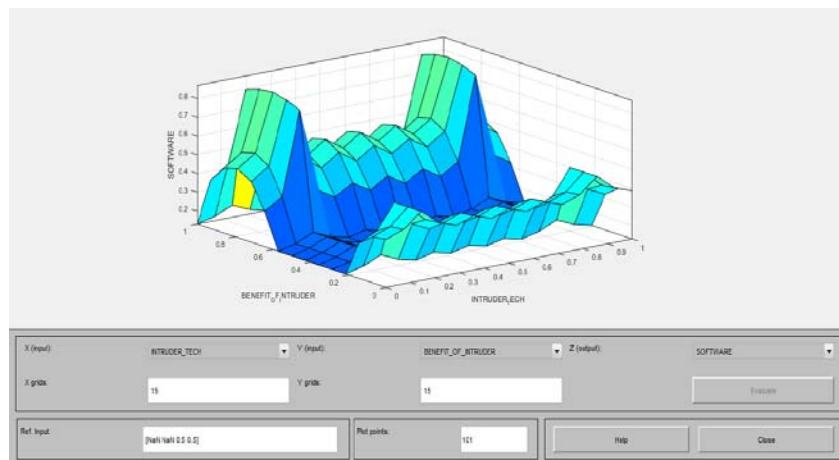


Figure 11: Input variables Intruder Techniques (IT), Benefit of Intruders (BI) vs. output variable Software (S).

Benefit of Intruders (BI) vs. output variable Software (S).

As shown in Figure 12 Benefit of intruders (BI) criteria is in x axis, and Target of Intruders (TI) criteria is in y axis, and solution criteria hardware (H) is in z axis.

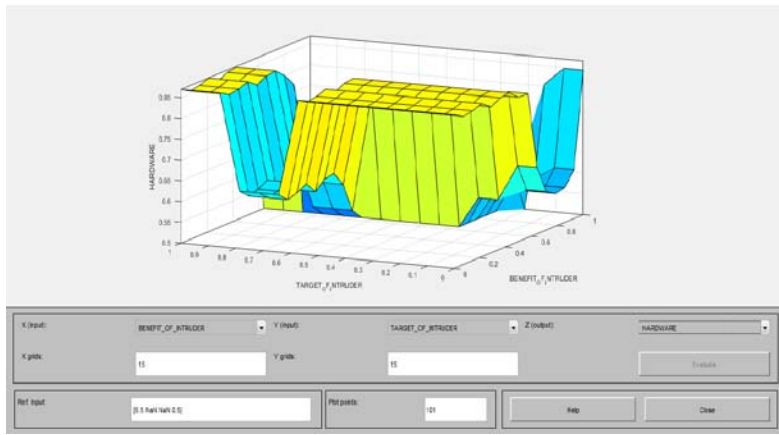


Figure 12: Benefit of intruders (BI) criteria is in x axis, and Target of Intruders (TI) criteria is in y axis, and solution criteria hardware (H) is in z axis

As shown Figure 13 benefits of intruders (BI) criteria is in x axis, and Target of Intruder (TI) criteria is in y axis, and solution criteria People ware (P) is in z axis.

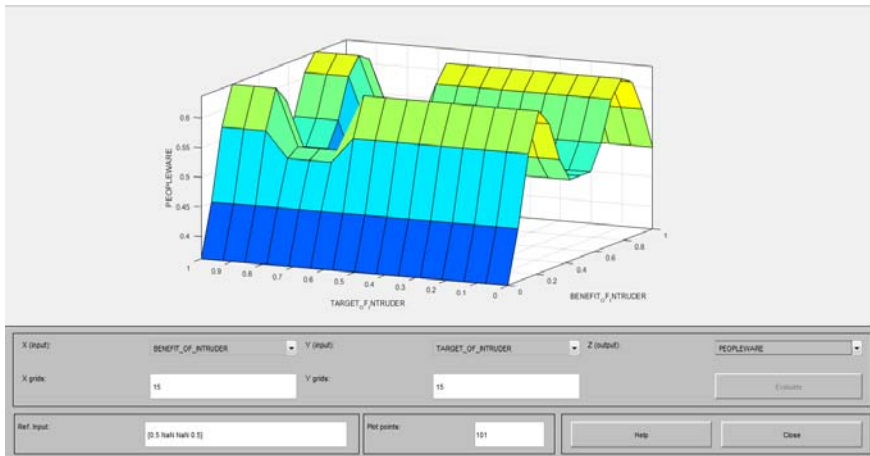


Figure 13: Input variables Benefit of Intruders (BI), Target of Intruder (TI), vs. output variable Peopleware (P)

As shown Figure 14 Intruders (I) criteria is in x axis, and Intruder techniques (IT) criteria is in y axis, and solution criteria Peopleware (P) is in z axis.

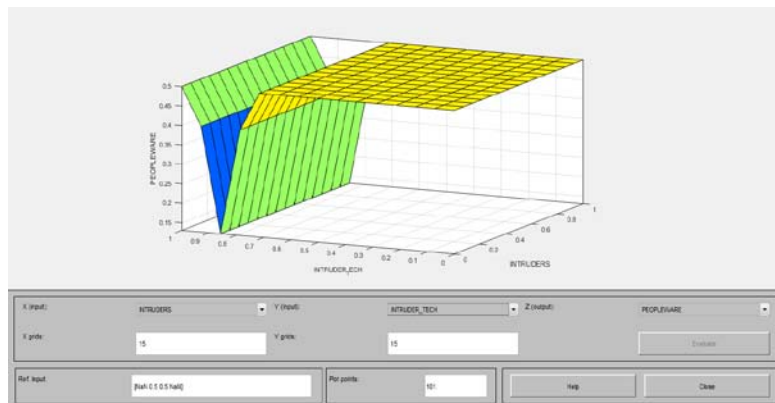


Figure 14: Input variables Intruders (I), Intruder Techniques (IT) vs. output variable Peopleware

As shown Figure 15 Target of Intruders (TI) criteria is in x axis and benefit of Intruder (BI) criteria is in y axis and solution criteria Software (S) is in z axis.

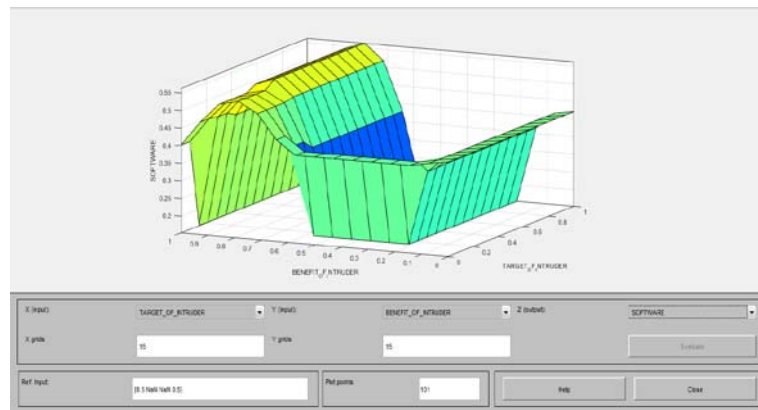


Figure 15: Input variables Target of Intruders (I), Benefit of Intruder (BI) vs. output variable Software (S)

In Figure 16 of fuzzy rule viewer for Intelligent cyber security system is shown using MATLAB. According to the proposed model, a sample solution is given in Figure 16 when IT=0.135; BI=0.32; TI=0.187; I=0.57. Here, model outputs are S=0.192; H=0.869

and P=0.839. Output of S=0.192 means that system Software Update (SU); H=0.571 means that system needs Technical support (TS); P=0.839 means that user needs user control (UC) is important.

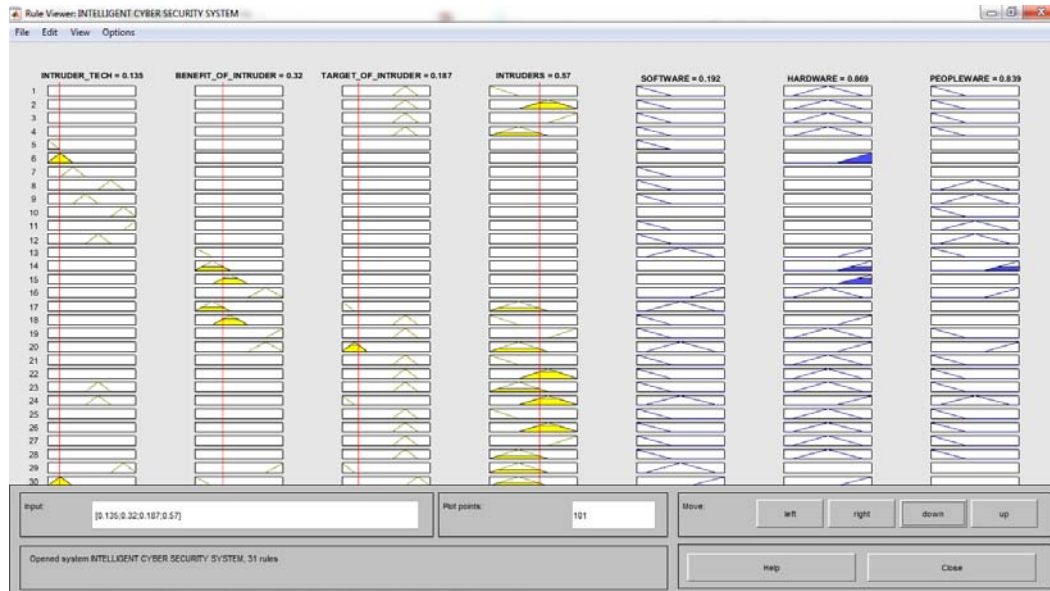


Figure 16: Fuzzy Rule viewer for intelligent cyber security system

V. CONCLUSION

Fuzzy controller has an advantage of performing according to linguistic rules in the manner of how a human behaves. The reasoning method in the fuzzy controller is also similar to that of the cyber expert handle. After an intelligent cyber security system was carefully designed, we test the system and discuss the impact of the input variables on the output variables as shown on the rules viewers and the surface viewers.

REFERENCES RÉFÉRENCES REFERENCIAS

1. Thanh T. N. and Vijay J.R. (2019) Deep Reinforcement learning for cyber security [CsCR] arxiv: 1906.05799 vol. I
2. Nickson M.K., Victor R.K. and Venter H.S. (2019) Diverging deep learning cognitive computing techniques into cyber forensics. Forensics science international library. Science Direct Vol. 1, 61-67.
3. Khan M. A., S.K., Pradham H., and Fatima M. (2017) Applying data mining techniques in cybercrimes: in anti-cybercrime (ICACC) 2017 2nd International conference on IEEE pp. 213-216.
4. Amosov O.S., Ivanov Y.S. and Amosova G. (2019) Recognition of abnormal traffic using deep learning neural network and fuzzy logic IEEE 2019 international multi-conference on industrial engineering and modern technologies

5. Yuan X. and Li X. (2017) deep defense Identify DDOS attack via deep learning IEEE international conference on smart computing 29-31, may, 2017
6. Fabio M., Fransesco M., Victoria N. and Antonella S. (2017) Car hacking identification through fuzzy logic algorithm IEEE 2017.
7. Goni & Ahmed L. Propose Neuro-Fuzzy-Genetic Intrusion Detection System. International Journal of Computer Applications 115(8): 1-5 (2015)





A Network Science-based Approach for an Optimal Microservice Governance

By Gihan S. Siriwardhana, Nishitha De Silva, Liyanage Sanjaya Jayasinghe,
Lakshitha Vithanage & Dharshana Kasthurirathna

Sri Lanka Institute of Information Technology

Abstract- With the introduction of microservice architecture for the development of software applications, a new breed of tools, platforms, and development technologies emerged that enabled developers and system administrators to monitor, orchestrate and deploy their containerized microservice applications more effectively and efficiently. Among these vast arrays of technologies, Kubernetes has become one such prominent technology widely popular due to its ability to deploy and orchestrate containerized microservices. Nevertheless, a common issue faced in such orchestration technologies is the employment of vast arrays of disjoint monitoring solutions that fail to portray a holistic perspective on the state of microservice deployments, which in turn, inhibit the creation of more optimized deployment policies. In response to this issue, this publication proposes the use of a network science-based approach to the creation of a microservice governance model that incorporates the use of dependency analysis, load prediction, centrality analysis, and resilience evaluation to effectively construct a more holistic perspective on a given microservice deployment.

Keywords: *auto-scaling, chaos engineering, kubernetes, machine learning, microservices, NSGA- II, time series.*

GJCST- B Classification: C.2.0



Strictly as per the compliance and regulations of:



A Network Science-based Approach for an Optimal Microservice Governance

Gihan S. Siriwardhana^α, Nishitha De Silva^σ, Liyanage Sanjaya Jayasinghe^ρ, Lakshitha Vithanage^ω
& Dharshana Kasthurirathna[¥]

Abstract- With the introduction of microservice architecture for the development of software applications, a new breed of tools, platforms, and development technologies emerged that enabled developers and system administrators to monitor, orchestrate and deploy their containerized microservice applications more effectively and efficiently. Among these vast arrays of technologies, Kubernetes has become one such prominent technology widely popular due to its ability to deploy and orchestrate containerized microservices. Nevertheless, a common issue faced in such orchestration technologies is the employment of vast arrays of disjoint monitoring solutions that fail to portray a holistic perspective on the state of microservice deployments, which in turn, inhibit the creation of more optimized deployment policies. In response to this issue, this publication proposes the use of a network science-based approach to the creation of a microservice governance model that incorporates the use of dependency analysis, load prediction, centrality analysis, and resilience evaluation to effectively construct a more holistic perspective on a given microservice deployment. Furthermore, through analysis of the factors mentioned above, the research conducted, then proceeds to create an optimized deployment strategy for the deployment with the aid of a developed optimization algorithm. Analysis of results revealed the developed governance model aided through the utilization of the developed optimization algorithm proposed in this publication, proved to be quite effective in the generation of optimized microservice deployment policies.

Keywords: *auto-scaling, chaos engineering, kubernetes, machine learning, microservices, NSGA-II, time series.*

I. INTRODUCTION

The term “microservices” was first introduced in 2011 [1] and was considered as a specialized implementation of Service-Oriented Architecture (SOA), coined to denote the common architectural approach of decomposing applications into smaller self-contained, loosely coupled services. The microservice architectural style was later widely adopted in place of the traditional monolithic architecture by many leading companies such as Amazon, Netflix, LinkedIn, and SoundCloud due to the capability to develop loosely coupled services possessing the ability to be independently deployed, versioned, and scaled while

ensuring in benefits such as faster delivery, more excellent performance, and greater autonomy [1].

The shift in architectural style from the traditional monolithic architecture to microservice architecture also brought forth the creation of a set of new methodologies and approaches that established the policies, standards, and best practices for the adoption of microservices, designed for the agile IT environment, known as “Microservices Governance” [2]. This approach to governance was entirely dissimilar to the traditional governance policies followed in monolithic applications primarily since governance in microservices followed a decentralized approach, whereas governance in monoliths followed a centralized approach where decisions were made “top-down” [2]. Although the decentralized approach of governance of microservice provided advantages such as the freedom to develop applications utilizing diverse technology stacks, a downside of this approach was that more steps should be taken to ensure effective governance is maintained, since typical applications required interconnections between a vast number of microservices where business process workflows were continuously introduced. Consequently, organizations required the service of a variety of tools, ranging from monitoring and autoscaling to others such as configuration management, service discovery, and fault tolerance, that facilitated the multitude of tasks required to ensure effective microservice governance was in effect.

In addition to the tools mentioned above, new deployment strategies that facilitated the newly developing microservice infrastructure were introduced. Amongst them, containerization of microservices became one of the most effective ways to deploy microservice applications due to its ability to efficiently package microservices by encompassing all the required libraries and dependencies needed during runtime. This procedure separated the application from the underlying infrastructure and enabled developers to run the application in an isolated environment, ensuring performance and functionality. As a result, propelled by services such as Docker, containerization became the preferred approach for effectively deploying microservices, in contrast to the traditional virtualization-based approach previously adopted. However, in the case when the number of microservices of a particular application increased, it

Author ^α ^σ ^ρ ^ω [¥]: Department of Software Engineering, Sri Lanka Institute of Information Technology, Malabe, Sri Lanka.
emails: it17016230@my.sliit.lk, it17006880@my.sliit.lk, it17012966@my.sliit.lk, it17410250@my.sliit.lk, dharshana.k@sliit.lk

became increasingly difficult to coordinate, schedule, monitor, and maintain the required containerized microservices, especially in times where utmost application performance was required. In response to this issue, the Kubernetes framework was introduced in 2014 [3] to allow organizations to run distributed systems more resiliently by providing effective solutions for load balancing, storage, orchestration, automated rollouts, and self-healing mechanisms [4]. The unique characteristics offered by Kubernetes in this regard, thereby transformed it into one of the most prominent microservice-based technologies available for organizations to deploy their vast arrays of microservice applications in production-grade environments.

The introduction of Kubernetes ushered in a new era of microservice governance through the introduction of container orchestration. Nevertheless, as evident throughout this publication, despite its immense use in orchestrating microservice applications, Kubernetes is still not able to provide a perfect governance solution to most modern microservice applications, as there are still prevalent issues that need to be addressed in Kubernetes particularly concerning the policies followed in the deployment of interdependent microservices.

A primary reason for the existence of inefficient optimization policies in Kubernetes based microservice deployments is the lack of the tools and services to obtain a holistic view of Kubernetes deployments and thereby optimize cluster performance. The current tools and services offered by Kubernetes often have to be pre-configured to the existing pre-conceived knowledge of the developers in contrast to the actual real-time utilization. Although implementing such solutions may be of use in the short term, it maybe it may be difficult to further improve upon the performance of the microservice cluster in the long term due to the lack of a holistic perspective on the interaction of the interdependent microservices in real-time use. Hence, it should be realized that if a particular microservice deployment is to be optimized for performance, a clear understanding regarding the relationships among the interdependent microservices during runtime is required. However, if a microservice deployment is to be truly optimized for optimal performance, it may also be necessary to take into account factors such as the resilience among the interdependent microservices, the effect of autoscaling policies, in addition to a clear understanding on the interactions of interdependent microservices. Regardless, even though there are several monitoring solutions available for such purposes, such as Prometheus, Istio, and Chaos Toolkit, their disjoint nature prevents them from allowing users to obtain a holistic perspective on the state of their deployed microservices. Furthermore, in cases such as fault management, error handling, and performance monitoring, due to the disjoint nature of these monitoring solutions, users are often unable to gain insight into possible solutions as to why a particular

problem or bottleneck has occurred even though they are often made aware of the presence of a particular problem by these monitoring solutions.

In addition to the above-mentioned issues, these monitoring solutions are also often and plagued with other challenges such as the difficulty in successfully configuring and integrating these monitoring tools with the existing tools used by organizations [5]. The issues mentioned above may also further complicate the already complicated management and configuration process prevalent in Kubernetes and, in turn, may confuse inexperienced developers and system administrators, ultimately leading towards misallocation of cluster resources and degradation of cluster performance.

In response to the issues stated above, this publication proposes a novel approach to the creation of a unified governance model that can be used by developers and system administrators to effectively oversee the performance of their microservice deployments factoring in dependency analysis, load prediction, centrality analysis, and residency evaluation in order to determine the optimal placement of microservices and thereby create an optimized deployment plan for a given microservice deployment. Thus, through the application of the proposed governance model, users would be able to obtain a more holistic view of their deployment, resulting in a greater understanding of the runtime behavior of the deployed microservices, thereby enabling greater optimization possibilities. Through application of the approach proposed in this publication, the authors wish to provide key insight to the contribution of a new set of microservice deployment optimization methodologies, which factor in the impact of key factors such as dependency among deployed microservices, autoscaling policies as well as resilience measures in microservice deployments.

The governance model proposed in this publication is comprised of four main components, each aimed at capturing a particular dimension of the microservice deployment with the ultimate goal of achieving a more holistic view of a given microservice deployment. Accordingly, the key components of the proposed model are as follows.

1. A generated microservice co-dependency map which is aimed at obtaining a clear perspective about the dependencies between each microservice and the importance of the deployment plan.
2. A load prediction and centrality analysis component for the prediction of the level of interdependency among co-dependent microservices, the resource utilization of pods in the cluster as well as performing the task of the calculation of centrality measures of microservices in the co-dependency network.
3. A resilience evaluation component to evaluate the resilience of microservices in the cluster.

- An optimal placement algorithm to determine the optimum placement of microservices in the Kubernetes cluster based on the above-stated measures.

The remainder of this publication is organized as follows. Section II discusses the background and the related work literature referenced in the development of this optimization model. Section III discusses the methodology followed in the development of the proposed model along with an overview of its key components. Section IV discusses the results obtained through the application of the developed model and, finally, the conclusion of this publication, along with directions for future work, is outlined in Section V.

II. BACKGROUND AND LITERATURE

The apparent need for improved microservice governance modeling strategies, along with some of the prevalent issues in current microservice governance methodologies, have been highlighted in several publications throughout the years. The authors of [6] highlight the need for new modeling strategies that capture the recent advances in deployment technology such as Kubernetes. The publication [7] states the inability of monitoring frameworks to measure microservice performance level metrics would lead to the creation of several new research topics, which include the development of holistic techniques for collecting and integrating monitoring data from microservices and datacenter resources. In contrast, publications such as [1] highlight the use of past actions and events to better inform resource management decisions in microservice environments along with the challenges such as the overloading of monitoring events faced in resource monitoring and management processes.

In addition, several publications have also proposed performance modeling strategies for Kubernetes deployments. In this regard, [8] proposes an architectural approach that federates Kubernetes clusters using a TOSCA-based cloud orchestration tool. In contrast, research publications such as [9] proposed a tool named Terminus to solve the problem of finding the best-suited resources for the microservice to be deployed so that the whole application achieves the best performance while minimizing the resource consumption. Other researches include the reference net-based model for pod & container lifecycle in Kubernetes proposed by the authors of [10] and the generative platform for benchmarking performance and resilience engineering approaches in microservice architectures as proposed in [11].

The approaches suggested in the publications stated above are all approaches that aim at performance optimization of Kubernetes deployments. However, a key aspect to note in this regard is the fact that the methodologies stated in the publications mentioned

above, fail to capture critical dimensions such as the dependent relationships between microservices, the effect of autoscaling policies, as well as resilience measures in the determination of the optimal placement of a particular microservice with regard to its global significance. Therefore, to our knowledge, there is no current solution proposed, that takes into consideration an integrated modeling strategy, factoring key elements essential to the optimization of microservice deployments such as co-dependencies present as well resilience and centrality measures among microservices when developing a holistic governance policy for Kubernetes based microservice deployments, as proposed in this research.

III. METHODOLOGY

The proposed governance model consists of four principal components each interlinked as depicted in Fig.1 below. The following sub-sections provide an in-depth analysis regarding the methodology followed in the development of the proposed governance model along with an overview of the respective functionalities of its components.

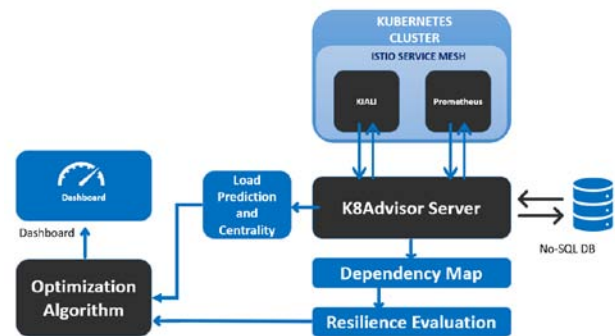


Fig. 1: High-level diagram of the proposed governance model

a) Microservice Co-dependency Network

The microservice co-dependency network consists of three sub-components which can be listed as follows.

- An Istio service mesh platform that incorporates Kiali and Prometheus monitoring solutions.
- A backend NodeJS "K8Advisor" server for integration with metric APIs provided by monitoring solutions.
- A database solution for the storage of gathered metric data.

The Istio service mesh provides the core metric servers such as Kiali and Prometheus, configured to retrieve data from the app, pod, and node levels in the cluster. In this regard, the microservice dependency map utilizes quantified measurements derived from request and response times obtained primarily from the Kiali metric server to facilitate the development of the microservice co-dependency map.

The K8Advisor server aggregates all APIs exposed from the Istio service mesh and exposes a single endpoint such that required metrics could be queried more effectively. The server is configured to query metrics and trigger required processes as per a configured scheduler. The metrics collected in this regard, are then stored in the No-SQL database along with additional information such as timestamps to facilitate the creation of time series datasets utilized in the training of machine learning models. The K8Advisor server is also capable of generating CSV (Comma Separated Values) files on demand by reading the No-SQL database. The server will also expose an endpoint that can be accessed via an HTTP request in order to trigger required functions on demand. All the data stored in the database is maintained within the same Kubernetes cluster without exposing it to the public in order to maintain the privacy of user data. Lastly, in addition to the above, the K8Advisor server is also responsible for the creation of a node latency map through the evaluation of latency measures between the nodes in the cluster. Here, the Round-Trip Time (RTT) of network calls between nodes in the cluster is evaluated and, through the use of a developed shell script, the average latency measures between cluster nodes are obtained and forwarded to the optimization algorithm.

b) Load prediction and Centrality Analysis

The key objective of the load prediction component and centrality analysis component is the utilization of historical data and centrality measures to aid in the optimization of microservice deployments and the creation of holistic autoscaling policies. In this regard, the component performs the following key tasks.

- Prediction of future resource utilization values (primarily CPU and memory) based on historical pod resource utilization data.
- Prediction of inter-microservice link weight (dependency measures), based on historical link weight data derived from the load-based metrics in the co-dependency network.
- Calculation of centrality measures of microservices in the co-dependency network.

The resource utilization prediction process is performed through performing a time series-based prediction on pod utilization metrics, in which predicted CPU and memory utilization values for a particular period are forecasted. The prediction process for resource utilization is performed through the application of a Long Short-Term Memory (LSTM) network in which a particular number of time steps of utilization metrics are used to predict future utilization values. Once predictions are made, the predicted utilization values for a particular period (e.g. - 24 hours in advance) are passed through to the optimization algorithm to infer optimal autoscaling decisions.

The process of inter-microservice link weight prediction is primarily a network-based time-series

prediction process in which the inter microservice link weights derived through load-based metrics are forecasted such that the next predicted weights for the links in the co-dependency map are determined. The forecasted weights determined through the use of an LSTM prediction model could then be used to provide an accurate estimation of the load that is expected to be received by microservices in the cluster, enabling the identification of key potential microservices which may in turn, highly manipulate microservice placement decisions and the realization of optimal cluster performance

The calculation of microservice centrality measures is also performed within the load prediction component. Here, the microservices in the co-dependency network are evaluated on several centrality measures to facilitate the identification of influential microservices in the cluster. These calculated centrality measures are then forwarded to the optimization algorithm as inputs, to infer autoscaling decision through determination of required service instance levels. In this regard, the proposed governance model is expected to make use of the key centrality measures such as degree, betweenness, closeness as well as eigenvector centrality measures to facilitate the identification process of influential microservices.

c) Resilience Evaluation

The resilience evaluation component is particularly based on chaos engineering principles and utilizes the dependency measures derived from the co-dependency network to effectively target the most prominent services in the cluster for the evaluation of resilience measures. This process is performed through the use of Chaos Toolkit and the resulting resilience measures thus obtained, are then utilized to derive a holistic perspective on the resilience and health of interdependent services in the cluster.

d) Optimization Algorithm

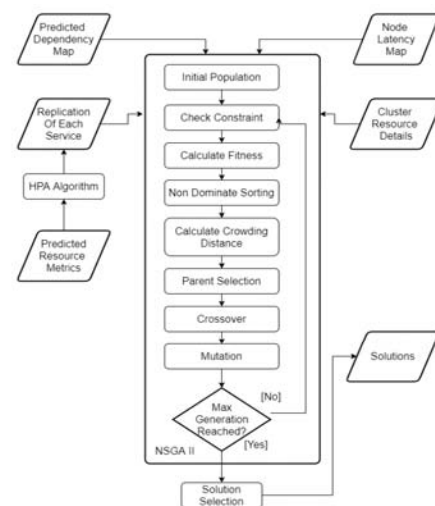


Fig. 2: Overview of the optimization algorithm

The optimization algorithm utilized in the proposed governance model is predominantly based on the NSGA-II (Non-Dominant Sorting Genetic Algorithm) algorithm. The algorithm generates a multitude of optimized solutions that enables the user to infer optimization decisions predicated on three key optimization categories, which are as follows.

- Solutions optimized for best performance and availability, thereby maintaining a balance between reduced latency and number of instances.
- Solutions optimized for optimal performance based on the reduction of latency.
- Solutions optimized for highest availability based on the maximization of the number of instances.

These optimized solutions are generated following four main input parameters utilized by the optimization algorithm as depicted in Fig. 2 above and can be listed as follows.

1. Predicted microservice dependency measures from the load prediction and centrality analysis component.
2. Node latency map generated from the Node Server.
3. Required number of microservice instances derived from centrality measures and predicted resource utilization metrics from the load prediction and centrality analysis component.
4. General cluster infrastructure information gathered from monitoring solutions.

The sub-sections below provide an in-depth insight into the manner these input parameters are utilized in the developed algorithm as well as their impact on the creation of holistic optimization policies.

i. *Predicted Microservice Dependency Measures*

In microservice deployments, although factors such as latency cannot be completely eliminated, dependent microservices can be deployed in nearby nodes or the same node in order to reduce the overall latency of an application. Therefore, making use of this approach while intending to solve low availability and sub-optimal performance issues, as well as to aid in the creation of autoscaling policies, the developed optimization algorithm makes use of the predicted load-based link weights obtained from the load prediction component. This is done such that optimal placement and scaling decisions could be performed ahead of time, establishing a future deployment strategy such that users such as DevOps engineers would be able to make use of the gathered information to create an optimized microservice deployment plan. In addition, making use of the predicted dependency measures (load-based link weight), optimal placement decisions are determined through the application of (1) and (2), as defined below, which calculates the average latency among the microservice instances, based on the dependency measures and as the node latency map obtained from the Node sever.

Table 1: Average Latency Calculation

N	Number of dependencies in pod-level
M	Number of dependency links in app-level
W	Dependency request weight in app-level
L	The latency of dependency in pod-level
D	Dependency average latency in app-level
TL	Total latency

$$D_j = \frac{\sum_{i=1}^{j=m} L_i}{n} \tag{1}$$

$$\text{Minimize TL} = \sum_{j=1}^{j=m} W_j \times D_j \tag{2}$$

ii. *Node Latency Measures*

The main objective of the optimization algorithm is the maximization of performance through the minimization of latency among microservices. Therefore, the developed optimization algorithm also utilizes a developed node latency map obtained from the Node Server, to evaluate the fitness of generated solutions.

iii. *Required Microservice Instances*

In the process of fitness calculation, the first step is the calculation of the required number of instances per microservices. Here, the calculation of the required number of microservices instances is performed by utilizing the predicted resource utilization values derived from the load prediction component, applied on the Horizontal Pod Autoscaling algorithm. Also, the centrality measures derived from the co-dependency network will be utilized to infer the optimum microservice instance levels, particularly in cases where historical information of the cluster is unknown. The required microservice instance levels are also utilized in availability fitness calculation measures, aided through the use of a generalized logistic function [12] to avoid giving high scoring fitness values from resources that require low resource consumption and are of low instance levels, thereby establishing a fairer scoring method. In this regard, the fitness is calculated as defined through (3) given below.

Table 2: Fitness Cucalation

R	Required instances for each service
S	The current number of instances in each service
TA	Total availability
N	Number of microservices

Maximize $TA =$

$$\sum_{i=1}^{i=n} R_i \times \text{generalizedLogisticFunction} \left(\frac{S_i}{R_i} \right) \quad (3)$$

The fitness function also makes use of a scoring system based on the distribution of the number of instances deployed on cluster node resources known as the scale value. In this regard, a higher number of instances distributed among cluster nodes throughout the deployment are given a higher score than localized instances deployed within a single node. This task is performed to avoid convergence of dependent services into one node and affecting availability. These scale values are then utilized to infer performance and availability decisions.

iv. General Cluster Information

The optimization algorithm also makes use of the general cluster infrastructure information such as the resource power consumption of nodes and node labels names. The information gathered in this regard is primarily utilized in the definition of constraints utilized by the optimization algorithm.

IV. RESULTS AND DISCUSSION

The developed optimization model was evaluated on a sample microservice cluster dataset containing 3 nodes and 6 microservices. For evaluation purposes, the JSON (JavaScript Object Notation) representation of this cluster dataset, along with the additional information required by the optimization algorithm which includes the node latency map, predicted inter-microservice dependency measures as well as the required number of microservice instances, is provided to the developed optimization algorithm in order to compute the optimized solutions. Fig. 3 below depicts the structure of the sample input JSON provided to the optimization algorithm.

```
{
  "nodes": {
    "0": {
      "ip": "",
      "cpu": 4000,
      "memory": 8000,
      "storage": 500000,
      "1": {
        "ip": "",
        "cpu": 2000,
        "memory": 4000,
        "storage": 500000,
        "2": {
          "ip": "",
          "cpu": 4000,
          "memory": 8000,
          "storage": 500000,
          "pods": {
            "0": {
              "name": "",
              "cpu": 300,
              "memory": 200,
              "storage": 300,
              "1": {
                "name": "",
                "cpu": 300,
                "memory": 200,
                "storage": 300,
                "2": {
                  "name": "",
                  "cpu": 200,
                  "memory": 200,
                  "storage": 300,
                  "3": {
                    "name": "",
                    "cpu": 200,
                    "memory": 200,
                    "storage": 300,
                    "4": {
                      "name": "",
                      "cpu": 200,
                      "memory": 200,
                      "storage": 300,
                      "5": {
                        "name": "",
                        "cpu": 200,
                        "memory": 200,
                        "storage": 300,
                        "nod_latencies": {
                          "[0, 1]": 20,
                          "[0, 2]": 30,
                          "[1, 2]": 20,
                          "[0, 0]": 1,
                          "[1, 1]": 1,
                          "[2, 2]": 1,
                          "pod_dependency_map": {
                            "[0, 2]": 1000,
                            "[1, 3]": 500,
                            "[4, 5]": 200,
                            "pod_importance": "",
                            "microservice_instances_requirement": [4, 4, 2, 2, 2, 2]
                          }
                        }
                      }
                    }
                  }
                }
              }
            }
          }
        }
      }
    }
  }
}
```

Fig. 3: Structure of sample JSON provided as input to the developed optimization algorithm

Once the optimization algorithm is executed, a set of optimized solutions are obtained. In this regard, two optimized solutions are obtained once the algorithm is executed; one solution represents the cluster orientation with the highest cluster performance as depicted in Fig. 4, whereas the second solution obtained depicts the solution that represents the cluster orientation with the highest cluster availability as depicted in Fig. 5. For added

clarification, the tabular format of the representation is given alongside the resulting solutions.

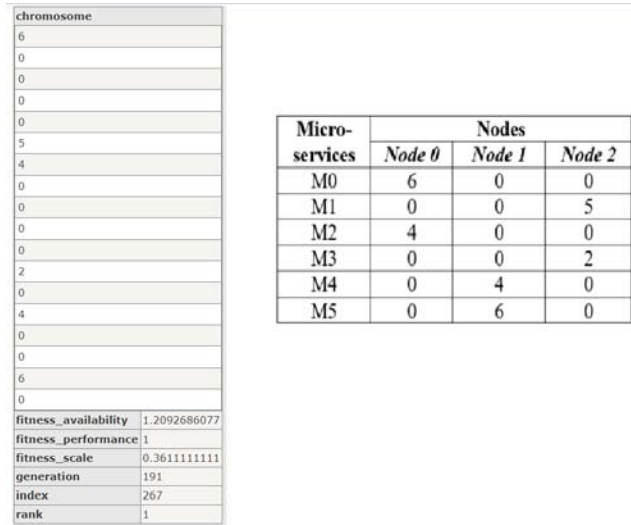


Fig. 4: Resulting solution representing cluster orientation with the highest performance

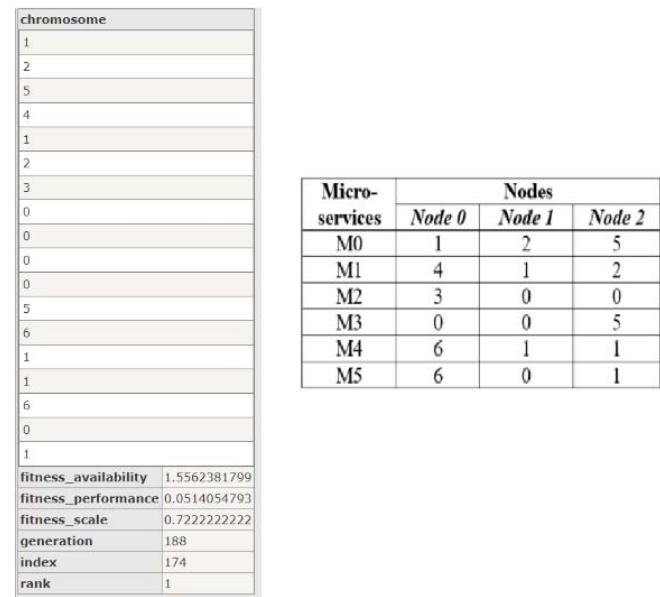


Fig. 5: Resulting solution representing cluster orientation with the highest availability

Note the fact that in the tabular format depicted in Fig. 4 and Fig. 5, each cell in the table represents the optimal number of instances of a given microservice that should be present in order to achieve the required optimization goal (highest performance or highest availability).

With regard to the resulting solution obtained that represents the cluster orientation with the highest performance, the fact that the optimization algorithm has successfully managed to determine the cluster orientation with the highest performance is evident primarily due to the fact that the highest dependent services as provided in the input JSON have been determined to be placed on

the same node by the optimization algorithm. This fact is determined through comparing the keys of the key-value pair sets in the “pod_dependency_map” feature of the input JSON which represents inter-dependent sets of microservices with the tabular representation of the resulting optimal performance solution, that also depicts the inter-dependent microservices as described in the input JSON (such as M0 and M2) placed on the same node. (For example: - “[0, 2]: 1000” in the input JSON represents microservice M0 and microservice M2 are interdependent microservices with a dependency level of 1000)

Similarly, through comparing the “microservices_instances_requirement” feature of input JSON which represents the required number of instances required for each of the six microservices respectively, with the resulting instance levels obtained from resulting highest availability solution, it is evident that the optimization algorithm has also ensured highest availability of microservices through the allocation of a higher number of microservice instances than the required instances. (For example- Microservice M0 requires the presence 4 instances and the optimization algorithm has allocated 8 instances of M0 as determined through its optimization process)

V. CONCLUSION

This publication suggests the application of a network-science based microservice governance model in an attempt to aid in the creation of optimized microservice deployment policies currently hindered due to the employment of disjoint monitoring solutions prevalent in microservice-based governance methodologies. In this regard, the proposed model seeks the creation of a holistic perspective of microservice deployments, through the incorporation of dependency analysis, load prediction measures, centrality measures as well as resilience measures. Furthermore, through the incorporation of the above measures, the research conducted utilizes the application of an optimization algorithm to determine an optimal deployment strategy for a given microservice deployment.

The publication also discusses the core architecture along with the methodologies followed in the development of the proposed governance model as well as the results obtained through the application of the proposed governance model. Analysis of the results suggests the developed governance model proved to be effective in determining the optimized cluster representations pertaining to the highest performance and availability. Future work will include considering the inner workings of applications deployed in a Kubernetes cluster so as to further increase the accuracy of existing prediction models and resilience analysis components.

REFERENCES RÉFÉRENCES REFERENCIAS

1. P. Jamshidi, C. Pahl, N. C. Mendonca, J. Lewis, and S. Tilkov, “Microservices: The journey so far and challenges ahead,” *IEEE Software*, vol. 35, no. 3, pp. 24–35, 2018, doi: 10.1109/MS.2018.2141039.
2. “Microservices Governance: A Detailed Guide.” <https://www.leanix.net/en/blog/microservices-governance> (accessed Jun. 16, 2020).
3. “Kubernetes. – Wikipedia.” <https://en.wikipedia.org/wiki/Kubernetes>. (accessed Jun. 16, 2020).
4. “What is Kubernetes? | Kubernetes.” <https://kubernetes.io/docs/concepts/overview/what-is-kubernetes/> (accessed Jun. 16, 2020).
5. “Kubernetes: The Challenge of Deploying & Maintaining.” <https://techolution.com/kubernetes-challenges/> (accessed Jun. 16, 2020).
6. R. Heinrich et al., “Performance engineering for microservices: Research challenges & directions,” *ICPE 2017 – Companion of the 2017 ACM/SPEC International Conference on Performance Engineering*, pp. 223–226, 2017, doi: 10.1145/3053600.3053653.
7. M. Fazio, A. Celesti, R. Ranjan, C. Liu, L. Chen, and M. Villari, “Open Issues in Scheduling Microservices in the Cloud,” *IEEE Cloud Computing*, vol. 3, no. 5, pp. 81–88, 2016, doi: 10.1109/MCC.2016.112.
8. D. Kim, H. Muhammad, E. Kim, S. Helal, and C. Lee, “TOSCA-based and federation-aware cloud orchestration for Kubernetes container platform,” *Applied Sciences (Switzerland)*, vol. 9, no. 1, 2019, doi: 10.3390/app9010191.
9. A. Jindal, V. Podolskiy, and M. Gerndt, “Performance modeling for cloud microservice applications,” *ICPE 2019 – Proceedings of the 2019 ACM/SPEC International Conference on Performance Engineering*, pp. 25–32, 2019, doi: 10.1145/3297663.3310309.
10. V. Medel, O. Rana, J. Á. Bañares, and U. Arronategui, “Modelling performance & resource management in Kubernetes,” *Proceedings – 9th IEEE/ACM International Conference on Utility and Cloud Computing, UCC 2016*, pp. 257–262, 2016, doi: 10.1145/2996890.3007869.
11. T. F. Düllmann and A. van Hoorn, “Model-driven generation of microservice architectures for benchmarking performance & resilience engineering approaches,” *ICPE 2017 – Companion of the 2017 ACM/SPEC International Conference on Performance Engineering*, pp. 171–172, 2017, doi: 10.1145/3053600.3053627.
12. “Generalised logistic function – Wikipedia.” https://en.wikipedia.org/wiki/Generalised_logistic_function (accessed Jul. 14, 2020).



This page is intentionally left blank



An Efficient Black-Hole and Worm-Hole Attacks Resilient Scheme for Cloud and Fog Assisted Internet of Vehicles

By Oladayo O. Olakanmi, Mbadiwe S. Benyeogor & Kehinde O. Odeyemi

University of Ibadan

Abstract- The Internet of Vehicles (IoV) is a distributed network that supports the use of data created by connected cars and vehicular ad-hoc networks (VANETs) for real-time communication among the vehicles and other infrastructures in the network. Although, IoV increases safety and efficient information exchange in transportation, its inter-connectivity exposes the vehicles and the people to different cyber-attacks such as black-hole and worm-hole which are capable of disrupting the network.

In this paper, we identify the black-hole and worm-hole attacks as the major security threats to the IoV technology. We then propose periodic-time slicing and trust factor approaches to detect and prevent a black-hole attack and a cryptography procedure to prevent other IoV related cyber-attacks.

Index Terms: car connectivity, cyber-security, cloud and fogassisted, internet of things, autonomous vehicles.

GJCST- B Classification: D.4.6



AN EFFICIENT BLACKHOLE AND WORMHOLE ATTACKS RESILIENT SCHEME FOR CLOUD AND FOG ASSISTED INTERNET OF VEHICLES

Strictly as per the compliance and regulations of:



RESEARCH | DIVERSITY | ETHICS

An Efficient Black-Hole and Worm-Hole Attacks Resilient Scheme for Cloud and Fog-Assisted Internet of Vehicles

Oladayo O. Olakanmi^α, Mbadiwe S. Benyeogor^σ & Kehinde O. Odeyemi^ρ

Abstract- The Internet of Vehicles (IoV) is a distributed network that supports the use of data created by connected cars and vehicular ad-hoc networks (VANETs) for real-time communication among the vehicles and other infrastructures in the network. Although, IoV increases safety and efficient information exchange in transportation, its inter-connectivity exposes the vehicles and the people to different cyber-attacks such as black-hole and worm-hole which are capable of disrupting the network.

In this paper, we identify the black-hole and worm-hole attacks as the major security threats to the IoV technology. We then propose periodic-time slicing and trust factor approaches to detect and prevent a black-hole attack and a cryptography procedure to prevent other IoV related cyber-attacks.

Index Terms: car connectivity, cyber-security, cloud and fogassisted, internet of things, autonomous vehicles.

I. INTRODUCTION

As IoV becomes more connected and more autonomous with advanced communication technologies for robust transportation services, it also becomes more attractive and susceptible to different cyber-attacks. IoV faces various types of attacks, such as replay, eavesdropping, Sybil, black-hole, and worm-hole attacks, which result in security and privacy challenges in IoV. Of all these attacks, worm-hole and black-hole attacks are the most active and elusive to most existing security schemes. They easily degrade the performance and reliability of the IoV as a result of the dynamism of the IoV network. Several solutions based on watchdog, statistical, predictive, heuristic, timing, trust, and incentives-based approaches have been developed to prevent black-hole and worm-hole attacks in the vehicular ad-hoc network and IoV [5]. However, the high complexity, high delay, and non-adaptiveness of some of them make them unsuitable to IoV networks.

Asides from black-hole and worm-hole attacks, enforcing privacy and data integrity are also the major issues in IoV. For example, malicious information from IoV can easily lead to loss of lives or compromise the

privacy of the car and passenger. In consequence of these, there is a need for a security scheme not only resilient to worm-hole and blackhole attacks but also capable of guarantee the privacy and integrity of IoV data.

In this paper, we propose a security scheme for IoV capable of detecting black-hole and worm-hole attacks. It uses periodic-slices and their corresponding concatenated hash, sent to the destination node through the secondary nodes, to detect black-hole attacks and a cryptography-based procedure to detect worm-hole attacks. The scheme includes incentive and trust models to establish a reputation-based communication to encourage cooperation and reduce black-hole attacks in the IoV. A provable one message authentication code, using onetime and mutual keys, is used to affirm the data integrity. The contributions of this paper are as follows:

1. A non-complex periodic-slices approach to detect blackhole attacks and a cryptography-based procedure to detect worm-hole attacks.
2. Incentive and trust model to enforce reputation and cooperation in IoV. attacks.

The paper is organized thus; the related past works on the security issues on IoV and existing solutions are discussed in section 2. Section 3 is the system overview where we describe the primitive, system, and adversary model. Section 4 describes the methodology of the proposed scheme with its incentive and trust model. Section 5 involves performance evaluation, this section consists of the results of the experimental analysis. We concluded the work in Section 6.

II. RELATED WORK

Detection and prevention of black-hole and worm-hole attacks are critical routing security issues in IoV. They can easily convert reliable cyber-physical paths in IoV for data and control packets routing into a compromised one. Meanwhile, they are elusive to most of the existing security solutions, therefore, the performance of IoV can be improved by making it resistible to malicious attacks likes black-hole and wormhole.

Author α σ ρ: Dept. of Electrical and Electronics Engineering University of Ibadan (of Aff.) Ibadan, Nigeria. e-mails: olakanmi@mit.edu, samrexbenzil@gmail.com, ko.odeyemi@ui.edu.ng

Black-hole attacker drops all packets it is supposed to forward to the destination node, meanwhile the worm-hole attacker re-direct packets taken from one location of the network to another part of the network.

Several approaches have been proposed to thwart blackhole in network [2], [8], [9], [10], [11], [3], [6], [12], [7]. For example, the work of Yao et al. [2] focus on blackhole. In the work, an entity-centric trust model is developed for detecting black-hole attacks, however, their approach may unfairly label honest nodes as black-hole attackers. Also, Daeinabi et al. [8] proposed an algorithm with a trust model capable of monitoring activities of a new entrant in VANET. The algorithm decreases the trust of a malicious new entrant who is dropping the packet and blacklists it once its trust is lower than the preset threshold. The authors in [9] improves the algorithm in [8] by enhancing the selection of the verifier and adding the prevention and isolation mechanism of blackhole attacks. Similar to [9], Uzma et al [10] enhanced the detection mechanism in [8] by increasing the verifier's selection criteria. In [11], Yao et al. developed a three-parameter of trust detection scheme for detecting selfish nodes in VANET.

Aside from using the trust model, the watchdog approach can still be used to detect black-hole. Watchdog approach checks the forwarding state of the

forwarded packets by monitoring the next-hop neighbor can be used to thwart blackhole attack [3]. Hortelano et al. [6] adopted a watchdog and trust mechanism to detect a black-hole attack. Also, [12], adopted a watchdog technique to detect black-hole attacks.

Meanwhile, Delkesh et al. [7], proposed a heuristic approach for detecting black-hole attacks in mobile ad-hoc networks. Their technique sends forged packets in the ad-hoc on-demand distance vector route discovery. Any node that replies to such fake destination IP address packets request is termed as a black-hole attacker. A predictive technique was used in [?] to prevent and detect intrusion. The approach can detect multiple misbehaviors of vehicles and selects the vehicle with the best trust value as the cluster head.

Like the black-hole, various solutions have also been proposed to detect worm-hole attacks in the network. Examples are the work in [15], [17], [18] and [16]. Safi et al. [15] introduced a solution that relies on the packet's maximum and allowed transmission distance in control packet and message authenticated packet [16] to detect worm-hole attacks. Hu et al. [17] adopted the temporal packet leash concept, with the notion of global clock synchronization. Their approach detects the worm-hole attacks from the exceptions in the

Table 1

Notation	Description
\mathbb{Z}_q	set of integer of order p
G	addition group of order q
P	generator of G
$H_k(\cdot)$	key based hash function l
I	trust factor
ϕ	incentive value
$\rho_j, \rho_i, \rho_d, \rho_c$	mutual public key parameter of $i, j, d,$ and $c,$ respectively
$\tau_{im\alpha ptoj}, \tau_{cm\alpha ptoj}$	entity-edge mutual secret key, cloud-edge mutual key
δ	one-time-key chain
F_i	pseudonym of entity i
n'	number of selected secondary nodes
λ_i	encrypted pseudonym of i
β	message authentication code
e	bilinear mapping function

packet transmission latency. C apkun et al. [18] used round trip travel time for the packet delivery to detect unusual wormhole channels. However, [17] and [18] solution are hardware based and presence of a global clock.

III. SECURITY GOALS AND PRIMITIVES

a) Security Goals

The security goals include detection of worm-hole attacks, integrity, and black-hole attacks in the IoV. Also, we gear the scheme towards secure local and global access of IoV data. To achieve the security goals, we develop periodic-slices and non-complex cryptography approaches for thwarting the elusive attacks in IoV networks.

b) Primitives

We adopted a cyclic addition group G of order q and generator P , a cryptographic hash functions $H : 0; 1^* \mapsto Z_q^*$, $H : 0, 1^* \times 0, 1^l \mapsto Z_q^*$, and a bilinear pairing e such that $e : GXG \mapsto G$ where l is the size of the secret key.

Table 1 shows the definition of the notations and symbols used in the scheme.

IV. BLACK-HOLE RESILIENT SCHEME WITH TRUST FACTOR

As shown in Figure 1, the system model of the IoV scheme consists of entities such as vehicles, pedestrians, infrastructures, roadside units (RSU), and storage facilities, which include location-bound edge

and cloud server. Each entity can perform multi-hop communication such as vehicle to vehicle, vehicle to infrastructure, and vehicle to pedestrian.

Each entity and the nearby edge generates a mutual public parameter and mutual secret key. The source entity, through either single-hop or multi-hop communication, pushes its loV information to the destination. The destination verifies the instance of attack and computes a reputation-based incentive for the source. It uploads the loV information to the edge for local access. The edge updates the source entity trust factor, reencrypts the loV information with the source trust factor, and pushes it to the cloud server for global access. The cloud then decrypts the loV information and updates its global trust table. The cloud re-encrypts the loV information and the source trust factor with the edge's mutual secret keys and pushes it to the corresponding edges to complete a global-request.

The proposed scheme is divided into four phases; set-up and key management, loV information hopping, loV attacks detection and integrity test, incentive and trust factor generation phases, each of these phases are described below.

a) *Set-Up and Key Management*

To set-up, each entity, cloud, and the nearby edge performs the following:

1. Each entity randomly generates r_i^* while the edge and cloud generate $k_j \in Z^*$ and u^* , respectively. Each entity computes and publishes its mutual public parameter as $\rho_i = e(P, P)^{r_i}$ while the edge j also computes and publishes its mutual public parameter as $\rho_j = e(P, P)^{k_j}$ to the surrounding entity, who uses it to compute edgeentity mutual secret key as $\tau_{i \rightarrow j} = \rho_j^{r_i} = e(P, P)^{r_i k_j}$.
2. Each entity then computes one-time-key as $\delta_{h+1} = H_{\tau_{i \rightarrow j}}(\delta_h) \forall h = 0, 1, \dots, w$, where $\delta_0 = H_{\tau_{i \rightarrow j}}(\tau_{i \rightarrow j} || F_i)$ and pseudonym as $F_i = H(id_i)$.
3. The cloud randomly generates u^* , computes and publishes $\rho_c = e(P, P)^{u^*}$ it to the surrounding edges, who also uses it to compute edge-cloud mutual key $\tau_{c \rightarrow j}$ as $\tau_j \mapsto c = \rho_c^{k_j} = e(P, P)^{u^* k_j}$.

b) *loV Data Hopping*

For each hopping session, the source sub-divides the unique session period into n' periods, selects the primary neighboring node for the loV packet, and another $n = n'$ secondary nodes for the transmission of the $n' - 1$ periodic slices and their concatenated hash value as shown in Figure 2. It then sends the periodic slices and concatenated hash value to the destination through the secondary neighboring entities.

It sends one of the periodic-slices, encrypted packet, and message authentication code through the primary neighboring node to the destination.

The destination detects black-hole by re-computing the concatenated hash value, compare it with the received hash value. If equal, it indicates no black-hole attack otherwise black-hole is detected. In case there is no black-hole attack, the destination confirms the worm-hole attack through the received pseudonym and the data integrity. The destination then computes the incentive for the source node, uploads the copies of the encrypted loV information and the incentive to the edge who updates the source trust factor. This phase is summarized as follows:

1. The source generates n' periodic-slices $t_1, t_2 ; \dots ; t_{n'-1}, t_{n'}$ by sub-dividing the time stamp t into n' .
2. The source selects the primary neighbouring entity for the loV information m and another $n = n'$ secondary entities within the coverage for the transmission of the $n' - 1$ periodic slices and hash value $\alpha_t = H(t_1 || t_2 | \dots || t_{n'})$ and encrypted source pseudonym as shown in Figure 2 and 3.
3. The source sends periodic slices $t_1, t_2, \dots, t_{n'-1}$ and $\alpha_t || \lambda_i$ to the destination through the corresponding secondary neighbouring n entities.
4. Generates mutual key between the destination d and the source i as $\tau_{i \rightarrow d} = (\rho_d)^{r_i}$. Then, encrypted packet $c_{i,t} = E_{\tau_{i \rightarrow d}}(m_{i,t})$, encrypts pseudonym of the source as $\lambda_i = E_{\delta_h}(F_i)$ using one of the next unused one-timekey in its key chain, generates message authentication code $\beta = H_{\tau_{i \rightarrow d}}(m_{i,t})$, and sends $t_{n'}, \beta, \lambda_i, c_{i,t}$ through the primary neighbouring entity to the destination node.

c) *loV Attacks Detection and Integrity Test*

As shown in Figures 2 and 3, to detect black-hole attack the destination on receiving loV data $(t_{n'}, \beta, \lambda_i; c_{i,t}$, and $\alpha_t)$ from the primary entity and $t_1, t_2 ; \dots ; t_{n'-1}, \alpha_t$ from secondary n' entities, it re-computes $\alpha'_t = H(t_1 || t_2 | \dots || t_{n'})$. Checks $\alpha'_t \stackrel{?}{=} \alpha_t$, if holds, it implies no black-hole, otherwise black-hole is detected and drops the whole loV information.

To detect worm-hole attack, the destination performs the following:

- Extracts λ_i, ρ_i and sends it to its edge for verification, who re-computes the edge-entity mutual key as $\tau'_{i \rightarrow j} = \rho_i^{k_j}$.
- The edge then re-computes the source one time secret key chain as $\delta'_{h+1} = H_{\tau'_{i \rightarrow j}}(\delta'_h) \forall h = 0; 1; \dots; w$, where $\delta'_0 = H_{\tau'_{i \rightarrow j}}(\rho_j || F_i)$. It decrypts the $F_i = E_{\tau'_{i \rightarrow j}}(\lambda_i)$ and for each δ'_{h+1} checks if $F_i \stackrel{?}{=} F_i$. If this does not hold for any of the δ'_{h+1} then worm-hole attack detected otherwise the edge clears the source node of the worm-hole.

After receiving the worm-hole clearance from the edge, the destination checks the integrity of the data as follows:

- Re-computes the one-time-key, using the mutual public parameter of the source, as $\tau'_{d \rightarrow i} = \rho_i^{\tau_d} = e(r_d P, r_i P) = e(P, P)^{r_d r_i}$
- Decrypts the loV information as $m_{i,t} = D_{\tau'_{d \rightarrow i}}(c_{i,t})$
- Re-generates message authentication code as $\beta = H_{\tau'_{d \rightarrow i}}(m_{i,t})$, and checks $\beta' \stackrel{?}{=} \beta$. If holds the integrity test holds and then accepts the loV information $m_{i,t}$; otherwise rejects the

d) Trust and Incentive Generation

To detect and dissuade black-hole attacks, we develop an incentive and trust models as shown in equation 1 and 2. These models are used by the destination and edge to compute incentive ϕ and trust factor I , respectively. The incentive and trust factors models are described as follows:

$$\phi = \epsilon_1^{(s_2+s_3)s_1} + \epsilon_2^{(s_1+s_3)s_2} + \epsilon_3^{(s_1+s_2)s_3} \tag{1}$$

$$I_{i+1} = I_i + (1 - e^{-T_{nbh}}) + T_{nbh} e^{\phi_i} \tag{2}$$

where ϕ is the incentive given to the source by the destination node, I_i is the previous trust factor of the source node, T_{nbh} is the total number of previous black-hole attacks launched by i , $\epsilon_1, \epsilon_2, \epsilon_3$ are the black-hole, worm-hole, and integrity attacks weights, respectively, s_1, s_2, s_3 are the corresponding black-hole, worm-hole, and integrity attacks launched status.

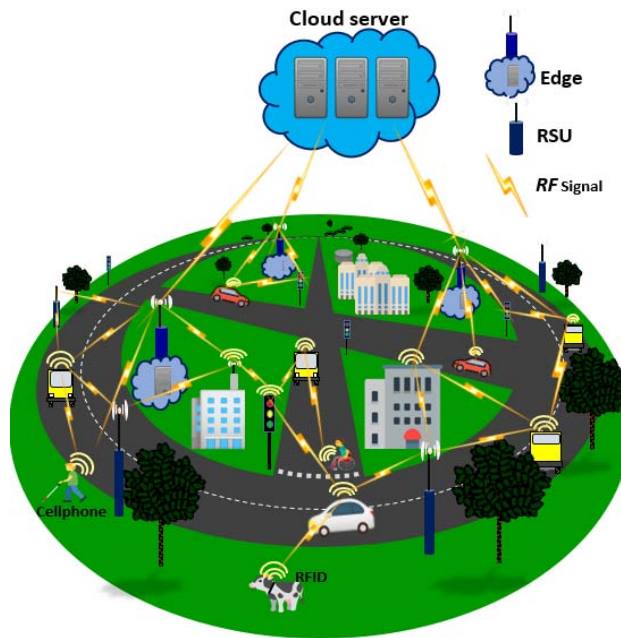


Fig. 1: System Model of the Proposed loV Scheme

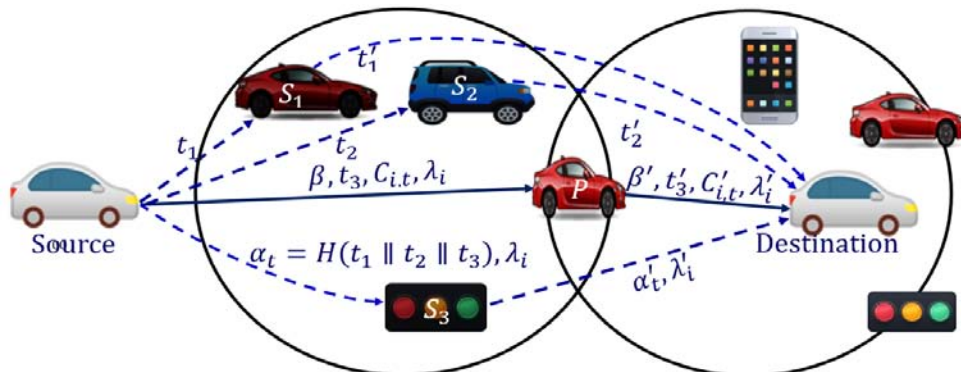


Fig. 2: Scenario of No Black-Hole Attack



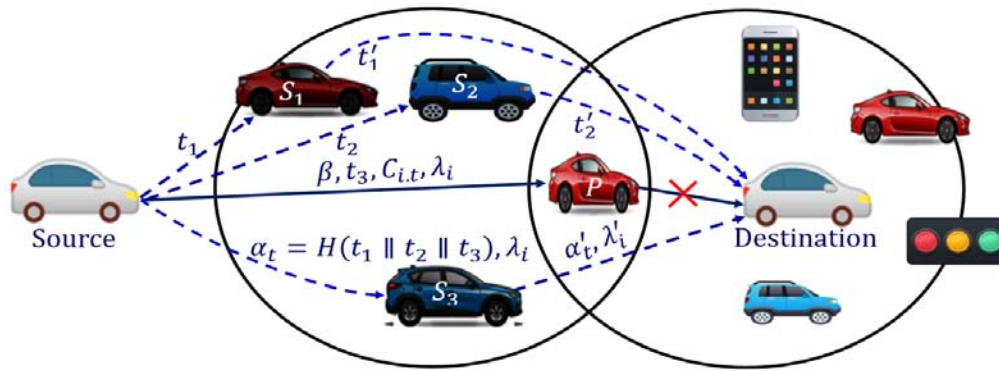


Fig. 3: Scenario of Black-Hole Attack

At the clearance of source node of worm-hole attack, successful black hole and integrity tests, the destination node computes the incentive ϕ using Eqn 1, encrypts the computed incentive as $E_{\delta_h}(\phi)$, using the next unused master secret key δ_h from its master secret key chain, and sends it to the edge. The edge decrypts the $E_{\delta_h}(\phi)$, updates the source node trust factor using equation 2, and pushes a copy of the updated trust factor table and the IoV data to the cloud server for other entities outside the edge coverage.

V. RESULTS AND DISCUSSIONS

In this section, we presented the experimental results for the proposed scheme in terms of communication and computation overheads incur as a result of the execution of the scheme.

The experimental set-up evaluates the computation and communication costs. To achieve this, we simulate each of the cryptographic operations used in the proposed scheme using a cryptoPP library [?] implemented on Intel(R) Core(TM)i3 2.73GHz.

The simulation shows that an exponentiation operation in G (Te) takes 5.5ms, a bilinear pairing operation (Tbp) takes 11.07ms, 256-bit Rijndael symmetric encryption (Tse) takes 1.9348ms, 0:007ms as the running time of a general hash function operation (TH), and a scalar multiplication operation (Tsm) takes 2.165ms. With the these cryptography operations running times, the set-up phase takes $Tbp + Te + (m0 + 1)TH = 16:807ms$ for any registered entity, while the edge and cloud each take $tbp = 11:07ms$. Meanwhile, in the IoV data hopping phase for a hop count, source takes $2Tse+Te+TH = 7:442ms$ while the destination node requires $(h'' + 2)TH + Tse + Te + Tdec = 19:184ms$. Figure 4 shows the summary of the computation overheads of each phases in terms of running time.

We also evaluate the communication overhead of the scheme. We notice that the source node incurs $n'|t|+3|H|+|c|$ bits as the communication overhead

during IoV data hopping where n' is the number of periodic-slices used, $|t|$ is the size of a periodic-slice, $|H|$ is the size of the hash function, and $|c|$ is the size of the ciphertext. The attacks detection and integrity test phase incur $|H|+|G|$ bits. That is, the total communication overhead of the scheme is $n0|t| + 4|H| + |c| + |G| = 232$ bytes for 256 bits ciphertext of Rijndael symmetric encryption, periodic-slice of size 16-bit, of 512-bit size group G, and 256-bit SHA-256. This reflects that the proposed scheme only has an insignificant communication overhead.

The proposed incentive and trust factors model are evaluated in terms of how different attack patterns A= "black hole, worm-hole, integrity" affects the incentive and trust of source node with initial trust value $l=50$, where "0" represents attack and "1" represent no attack. Figure 5 shows the incentives of source nodes launching different patterns of black-hole, wormhole, and integrity attacks. It indicates that any instance of attack reduces the incentive and both worm-hole and blackhole attacks significantly reduce the source node incentive at an instance of integrity attack. Figure 6 depicts the effect of different attacks of different patterns on the trust values of the source node. It implies that the scheme assigns the highest trust value for a source node with no record of attack in the network. That is, it indicates a good reputation for the source node with no or few records of attacks.

Also, the mean waiting time of the destination node for different network sizes and one-time key chains are shown in Figure 7. It shows that the network size does not affect the mean waiting time, that is with the increase in the network size the proposed scheme introduces insignificant delay. However, there is a significant delay as the entity's time key chain increases.

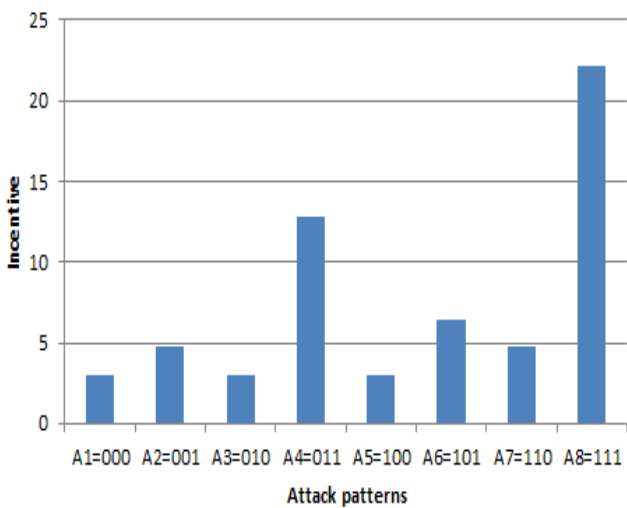


Fig. 4: Effect of different attacks on the incentive of a source node

VI. CONCLUSION

Communication in IoV is susceptible to different attacks, among which black-hole, worm-hole, and integrity attacks are ranked as the most elusive attacks. They can cause serious damage when the road information depicts a serious incident.

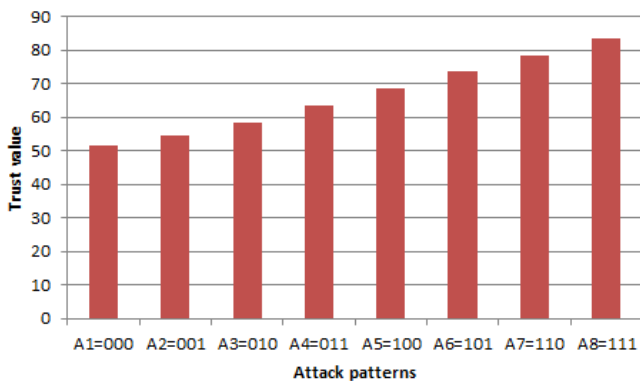


Fig. 5: Effect of different attacks on the reputation of a source node

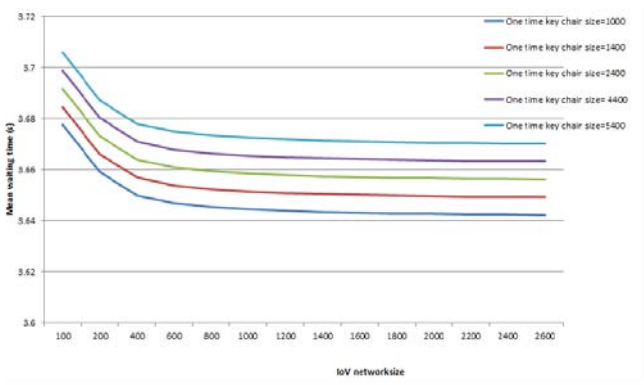


Fig. 6: Mean waiting time of the destination node for different network and one time key chains sizes

This paper proposed a new method to detect the black hole, worm-hole, and integrity attacks during communication in an IoV environment and assigns high trust and incentive to an honest entity but low or no trust and incentive to a malicious entity.

REFERENCES RÉFÉRENCES REFERENCIAS

1. Badreddine Cherkaoui, Abderrahim Beni-hssane, Mohammed Erritali, "Black-hole Attack Detection in Vehicular Ad Hoc Networks Using Statistical Process Control", International Journal on Communication Antenna and Propagation, Vol. 7, No. 3, 2017
2. X. Yao, X. Zhang, H. Ning, and P. Li, "Using trust model to ensure reliable data acquisition in VANETs," Ad Hoc Networks, vol. 55, pp. 107–118, Feb. 2017.
3. H. Sanadiki, H. Otrok, A. Mourad, and J.-M. Robert, "Detecting attacks in QoS-OLSR protocol," in 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC), 2013, pp. 1126–1131.
4. Y.C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, 2003, vol. 3, pp. 1976–1986.
5. Fatih Sakiz Sevil Sen, "A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems: VANETs and IoV", Ad hoc Network, 2017, Vol. 61, Pp.33-50
6. J. Hortelano, J. C. Ruiz, and P. Manzoni, "Evaluating the usefulness of watchdogs for intrusion detection in VANETs," in Proc. IEEE Int. Conf. Commun. Workshops, Capetown, South Africa, May 2010, pp. 1–5.
7. T. Delkesh and M. Jabraeil Jamali, "EAODV: Detection and removal of multiple black hole attacks through sending forged packets in MANETs," J. Ambient Intell. Hum. Comput., vol. 10, no. 5, pp. 1897–1914, 2019.
8. A. Daeinabi and A. G. Rahbar, "Detection of malicious vehicles (DMV) through monitoring in vehicular ad-hoc networks," Multimedia Tools Appl., vol. 66, no. 2, pp. 325–338, Sep. 2013.
9. M. Kadam and S. Limkar, "Performance investigation of DMV (detecting malicious vehicle) and DPMV (detection and prevention of misbehave/malicious vehicles): Future road map," in Proc. Int. Conf. Frontiers Intell. Comput., Theory Appl. (FICTA), 2014, pp. 379– 87.
10. U. Khan, S. Agrawal, and S. Silakari, "Detection of malicious nodes (DMN) in vehicular ad-hoc networks," Procedia Comput. Sci., vol. 46, pp. 965–972, Jan. 2015.

11. X. Yao, X. Zhang, H. Ning, and P. Li, "Using trust model to ensure reliable data acquisition in VANETs," *Ad Hoc Netw.*, vol. 55, pp. 107–118, Feb. 2017.
12. O. A. Wahab, H. Otok, 161 and A. Mourad, "A Dempster–Shafer based tit-for-tat strategy to regulate the cooperation in VANET using QoS-OLSR protocol," *Wireless Pers. Commun.*, vol. 75, no. 3, pp. 1635–1667, Apr. 2014.
13. R. Baiad, H. Otok, S. Muhaidat, and J. Bentahar, "Cooperative crosslayer detection for blackhole attack in VANET-OLSR," in *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Nicosia, Cyprus, Aug. 2014, pp. 863–868.
14. Sun, Y., Wu, L., Wu, S., Li, S., Zhang, T., Zhang, L., . . . Cui, X. (2016). Attacks and countermeasures in the internet of vehicles. *Annals of Telecommunications*, 72(5-6), 283–295. doi:10.1007/s12243-016-0551-6
15. S. M. Safi, A. Movaghar, and M. Mohammadzadeh, "A novel approach for avoiding wormhole attacks in VANET," in *2009 First Asian Himalayas International Conference on Internet*, 2009, pp. 1–6.
16. S. Biswas and J. Misić, "A Cross-Layer Approach to Privacy-Preserving Authentication in WAVE Enabled VANETs," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2182–2192, Jun. 2013.
17. Y. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *Proceedings of the 22nd Annual Joint Conference on the IEEE Computer and Communications Societies*, vol. 3, pp. 1976–1986, April 2003.
18. S. Ç apkun, L. Buttya ´n, and J. -P. Hubaux, "SECTOR: secure tracking of node encounters in multi-hop wireless networks," in *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03)*, pp. 21–32, Fairfax, Va, USA, 2003. View at: [Publisher Site](#) — [Google Scholar](#)
19. J. Eriksson, S. V. Krishnamurthy, and M. Faloutsos, "TrueLink: a practical countermeasure to the wormhole attack in wireless networks," in *Proceedings of the 14th IEEE International Conference on Network Protocols (ICNP '06)*, pp. 75–84, November 2006.





This page is intentionally left blank



Cloud Computing and other ICT Advancements use in Kenya's Agricultural Sector

By Jeremiah Osida Onunga & Alice Nambiro

Kibabii University

Abstract- According to the latest World Economic Forum study, agriculture provides a living for over 70% of Kenya's people. As a result, agriculture is a crucial sector in Kenya. Agricultural productivity is still low, and food poverty remains a problem. This has resulted in a number of projects in recent years to use ICT advancements to boost agricultural output. Cloud computing is one of the advancement that can be used by organizations that still have the traditional on premise IT systems. Agriculture is one of the most important areas that has shaped the socioeconomic growth of most countries. Over time, the benefits of widespread adoption and usage of information and communication technologies in agriculture have included improved agricultural productivity and linkages to remunerative markets, food security, and national economies, among other things. E-agriculture is a branch of activity that involves the use of information and communication tools and technology to boost agricultural productivity and make information pertinent to agricultural research, planning, extension, production, monitoring, marketing, and trade available.

Keywords: *development, information and communications technology (ICT), innovation, kenya, agriculture.*

GJCST- B Classification: *1.0*



CLOUDCOMPUTINGANDOTHERICTADVANCEMENTSUSEINKENYASAGRICULTURALSECTOR

Strictly as per the compliance and regulations of:



RESEARCH | DIVERSITY | ETHICS

Cloud Computing and other ICT Advancements use in Kenya's Agricultural Sector

Jeremiah Osida Onunga ^α & Alice Nambiro ^σ

Abstract- According to the latest World Economic Forum study, agriculture provides a living for over 70% of Kenya's people. As a result, agriculture is a crucial sector in Kenya. Agricultural productivity is still low, and food poverty remains a problem. This has resulted in a number of projects in recent years to use ICT advancements to boost agricultural output. Cloud computing is one of the advancement that can be used by organizations that still have the traditional on premise IT systems. Agriculture is one of the most important areas that has shaped the socioeconomic growth of most countries. Over time, the benefits of widespread adoption and usage of information and communication technologies in agriculture have included improved agricultural productivity and linkages to remunerative markets, food security, and national economies, among other things. E-agriculture is a branch of activity that involves the use of information and communication tools and technology to boost agricultural productivity and make information pertinent to agricultural research, planning, extension, production, monitoring, marketing, and trade available. The goal of this desktop review research is to look into how ICT advancements have been used in Kenya's agriculture sector. Cloud computing as an advancement was reviewed. Cloud computing saves money by removing the need for costly infrastructure and it also gives businesses an easy-to-use, cost-effective, adaptable, dynamic, and secure environment in which to do business. Radios are still commonly utilized to disseminate agriculture information to rural farmers, according to the analysis, while computers are primarily used by researchers. Despite the fact that mobile-based services aimed to improve access to accurate and timely agriculture information, previous literatures show that adoption is hampered by poor technological infrastructure, ineffective ICT policies, and low user capacity, particularly among farmers, to use the technologies.

Keywords: development, information and communications technology (ICT), innovation, kenya, agriculture

I. INTRODUCTION

Kenya's agriculture industry is underdeveloped, and food insecurity remains a problem. Kenya is still a net importer of food, despite its abundant natural resources and strong agricultural potential. According to an African Development Bank research (Moyo, Bah, & Verdier-Chouchane, 2019), Kenya imports 14.6 percent of its food.

Author α: Tutorial Fellow, Turkana University College and PhD Candidate, Kibabii University. e-mail: jerryosida@gmail.com

Author σ: Director, Open Distance & elearning (ODEL), Kibabii University. e-mail: anambiro@kibu.ac.ke

Agricultural commodity value addition and processing are similarly low, and postharvest losses are substantial. Agriculture, on the other hand, continues to be an important sector in the country. It is the primary source of income for the vast majority of the country's rural residents. Agriculture employs about two-thirds of the workforce and contributes for roughly 75 percent of all domestic trade (World Bank, 2010). The bulk of the rural population relies on agriculture for a living, hence the sector's growth and development are vital. The agricultural sector's growth and development can be aided by the appropriate use of information and communication technology (ICT)

ICTs has been a key contributor to growth and socio-economic development in nations and sectors where they are properly deployed, according to the Food and Agriculture Organization (FAO, 2017). The effective integration of ICT in the agriculture sector in American and European countries has resulted in a significant increase in the efficiency and productivity of the agriculture value chain. Traceability technologies such as block-chain and radio frequency identification (RFID), for example, have enabled transparency and efficiency throughout the food chain by allowing food to be tracked and traced from farm to fork. Kenya, on the other hand, has yet to undergo such a shift. Efforts to reform the sector have resulted in the proliferation of various mobile-based applications and services in recent years.

Cloud computing as an ICT advancement is defined as a methodology for providing on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be quickly supplied and released with minimal administration effort or Cloud provider interaction.

Cloud computing is sweeping the IT world today, bringing significant changes to how IT services are created, distributed, consumed, and maintained. The residual consequences of the global recession, which caused many firms to slash their cost structure (capital and operating) while still meeting customer needs, have spurred demand for cloud computing – and its antecedents, virtualization and off-premise services.

Cloud computing is a strategic endeavor for businesses that tries to achieve the correct balance between cost reduction and growth potential. Cloud

computing is a tried-and-true method for lowering IT capital expenses and increasing operational efficiencies. Many CIOs have been put off by concerns about data security, service availability, performance, and integration complexity.

According to the Technical Centre for Agriculture and Rural Cooperation's (TCARC) recent digitalization research (Digitalization of African Agriculture, 2019), 33 million smallholder farmers are already accessed by digital applications, with this number expected to rise to 200 million by 2030. Advisory and information services, market connections, financial access, and supply chain management are among the applications targeted, with advisory and information services dominating the market (Digitalization of African Agriculture, 2019). Kenya, as an African country, fits under this group as well. According to (El Bilali and Allahyari2018), ICT-based innovations can improve rural livelihoods and empower smallholder farmers in Kenya's developing counties by boosting connectivity and access to accurate and timely agriculture information. Data mining applications, for example, which are a popular technology platform in Kenya, combine mobile and web services to improve access to extension services and market information. This lowers the expense of searching for market data and allows farmers to receive real-time weather and extension guidance.

Cloud Computing, radio, television, and mobile phones have all advanced in recent years, as have sophisticated technologies such as block-chain, artificial intelligence, cloud computing, the Internet of Things (IoT), and big data analytics (OECD, 2017). According to (El Bilali and Allahyari2018), these disruptive ICT developments have the potential to help agricultural migrate to sustainability by increasing efficiency, transparency, and traceability. (Iliyas, 2014) emphasized that satellite-based remote sensing and geographic information systems can be used to boost agricultural output. 2020)

In addition, big data analytics can be applied in farming operations to deliver predictive insights, drive real-time operational choices, and rethink business processes (Wolfert et al., 2017) (Ahoa et al.2020) (Kassahun et. al, 2020). Precision agriculture, which employs a variety of technologies such as GPS, GIS, mobile computing, advanced information processing, and software, can provide comprehensive data on production variability in both place and time (Zhang et al, 2002) (Koksai & Tekinerdogan, 2019). (Verdouw et al., 2019).

There exist little research on ICT breakthroughs in the past. (Zewge and Dittrich2017) used a systematic mapping approach to describe the current level of ICT for Agriculture research in underdeveloped nations. Their research focused on journal and conference articles published in developing countries between 2006

and 2014. Mobile phones, PCs, tele-centers, and the internet were recognized as the key ICTs in developing countries, with the mobile phone being the favored technology, particularly in rural regions, according to their research. Similarly, (Lwoga and Sangeda2019) conducted a systematic review in developing countries to describe ICT for development research trends, techniques, and conceptual frameworks.

According to Kevin Yin (2016), data centers serve as platforms for typical enterprise IT applications. IT resources and separate IT apps are part of their stack architecture. Traditional data center architecture, on the other hand, will no longer be able to meet market expectations as the number of enterprise IT applications grows. In previous years, the overall number of resources (including servers and storage devices) expanded by 40% to 70% each year, while typical resource usage was only 10% to 25%. He further opines that a data center is a physical facility that organizations use to house their critical applications and data. A data center's design is based on a network of computing and storage resources that enable the delivery of shared applications and data. The key components of a data center design include routers, switches, firewalls, storage systems, servers, and application-delivery controllers. In the world of enterprise IT, data centers are designed to support business and agricultural applications and activities that include: email and file sharing, productivity applications, Customer Relationship management (CRM), Enterprise resource planning (ERP) and databases, Big data, artificial intelligence, and machine learning and Virtual desktops, communications and collaboration services, this are used to provide the vital information to farmers and also inform the general public on the availability of different agricultural needs in Kenya.

II. METHODOLOGY

The main methodology employed was a desktop review of past studies in ICT and its use in agriculture. In addition, desktop review revealed that user-centered design research is rarely used in the development of ICT applications. In order to gather insights and improve collective problem definition in the given environment, the study advocates a paradigm change from developing technologies for users to designing and developing applications with users. This will improve the adoption and actual use of ICT advancements to improve our livelihoods. In this review work not much was available on ICT advancements for agricultural development in Kenya. As a result, the goal of this study is to carry out a desktop review examine the current condition of ICT advancements in Kenya's agriculture sector. The desktop review included a thorough examination of the previous literature on agriculture and ICT. This review of work on ICT

advancements in Kenya is important for adding to the body of knowledge in Kenyan agriculture.

In this desktop review article, the researcher adopted (Kitchenham et al., 2019) method which entailed; identification of research questions, defining research strategy, defining quality assessment criteria, defining data extraction strategy, performing data extraction and defining data synthesis methods. The research topics identified for review were addressed using this approach. The search technique, which included identifying study selection criteria, was then detailed. After that, the researcher created quality assessment criteria in the form of a well-defined checklist to evaluate the studies that were chosen. The selection and quality criteria were then used to choose primary studies. The researcher next extracted and examined the pertinent review data from the primary studies.

The researcher's interest in this work is to look into empirical studies on the current state of ICT advancements in Kenya's agriculture industry. The review further put more emphasis on cloud computing as an emerging ICT advancement in agriculture in regards to data mining. The following research questions were developed to attain this goal:

1. Who are the agriculture stakeholders?
2. What are the common ICT technologies utilized in agriculture?
3. What are the benefits of using Cloud Computing in Agriculture Sector?

a) *Data Synthesis*

The data synthesis's goal is to summarize and present the findings of the desktop review in a way that is appropriate for answering our research objectives. This work fits into a qualitative study based on the research purpose and findings from the primary studies that were chosen, hence a descriptive synthesis of the retrieved data was undertaken. The researcher looked at each study individually as well as the group of studies as a whole. Studies with similar or identical meanings but distinct concepts were found and placed together under a single heading.

III. RESULTS

The results of this desktop review are presented in this section. To begin, descriptive data of the chosen reviewed previous related papers are presented. This part also includes the outcomes that match this review topic. The results will be presented as per the questions that this review work sought to answer.

a) *The Agriculture Stakeholders Identified in the Reviews*

The purpose of this review question is to identify the agriculture stakeholders who are being investigated in the papers under evaluation. A large number of

studies have looked into the usage of ICTs by farmers. Farmers, according to the study, utilize ICTs like mobile phones to communicate with extension workers and access prices for agricultural inputs and commodities. The use of ICTs by researchers, extension workers, and agribusinesses is discussed in a study by Mugwisi, T., Mostert, J., and Ocholla, D.N. (2015).

The application of ICTs in agriculture research is the focus here. Other studies looked into researchers' and extension workers' access to and use of ICTs. Another study (Aleke, B., Ojjako, U., & Wainwright, D. 2011) looked at the social determinants that influence agribusinesses' adoption of ICTs in rural areas. Socio-technical variables that limit the use of ICTs by agriculture researchers are examined in another study (Barakabitze, A.A., Kitindi, E.J., Sanga, C., Shabani, A., Philipo, J., & Kibirige, G. 2015).

This review paper agrees with the previous studies that identified the stakeholders in the agriculture sector. The stakeholders are farmers, researchers, extension workers and individuals in agribusiness. This review paper also agrees that the all stakeholders in the agriculture sector also use ICT applications.

The targeted agriculture domain of the selected publications in the study was examined to address this review question. The bulk of the publications (56%) focused on the agriculture industry as a whole while researching ICT developments within it. The agricultural sub-domain was highlighted in 36% of the studies, while the livestock and agroforestry sub-domains were highlighted in 2% and 6% of the papers analyzed, respectively.

b) *Common ICT Technologies Utilized in Agriculture*

The purpose was to figure out which ICT technologies were most commonly used in Kenya's agriculture industry. In the majority of polls, mobile phones were identified as the most widely utilized ICT tool in the agriculture industry. According to surveys, the growth of mobile phones on the African continent has resulted in the development of mobile-based apps and services in the business. Farmers are the primary target of these services and applications, which range from providing agriculture information such as market prices for farm produce, weather, agriculture input, and improved agriculture techniques to providing farmers with agriculture information such as market prices for farm produce, weather, agriculture input, and improved agriculture techniques. In the study (Kiambi, D. 2018) a farmer's helpline service in Kenya that provides agricultural assistance and information to smallholder farmers was mentioned. Farmers can receive information on increasing agricultural productivity, inputs, processing, climate, and market information by using a cell phone. Farmers that use this service call a toll-free number with specific questions, and agricultural specialists and subject matter experts respond.

Studies (Hudson et al. 2016, 2017), (Barakabizwe et al. 2017), (Mwombe et al. 2014), (Misaki et al. 2014), (Magesa et al 2017), (Mitegi W.P. and Msungu A.C. 2013), (Kiambi D. 2018), (Mubichi F and Freeman K. 2017), Radio remained the most extensively utilized medium in rural Kenya, Studies used the example of an interactive radio project in Tanzania, Uganda, Malawi, and Ethiopia to help small-scale farmers increase their production. Regular radio broadcasts on agricultural information for farmers were part of the radio program. Farmers may send questions to the program through SMS or phone, and the answers were broadcast on the radio. Studies also show most farmers use radio, according to (Hudson et al... 2017), (Barakabizwe et al...2017), and (Mwombe et al 2014), since radio programs are broadcast on community radio stations and in the farmers' own language, making it simple for them to absorb the information.

ICT technologies like as computers and remote sensing technologies are widely employed by both researchers and agribusiness professionals, according to studies (Mugwisiet al.2015), (Akele et al.2011), (Barakabizwe et al. 2015), (Mtega W.P and Msungu A.C 2013), (Kiambi D. 2018), (Awuor et al...2016) these technologies, however, were identified as being inaccessible to most farmers due to a lack of knowledge and financial resources to purchase them.

The findings of the desktop review on the use of ICTs in Kenya's agriculture area were provided in this desktop review. The researcher discovered that high-quality studies on ICT adoption have been published in recent years. The proliferation of ICTs such as television, radio, computer, and mobile phone in the agriculture sector was revealed by the review of the studies. The mobile phone was selected as the most often used ICT in the sector, which corresponds to the findings of (Zewge and Dittrich 2017).

Farmers can obtain financial and extension-advisory services such as weather, market, and agriculture advice through apps and services on their mobile phones, which are primarily geared at farmers. The usage of remote sensing technologies, which is one of the internet of things' enabling technologies, is also available in the industry, but it is mostly available to researchers and agribusinesses. The majority of these ICTs are employed for research reasons. However, poor infrastructure and regulatory environment, fragmentation and low coordination in the agricultural research sector, and low ICT skills and capabilities of farmers continue to limit utilization and accessibility.

From the above review this study confirms that the most commonly used ICT technologies in the agriculture sector are Mobile Phones, Radio, Television, Computer and Remote Sensing in order of the most commonly used to the least commonly use

c) *Benefits of using Cloud Computing in the Agricultural Sector*

After the desktop review of previous literature the following benefits of using cloud computing in the agricultural sector discussed:

i. *A High Level of Availability*

DR (Disaster Recovery) and Business Continuity Plans (BCP) solutions are used by most cloud-based services to back up user data. This means that even if the primary server goes down or is taken offline for maintenance, the EUs will continue be served by the backup system. Furthermore, most cloud-based services are likely to be run from world-class datacenters, reducing the danger of any form of outage in the first place.

ii. *Location Independence*

You access your data through an end terminal in a cloud-based computer environment by putting in an identifying key or password. This password can be used on any computer. The end user does not have to worry about a corrupt hard disk or malfunctioning RAM because the data is not stored on a specific end user (EU) terminal. Even if your machine fails, you will not lose your data. Consider it like signing into Facebook or Gmail on a friend's computer when yours fails.

iii. *No Updates*

Because programs are also hosted on service provider servers, all updates are carried out there. In other words, the service provider is responsible for any operating system (OS) or application patches, new versions, or any other type of modification that needs to be implemented.

iv. *No Need for an Antivirus*

Because the data is stored on service providers' servers, security methods are implemented to protect the data.

v. *Lower Computer Costs*

To use Cloud computing's web-based services, you don't need a powerful and expensive computer. Because apps run in the cloud rather than on your desktop PC, you don't need the processing power or hard disk space that traditional desktop software requires. When you use web-based apps, your PC can be less expensive because it has a smaller hard disk, less memory, and a more efficient processor. In fact, your PC doesn't even need a CD or DVD drive in this scenario because no software packages or document files need to be saved.

vi. *Improved Performance*

You'll get greater performance from your computer if you have fewer bloated programs sucking its RAM. Simply put, because cloud computing computers have fewer programs and processes stored into memory, they boot and function faster.

vii. *Reduced Software Costs*

Instead of spending money on software, you may acquire the majority of what you need for free. That's right: most cloud computing programs today are completely free, such as the Google Docs suite.

viii. *Instant Software Updates*

Another benefit of cloud computing in terms of software is that you no longer have to choose between outdated software and excessive update charges. When you use a web-based application, changes are automatically applied and are available the next time you log into the cloud. You obtain the most recent version of a web-based application without having to pay for or download an upgrade.

ix. *Improved Document Format Compatibility*

You don't have to be concerned about your documents being compatible with other people's apps or operating systems. All documents written by web-based apps can be viewed by any other user accessing that application, even if Word 2010 documents can't be opened on a computer running Word 2003. When everyone shares documents and apps in the cloud, there are no format mismatches.

x. *Unlimited Storage Capacity*

Cloud computing allows you to store nearly unlimited amounts of data. The 200 gigabyte hard drive on your PC is nothing compared to the hundreds of petabytes (a million gigabytes) available on the cloud. You can store whatever you want.

xi. *Increased Data Reliability*

In contrast to desktop computing, where a hard drive disaster might wipe out all of your important data, a computer crash in the cloud should not affect your data storage. That also implies that even if your personal computer fails, all of your data is still available in the cloud. Cloud computing is the ultimate in data-safe computing in a world where few individual desktop PC users back up their data on a regular basis.

xii. *Universal Document Access*

Have you ever gotten home from work and realized you left a crucial paper at work? Or did you forget to bring a file with you on your trip? Because you don't take your documents with you when you use cloud computing, this isn't an issue. Instead, they are stored on the cloud and may be accessed from any computer with an Internet connection. There's no need to bring your documents with you because they're instantly accessible from wherever you are.

xiii. *Latest Version Availability*

Another benefit of cloud computing for documents is that when you modify a document at home, the edited version is what you see when you access it at work. The cloud always has the most recent version of your documents; as long as you're connected, you'll never have an outdated copy.

xiv. *Easier Group Collaboration*

Sharing and collaborating on papers are inextricably linked. One of the most essential advantages of cloud computing, according to many users, is that numerous users may effortlessly collaborate on documents and projects. Because the documents are stored in the cloud rather than on individual computers, all you need is an Internet-connected computer to collaborate.

xv. *Device independence*

Finally, consider this benefit of cloud computing: You aren't bound to a single machine or network any longer. Your previous applications and documents will follow you across the cloud if you switch computers. Your apps and documents will still work if you switch to a portable device. There's no need to purchase a device-specific version of a program or save your document in a format that's specific to that device. No matter what computer or other device you're using, your documents and programs are the same.

xvi. *Better Return on Investments (ROI)*

Assuming that the IT asset returns on Cloud and on-premise IT are equivalent, it makes sense to use the Cloud's pay-as-you-go approach, in which the cost is incurred at the same time as the value is produced (James Staten, 2009).

From the review above, it showed that cloud computing as an ICT advancement is adopted in the agricultural sector can be beneficial to both farmers and the business community within the agricultural value chain.

IV. CONCLUSION

The researcher has presented a desktop review of the state of ICT advancements and the benefits of Cloud Computing as an ICT advancement in the Kenyan agriculture industry in this paper. The study's findings will be added to the body of knowledge on ICT adoption in Kenya. According to the studies reviewed, mobile-based services and platforms are the most often ICT advancement application in Kenya's agriculture industry. Radio and TV are common among the rural population.

From the reviews, the many benefits of cloud computing make farmers and organizations in the agriculture sector adopt it. Farmers can use mobile phone applications and services to get extension-advisory services like weather and market price information. Radios are still commonly utilized in rural areas to disseminate agricultural information. Weak policy environment, insufficient capability, and poor technological infrastructure within the country have all been identified as barriers to Cloud computing and other ICTs adoption

Smallholder farmers should be trained and empowered, according to the study, to improve their ability to deal with new agriculture technologies. In

addition, a favorable governmental and economic environment that encourages the use of ICTs and other digital technologies is required. Strong dedication, trust, and teamwork among the various participants in the agriculture value chain are also required.

REFERENCES RÉFÉRENCES REFERENCIAS

- Ahoa, E., Kassahun, A., Tekinerdogan, B. Business processes and information systems in the Ghana cocoa supply chain: A survey study, *NJAS - Wageningen Journal of Life Sciences*, Volume 92, 2020, 100323, ISSN 1573-5214, <https://doi.org/10.1016/j.njas.2020.100323>.
- Aleke, B., Ojiako, U., & Wainwright, D. (2011). Social networks among small agribusiness in Nigeria. *Society and Business Review*, 6 (3), 214-228.
- Awuor, F., Raburu, G., Onditi, A., & Rambim, D. (2016). Building E-Agriculture Framework in Kenya. *Journal of Agricultural Informatics*, 7 (1), 75-93.
- Barakabitze, A.A., Kitindi, E.J., Sanga, C., Shabani, A., Philipo, J., & Kibirige, G. (2015). New technologies for disseminating and communicating agriculture knowledge and information: Challenges for agricultural research institutes in Tanzania. *Electronic Journal of Information Systems in Developing Countries*, 70 (2), 1-22.
- El Bilali, H., & Allahyari, M. S. (2018). Transition towards sustainability in agriculture and food systems: Role of information and communication technologies. *Information Processing in Agriculture*, 5(4), 456-464.
- Food and Agriculture Organisation (FAO). (2017). Information and Communication Technology (ICT) in Agriculture: A Report to the G20 Agricultural Deputies.
- Hudson, H.E., Leclair, M., Pelletier, B., & Sullivan, B. (2017). Using radio and interactive ICTs to improve food security among smallholder farmers in Sub-Saharan Africa. *Telecommunications Policy*, 4, 670-684.
- Iliyas, S. (2014). Impact of Information Technology in Agriculture Sector. *International Journal of Food, Agriculture and Veterinary Sciences*, 4(2), 17-22.
- IoT-based food and farm systems: A multiple case study, Elsevier *Computers and Electronics in Agriculture*.
- Jere, N.J., & Maharaj, M. S. (2017). Evaluating the influence of information and communications technology on food security. *South African Journal of Information Management*, 19(1), a745.
- Kabbiri, R., Dora, M., Kumar, V., Elepue, G., & Gellyncka, X. (2018). Mobile phone adoption in agri-food sector: Are farmers in Sub-Saharan African connected? *Technological Forecasting & Social Change*, 131, 253-261.
- Kassahun, A., Tekinerdogan, B. BITA*: Business-IT alignment framework of multiple collaborating organisations, Elsevier *Information and Software Technology*, Volume 127, 2020, 106345, ISSN 0950-5849, <https://doi.org/10.1016/j.infsof.2020.106345>.
- Kiambi, D. (2018). The use of Information Communication and Technology in advancement of African agriculture. *African Journal of Agricultural Research*, 13(39), 2025-2036.
- Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering - A systematic literature review. *Information and Software Technology*, 51 (1), 7-15.
- Köksal, Ö., Tekinerdogan, B. Architecture design approach for IoT-based farm management information systems. *Precision Agric* 20, 926-958 (2019). <https://doi.org/10.1007/s11119-01809624-8>
- Lwoga, E. T., & Sangeda, R. Z. (2019). ICTs and development in developing countries: A systematic review of reviews. *Electronic Journal of Information Systems in Developing Countries*, 85(1), 1-17.
- Magesa, M.M., Michael, K., & Ko, J. (2017). Towards a framework for accessing agricultural market information. *Electronic Journal of Information Systems in Developing Countries*, 66 (3), 1-16
- Misaki, E., Apiola, M., Gaiani, S. (2016). Technology for small scale farmers in Tanzania: A design science research approach. *Electronic Journal of Information Systems in Developing Countries*, 74(4), 1-15.
- Moyo, J. M., Bah, E.-H. M., & Verdier-Chouchane, A. (2015). Transforming Africa's Agriculture to Improve Competitiveness. *The Africa Competitiveness Report*. 37-52.
- Mtega, W. P., & Msungu, A. C. (2013). Using Information and Communication Technologies for Enhancing the Accessibility of Agricultural Information for Improved Agricultural Production in Tanzania. *Electronic Journal of Information Systems in Developing Countries*, 56(1), 1-14.
- Mugwisi, T., Mostert J., & Ocholla, D.N. (2015). Access to and Utilization of Information and Communication Technologies by Agricultural Researchers and Extension Workers in Zimbabwe. *Information Technology for Development*, 21(1), 67-84.
- Mwombe, S.O.L., Mugivane, F.I., Adolwa, I.S., & Nderitu, J.H. (2014) Evaluation of Information and Communication Technology Utilization by Small Holder Banana Farmers in Gatanga District, Kenya. *The Journal of Agricultural Education and Extension*, 20(2), 247-26.,
- OECD (2017), Science, technology and industry scoreboard 2017. The digital transformation OECD Publishing, Paris, France. Available at <https://doi.org/10.1787/20725345>.

24. Technical Centre for Agriculture and Rural Cooperation (CTA). (2019). The Digitalization of African Agriculture Report.
25. Verdouw, C., Sundmaeker, H., Tekinerdogan, B., Conzon, D., Montanaro, T. Architecture framework of
26. Wolfert, S., Ge, L., Verdouw, C., & Bogaardt, J.M (2017). Big Data in Smart Farming – A review. *Agricultural Systems*, 153, 69–80
27. World Bank. (2008). Agriculture Development. In *World Development Report, Agriculture for Development*.
28. Zewge, A., & Dittrich, Y. (2017). Systematic mapping study of information technology for development in agriculture (the case of developing countries). *Electronic Journal of Information Systems in Developing Countries*, 82(1), 1–25.
29. Zhang, N., Wang, M., & Wang, N. (2002) Precision agriculture—a worldwide overview. *Computers and Electronics in Agriculture*, 36, 113-132.





This page is intentionally left blank



The State-of-the-Art Machine Learning in Prediction Covid-19 Fatality Cases

By Maleerat Maliyaem & Nguyen Minh Tuan

King Mongkut's University

Abstract- Day by day, the number of confirmed Covid-19 cases significantly increases all over the world. In India, the second wave of coronavirus has come back and created a disastrous impact. On April 3rd, India continuously recorded the highest number of daily cases globally, according to Financial Times, there was a scarcity of crematoriums and burial grounds due to the high number of corpses. The outbreak of death cases was an unprecedented circumstance, hence, there was a shortage of medical necessities. Prediction of death cases could help the government to manage the medical facilities such as beds and oxygen supply for the hospital. Machine learning could be used to analyze and predict fatality cases. PySpark library is used to process raw data and update new data each day, as the library allows the processing of a large amount of raw data efficiently. By using the Naïve Bayes algorithm available in PySpark, the prediction accuracy has increased to 81.3%.

Keywords: *pyspark, machine learning, Naïve bayes, fatality, covid-19.*

GJCST- B Classification: *H.1.2*



THE STATE OF THE ART MACHINE LEARNING IN PREDICTION COVID-19 FATALITY CASES

Strictly as per the compliance and regulations of:



RESEARCH | DIVERSITY | ETHICS

The State-of-the-Art Machine Learning in Prediction Covid-19 Fatality Cases

Maleerat Maliyaem ^α & Nguyen Minh Tuan ^σ

Abstract- Day by day, the number of confirmed Covid-19 cases significantly increases all over the world. In India, the second wave of coronavirus has come back and created a disastrous impact. On April 3rd, India continuously recorded the highest number of daily cases globally, according to Financial Times, there was a scarcity of crematoriums and burial grounds due to the high number of corpses. The outbreak of death cases was an unprecedented circumstance, hence, there was a shortage of medical necessities. Prediction of death cases could help the government to manage the medical facilities such as beds and oxygen supply for the hospital. Machine learning could be used to analyze and predict fatality cases. PySpark library is used to process raw data and update new data each day, as the library allows the processing of a large amount of raw data efficiently. By using the Naïve Bayes algorithm available in PySpark, the prediction accuracy has increased to 81.3%.

Keywords: pyspark, machine learning, Naïve bayes, fatality, covid-19.

I. INTRODUCTION

The world has spent to the heart-rending day when fatalities passed 4 million people while the crisis becoming the race between vaccinating and new dangerous variants. Prediction is another way to control the Covid-19 situation and propose a new method to face the new stage of devastation coronavirus [18]{21}. In paper [1], they used linear regression and polynomial regression to predict the results of fatalities. These two algorithms were applied to find the best fit line to estimate the average values of the two variables. These

algorithms are dependent on the variation and dispersion of the data. The best fit line will divide the data into two parts with the same distance between the values of data from the best fit line. They also used root mean square error to estimate the accuracy of prediction. Root mean square error is a kind of metric to calculate the error when analyzing the data using regression algorithms. Root mean the square error will be calculated as the mean of the values and ensure the distances are the same as the points. The root means square error measures the variation and the concentration of the values around the mean. Many kinds of data could be expressed in Fig 1, the exactness belongs to the distribution of data.

In paper [2], they predicted the outbreak of Covid-19 in Ethiopia by comparing the Support Vector Machine (SVM) model and the Polynomial Regression (PR) model in the ScikitLearn library. The paper showed that SVM gets better performance than PR banked on evaluating graph performance and metric Mean Square Error (MSE), Mean Absolute Error (MAE) [3]{7, 9}. With the same evaluation in paper [1], the results were also depending on the distribution of the data and this evaluation is just counted on the mean of the values that if the data is dense on the prediction, the mean of the values will be closed to the mean of prediction. This calculation usually makes the approximate values instead of exact values.

Table 1: Random Correlation Example for Data

	Total_cases	new_cases	new_cases_smoothed	total_deaths	new_deaths	new_deaths_smoothed
Total_cases	1.000000	0.862925	0.879309	0.984957	0.845896	0.871108
new_cases	0.862925	1.000000	0.989568	0.864804	0.928043	0.922668
_cases_smoothed	0.879309	0.989568	1.000000	0.879013	0.921921	0.937985
total_deaths	0.984957	0.864804	0.879013	1.000000	0.872722	0.898039
new_deaths	0.845896	0.928043	0.921921	0.872722	1.000000	0.976566
new_deaths_smoothed	0.871108	0.922668	0.937985	0.898039	0.976566	1.000000

In this paper, we considered the unformed data with the information in Fig 1. We calculated the correlation between the attributes of data and applied an accuracy metric to evaluate the exact values. We proposed the algorithms could solve with discrete and

unformed data by calculating the correlation shown in Table 1. We defined very strong positive correlation when values are greater than or equal to 0.8, strong positive correlation when values are greater than or equal to 0.6 and smaller than 0.8, weak positive correlation when values are greater than or equal to 0.4, and smaller than 0.6. We omitted no correlation (values are in the interval of -0.4 to 0.4), weak negative correlation (Values are

Authors α σ: King Mongkut's University of Technology North Bangkok, Thailand. e-mails: maleerat.m@itd.kmutnb.ac.th, minh.tuan@itd.kmutnb.ac.th, http://kmutnb.ac.th/

smaller than or equal to -0.4 and greater than -0.6), strong negative correlation (Values are greater than -0.8 to values smaller than or equal to -0.6) and very strong negative correlation (Values are smaller or equal to -0.8). We tried models and chose the metric accuracy to calculate the true prediction and the percentage of the prediction. With this metric, we could evaluate exactly the number of predictions and depicted the records related to prediction. PySpark is one of the branches of Hadoop structure becoming strongly and easily in analyzing the data. With the powerful libraries, PySpark supplies the structure for direct and indirect processing, graph environment with ease of use, short time analyzing the big data. PySpark sponsors many

sections with many kinds of functions such as Spark SQL, DataFrame, Streaming, MLlib, and Spark Core. PySpark could solve with big data and costs less time to analyze the classification problems. Table 2 shows details of the sections and functions in the PySpark library. The steps for analyzing data could not follow the sections but could form the data before applying the sections and functions (Fig 1). The data will be extracted feature and applied to the model to transform to right form data by choosing basic statistics. After that, we could confirm and make the kinds of problems such as classification, regression, or clustering problems. Finally, we applied evaluation metrics to estimate the models (Equations 1-4).

$$Accuracy = \frac{\sum_{i=1}^n T_{iV}}{\sum_{i=1}^n T_{iV} + \sum_{j=1}^m F_{jV}} \quad (1)$$

Where n ; m are numbers of classes, T_{iV} is a true value of prediction at class i ; F_{jV} is a false value of label at class j .

$$Precision = \frac{\sum_{i=1}^n T_{iP}}{\sum_{i=1}^n T_{iP} + \sum_{j=1}^m F_{jP}} \quad (2)$$

Where T_{iP} is the true positive at class i and F_{iP} is false positive at class i . F_{jN} is false negative at class j .

$$Recall = \frac{\sum_{i=1}^n T_{iP}}{\sum_{i=1}^n T_{iP} + \sum_{j=1}^m F_{jN}} \quad (3)$$

$$F_1 - Score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (4)$$

II. LITERATURE REVIEW

Nowadays, machine learning is becoming an essential part of computer science. PySpark is a strong application for analyzing the data with open-source libraries where we can run R, Python, Java, and Scala. PySpark is free for users and easy to use. PySpark supports two strong libraries with Spark MLlib and Spark ML packages where they can solve big data and analyze it in a very short time [17]. However, the processing for analyzing data could follow as Fig 2 shown. We summarized the algorithms used in the PySpark library shown the detail in Table 2.

III. EXPERIMENTS

In this paper, we got data downloaded on June 10th, 2022 from the website <https://ourworldindata.org/covid-deaths> and updated every day (Table 2). The data totally consists of 59 attributes and we also chose the attribute with the

Table 2: Library support in PySpark

MLlib	Sections	Features
Data types	Local vector	The vector is formed by an integer or double or zero-based type. The data can be distributed densely or sparsely.
	Labeled point	A kind of local vector using supervised machine learning algorithms with data is labeled. Labels sometimes are 0 and 1 or start from 0, 1,2,.. The data can be established in dense or sparse distribution.
	Distributed matrix	A kind of local matrix with long rows and columns. It is so difficult that we can't turn the matrix into another format matrix.
Basic Statistics	Summary Statistic	Giving the information of the instance consists of mean, max, min, variance, and nonzeros.
	Correlations	Depend on the input data, the output could be formed double or matrix.
Classification and Regression	Linear Models	Replied to the input data, the output could be formed double or matrix.MLlib supports the classification and regression algorithms. The classification consists of linear support vector and logistic regression. Regression consists of Lasso, and Ridge regression.
	Decision Trees	Solving any kind of classification problems, this ease of use and handle complicated tasks.
	Random Forest	Using the same model with Decision Trees, Random Forest uses the average of the values to improve the exact predictions but sometimes cost more time than Decision Trees
	Naïve Bayes Isotonic regression	Very strongly applied in labeled data and solving classification problems efficiently. It can be usually applied in sparse vectors conveniently.
Feature	StringIndexer	To turn string attributes into label attributes. If the column is a string, we could change it to a string column and label the string column.
	OneHotEncoder	Change a label column to binary column vectors
	VectorAssembler	Combining all kinds of categorical columns to build a vector column for model prediction.
Evaluation metrics	Classification model evaluation	Applied for binary and multiclass classification, the output could show the confusion matrix, accuracy, precision, recall, and F1-measure.
	Regression model evaluation	Applied for predicting continuous values with Mean Square Error, Root Mean Square Error, Mean Absolute Error, and Coefficient of Determinant.



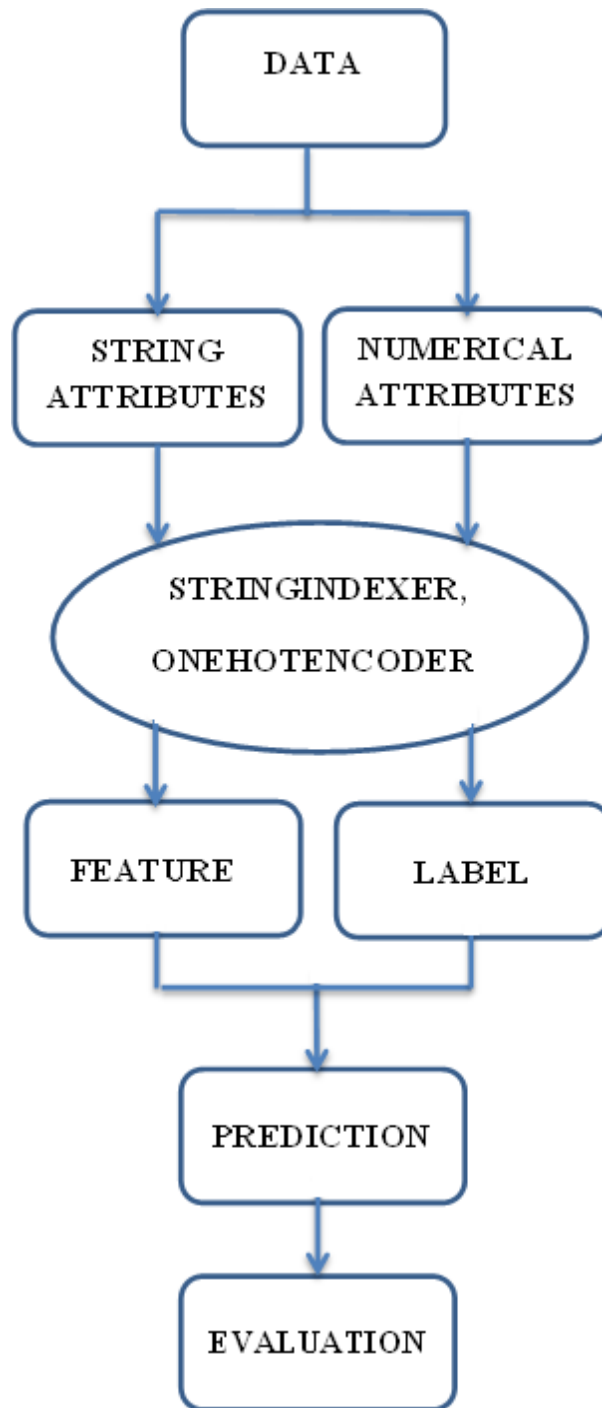


Fig. 1: Steps to Process Data

greatest correlation values in the set of very strong correlation values for building features combining location and total deaths is chosen as labels. The raw data chosen comprises about 208,111 instances and is cleaned by keeping specific character contributes.

As Fig 1 shown, we need to process the data in the right format by using PySpark libraries. The columns selected will be divided into two parts: One part for features and another for labels. We applied StringIndexer to change to the column labeled and applied OneHotEncoder to established binary vector

and after that, we applied VectorAssembler to combine with total cases column to make column features for prediction. We also applied StringIndexer to turn total deaths into a label column for target prediction (see Table 2). Besides metrics accuracy to evaluate the ratio of right targets and total targets, we considered evaluating by Precision, Recall, and F1-score occupied great important units in the medical aspect. Precision is confirmed the rightly positive cases while Recall is to confirm rightly negative cases to decide the right method for curing. F1-score, calculated as the average

of Recall and Precision, is applied to confirm how much Recall is more important than Precision. In the medical branch, it is used to decide prior Recall or Precision to choose an appropriate patients' situation.

Compared to deep machine learning, we also analyze the data when trying with deep learning [8]{13} such as LSTM, and GRU but get the worse results prediction shown such as the time costs too much time (5,435s/step), accuracy for the first step is 0.138 and the second step is 0.1384. The parameters for solving this data are a total of 202,878,594 parameters and the batch size is 1,318 parameters. PySpark has shown better performance with the best accuracy and least time to evaluate.

IV. RESULTS

In this paper, we tried the models in PySpark and choose the models that could analyze the data. After trying the models in Spark.MLlib and Spark.ML, we got the results in Table 3. The results showed that Naïve Bayes has the best performance in predicting fatalities with an accuracy of 0.813. Following that was the Decision Tree model with an accuracy is 0.621. Table 4 shows some example prediction results with the models. Fig 2-3 showed the screen of prediction using Naïve Bayes and Random Forest.

Table 3: Prediction Results for All Models

Models	Accuracy	Precision	Recall	F1-Score
Naïve Bayes	0.813	0.571	0.381	0.457
Random Forest	0.139	0.632	0.003	0.005
Decision Tree	0.621	0.824	0.013	0.026

Table 4: Example Results for Naïve Bayes Prediction

Label	Naïve Bayes	Random Forest	Decision Trees
8.0	5	4	3
20.0	32	3	16
23.0	16	1	8
38.0	28	31	12
43.0	46	3	41

V. CONCLUSION

To aim with getting the best prediction for Covid-19 fatalities, we applied Spark.MLlib and Spark.ml to get the best result in Naïve Bayes model [14]{16}. We also try with deep machine learning like LSTM, GRU but get no better answers. With this paper, we hope to have a good prediction in India and other countries getting the Covid-19 cases increasing every day. With this result, we hope we and other researchers could get more information to continue facing the Covid-19 tornado. This result is also the basic report supplied for the government in repairing the utilities for Covid-19 cases. This also proposes a way to solve big data in the new technology era with unformed data.

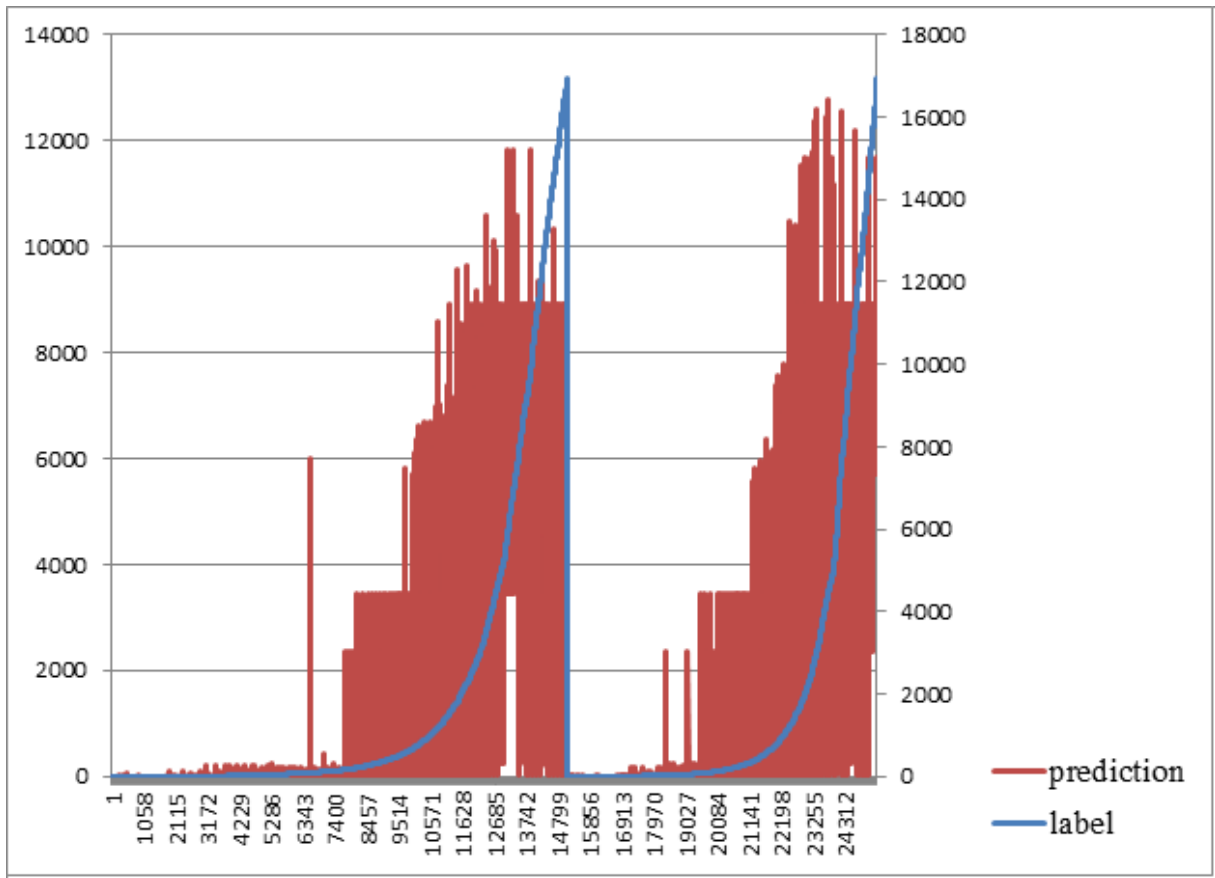


Fig. 2: A Prediction using Naive Bayes

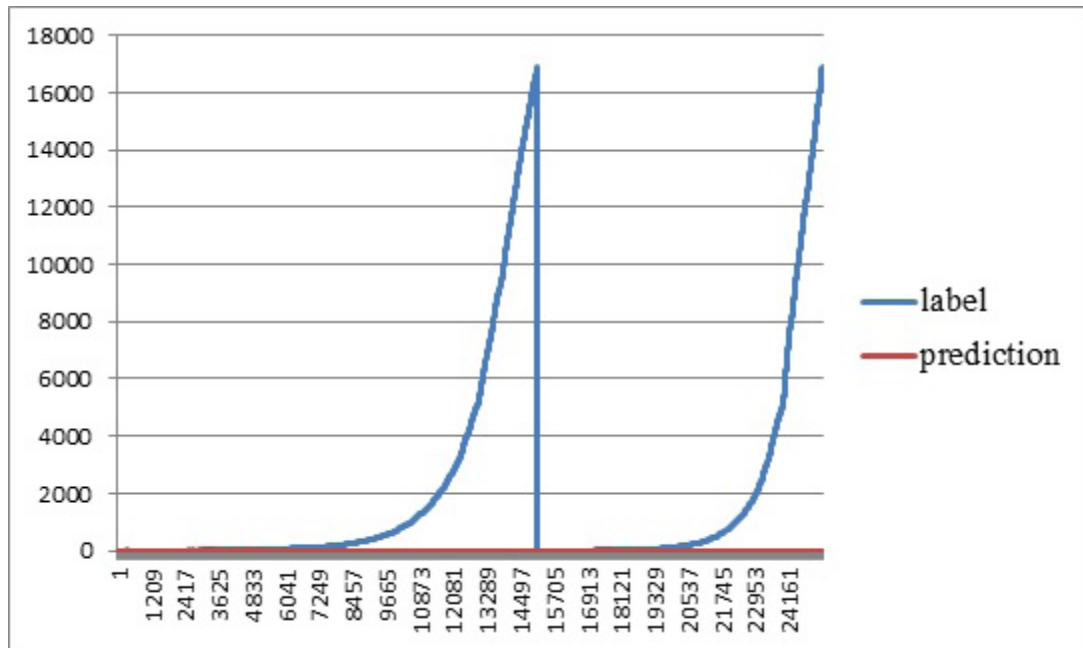


Fig. 3: A Prediction using Random Forest

REFERENCES RÉFÉRENCES REFERENCIAS

1. Manpinder Singh, Saiba Dalmia, Prediction of number of fatalities due to Covid-19 using Machine Learning, IEEE 17th India Council International Conference (INDICON), 2020.
2. Sirage Zeynu Ahmed, Analysis and forecasting the outbreak of Covid-19 in Ethiopia using machine learning, .
3. Tamer Sh. Mazen, A novel machine learning based model for COVID-19 prediction, International Journal

- of Avanced Computer Science and Applications, 2020.
4. Roseline Oluwaseun OGUNDOKUN, Joseph Bamidele AWOTUNDE, Machine learning prediction for Covid 19 pandemic in India, 2020.
 5. Sudhir Bhandari, Ajit Singh Shaktawat, Amit Tak, Bhoopendra Patel, Jyotsna Shukla, Sanjay Singhal, Kapil Gupta, Jitendra Gupta, Shivankan Kakkar, Amitabh Dube, Logistic Regression Analysis to Predict Mortality Risk in COVID 19 Patients from Routine Hematologic Parameters, *Ibnosina Journal of Medicine and Biomedical Sciences*, 2020.
 6. Arjun S. Yadaw, Yan-chak Li, Sonali Bose, Ravi Iyengar, Supinda Bunyavanich, and Gaurav Pandey, Clinical predictors of COVID-19 mortality: development and validation of a clinical prediction model" in *Lancet Digit Health*, 2020.
 7. Shreshth Tuli, Shikhar Tuli, Rakesh Tuli, Sukhpal Singh Gill, predicting the growth and trend of Covid-19 pandemic using machine learning and cloud computing, *Elsevier public health emergency collection*, 2020.
 8. Mohammad Behdad Jamshidi, Ali Lalbakhsh, Jakub Talla, Zden_ek Peroutka, Farimah Hadjilooei, Pedram Lalbakhsh, Morteza Jamshidi, Luigi La Spada, Mirhamed Mirmozafari, Mojgan Dehghani, Asal Sabet, Saeed Roshani, Sobhan Roshani, Nima Bayat-Makou, Bahare Mohamadzade, Zahra Malek, Alireza Jamshidi, Sarah Kiani, Hamed Hashemi-Dezaki, and Wahab Mohyuddin, *Artificial Intelligence and COVID-19: Deep Learning Approaches for Diagnosis and Treatment*, *IEEE public health emergency collection*, 2020.
 9. Sina F. Ardabili, Amir Mosavi, Pedram Ghamisi, Filip Ferdinand, Annamaria R. Varkonyi-Koczy, Uwe Reuter, Timon Rabczuk, and Peter M. Atkinson, *COVID-19 Outbreak Prediction with Machine Learning*, *MDPI*, 2020.
 10. Mohammadreza Nemat, Jamal Ansary, and Nazafarin Nemat, *Machine-Learning Approaches in COVID-19 Survival Analysis and Discharge-Time Likelihood Prediction Using Clinical Data*, *CellPress*, 2020.
 11. Batista AFM, Miraglia JL, Donato THR, Chiavegatto Filho ADP, *COVID-19 diagnosis prediction in emergency care patients: a machine learning approach*, *CSH*, 2020.
 12. Hongwei Zhao, Naveed N Merchant, Alyssa McNulty, Tifiany A Radclifi, Murray J Cote, Rebecca Fischer, Huiyan Sang, Marcia G Ory, *COVID-19: Short term prediction model using daily incidence data*, *Plos One Collection*, 2021.
 13. Rajan Gupta, Gaurav Pandey, Poonam Chaudhary, Saibal K. Pal, *Machine Learning Models for Government to Predict COVID-19 Outbreak*, *ACM Journal*, 2020.
 14. Kelly, Anthony; Johnson, Marc Anthony, *Investigating the Statistical Assumptions of Naïve Bayes Classifiers*, *55th Annual Conference on Information Sciences and Systems (CISS)*, 2021.
 15. Sharmila, B S; Nagapadma, Rohini, *Intrusion Detection System using Naive Bayes algorithm*, *IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE)*, 2019.
 16. B S Sharmila, Rohini Nagapadma, *Intrusion Detection System using Naive Bayes algorithm*, *IEEE International WIE Conference on Electrical and Computer Engineering*, 2019.
 17. Tuan Nguyen M, Meesad P, Nguyen Ha H.C, *English-Vietnamese Machine Translation Using Deep Learning*, *Recent Advances in Information and Communication Technology*, 2021, https://doi.org/10.1007/978-3-030-79757-7_10.
 18. Maliyaem M, Tuan Nguyen M, Lockhart D, Muenthong S, *A Study of Using Machine Learning in Predicting COVID-19 Cases*. *Cloud Computing and Data Science*, 2022.
 19. Tuan Nguyen M, Phayung Meesad, *A Study of Predicting the Sincerity of a Question Asked Using Machine Learning*, *5th International Conference on Natural Language Processing and Information Retrieval (NLPiR)*, 2021.
 20. Tuan Nguyen M, *Machine Learning Performance on Predicting Banking Term Deposit*, *International Conference on Enterprise Information Systems (ICEIS)*, 2022.
 21. Siti NurhidayahSharin, Mohamad KhairilRadzali, Muhamad Shirwan Abdullah-Sani, *A network analysis and support vector regression approaches for visualizing and predicting the COVID-19 outbreak in Malaysia*, *ScienceDirect*, 2022.

GLOBAL JOURNALS GUIDELINES HANDBOOK 2022

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

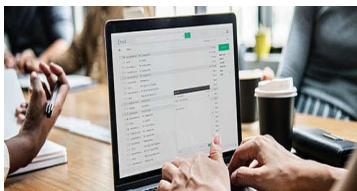
FUTURE WORK

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
<p>\$4800 lifetime designation</p> <hr/> <p>Certificate, LoR and Momento 2 discounted publishing/year Gradation of Research 10 research contacts/day 1 GB Cloud Storage GJ Community Access</p>	<p>\$6800 lifetime designation</p> <hr/> <p>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</p>	<p>\$12500.00 organizational</p> <hr/> <p>Certificates, LoRs and Momentos Unlimited free publishing/year Gradation of Research Unlimited research contacts/day Unlimited Cloud Storage Online Presense Assistance GJ Community Access</p>	<p>APC per article</p> <hr/> <p>GJ Community Access</p>



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 through 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
<i>Abstract</i>	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
<i>Introduction</i>	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
<i>Methods and Procedures</i>	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
<i>Result</i>	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
<i>Discussion</i>	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
<i>References</i>	Complete and correct format, well organized	Beside the point, Incomplete	Wrong format and structuring



INDEX

A

Ambimorphic · 1, 3
Annealing · 1, 4
Appraisal · 24
Archetypes · 4

C

Ciphertext · 45
Concatenated · 41, 43

E

Eavesdropping, · 40
Eigenvector · 35
Emulating · 3, 4
Enormous · 30
Enumerated · 4

F

Federates · 34

H

Heterogeneous · 4, 21
Heuristic · 1, 41
Hierarchical · 1

I

Iterations · 30

L

Latency · 35, 36, 37, 38, 42

M

Malicious · 41, 46
Manipulate · 35
Mechatronics, · 13
Misallocation · 33

O

Orchestration · 32, 33, 34, 40

P

Pioneer · 6
Proliferation · 48, 51
Pseudonym · 42, 43
Psychoacoustic · 1

Q

Quagmire · 1
Quantum · 23

R

Reencrypts · 42
Referred · 22
Roughly · 48

S

Skeptics · 3
Sought · 50
Stringindexer · 57, 58

V

Vehicular · 40, 41, 46
Vertex · 6
Vulnerability · 13



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