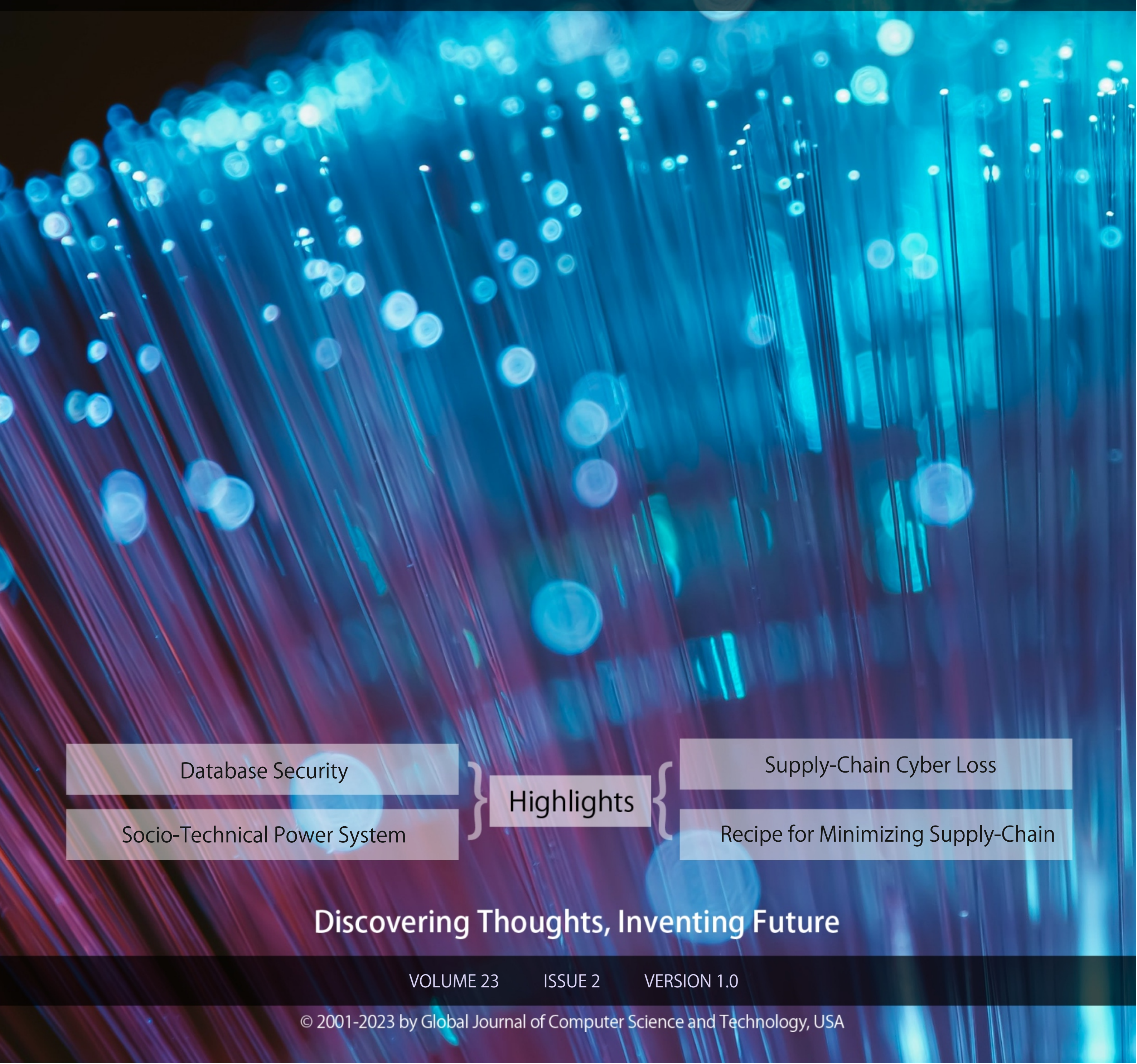
Online ISSN : 0975-4172
Print ISSN : 0975-4350
DOI : 10.17406/GJCST

Global Journal

of Computer Science and Technology: E

Network, Web & Security



Database Security

Socio-Technical Power System

Highlights

Supply-Chain Cyber Loss

Recipe for Minimizing Supply-Chain

Discovering Thoughts, Inventing Future

VOLUME 23 ISSUE 2 VERSION 1.0

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

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

Volume 23 Issue 2 (Ver. 1.0)

Open Association of Research Society

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

Global Journals Inc.

*(A Delaware USA Incorporation with "Good Standing"; **Reg. Number: 0423089**)*
Sponsors: *Open Association of Research Society*
Open Scientific Standards

Publisher's Headquarters office

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

Offset Typesetting

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

Packaging & Continental Dispatching

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

Find a correspondence nodal officer near you

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

eContacts

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

Pricing (Excluding Air Parcel Charges):

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

Editorial Board

Global Journal of Computer Science and Technology

Contents of the Issue

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 23 Issue 2 Version 1.0 Year 2023
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Board Recipe for Minimizing Supply-Chain Cyber Loss

By Jason K. Deane & Wade H. Baker

Introduction- After attending corporate board meetings for approximately 85 different Fortune 500 organizations and listening to CEOs and CISOs discuss cyber risk in supply chains; and after then meeting with many of them personally, we came away with three primary takeaways. First, the main cybersecurity interest of most upper-level managers is primarily in avoiding major negative consequences (i.e., Black Swans) to their firms. Second, over 90% of corporate board members we have met with are either neutral or not confident with their security program's effectiveness. But finally, and of major concern to us, was the observation that CISOs primarily tell their boards "anecdotes" or "stories," and they do not present boards with any substantive and specific direction to avoid supply-chain cyber loss.

GJCST-E Classification: FOR Code: 150314

A Board Recipe for Minimizing Supply-Chain Cyber Loss

Jason K. Deane [α] & Wade H. Baker [σ]

I. Introduction

After attending corporate board meetings for approximately 85 different Fortune 500 organizations and listening to CEOs and CISOs discuss cyber risk in supply chains; and after then meeting with many of them personally, we came away with three primary takeaways. First, the main cybersecurity interest of most upper-level managers is primarily in avoiding major negative consequences (i.e., Black Swans) to their firms. Second, over 90% of corporate board members we have met with are either neutral or not confident with their security program's effectiveness. But finally, and of major concern to us, was the observation that CISOs primarily tell their boards "anecdotes" or "stories," and they do not present boards with any substantive and specific direction to avoid supply-chain cyber loss. We believe this is unfortunate because, based on a different set of experiences we have had, namely performing several thousand forensic studies, including about one thousand for the U.S. Secret Service-most with about 100 page or more reports, we believe corporate boards can take specific reasoned actions and thereby reduce significantly their organization's exposure to, and subsequent losses from, supply-chain cyber-attacks.

To state the situation in different terms, we have found that, yes, *being in a supply chain increases your risk*. In particular, our data show that under average circumstances, by joining a supply chain, a firm increases its risk by 70%. But, *yes, it is also possible to effectively mitigate cyber risk, and if a firm doesn't, it may really pay for that non-action*. Most importantly, we have learned that *how a firm manages its risk given its membership in a supply chain does make a difference*. And we have developed a recipe for managing this supply chain cyber risk. We believe our results completely agree with the framework established by Parenty and Domret [HBR, 2019], but we in fact extend their findings to a supply-chain context. We believe corporate boards can, and need, to be involved in mitigating cyber risk and that the actions to be taken go significantly beyond the recounting of anecdotes and "stories," as we will shortly explain.

Very briefly, how did we arrive at this recipe? In order to understand and extrapolate from the two thousand or so forensic cyber cases we investigated, we noticed very early on that we needed to come up with a new way of recording the cyber causes and effects of supply chain risk and consequences we were seeing. Thus, we developed the *A4 Threat Model*, which provides a robust schema for describing security incidents in a structured and repeatable manner. Specifically, the A4 model records data in three major sections-Victim, Event (represented as the "4A's"-*Actor*, *Action*, *Asset*, *Attribute*), and Impact-along with some miscellaneous context about the incident itself. Thus, the A4 model essentially categorizes cyber possibilities into 378 (3 actors, 7 actions, 6 assets, and 3 attributes) distinct threat events.

The A4 model is now an industry standard; it aims to provide a database for an information security Decision Support System. With this threat model, we can constructively and cooperatively learn from our experiences to better measure and manage risk, which is especially important in tightly integrated and highly collaborative supply networks. Boards do not need to get involved in the intimate details, such as which of the 378 specific possible scenarios they need to worry about. Rather, *our* studying 2,000 forensic episodes and categorizing each into the 378 possible types, has led us to garner insight, which we are now able to both generalize and yet detail how a corporate board should get involved to minimize organizational risk.

II. The Board Recipe

Here is the basic recipe for a board to best manage its organization's supply-chain risk.

a) Establish your Context

Deane et al. [2022] and Parenty and Domret in a recent *Harvard Business Review* [2019] article have argued that corporate management is *not* involved, but *should get involved*, in managing corporate cyber risk in general. Then these authors provided a very insightful approach whereby they specified what they call a four-step *cyber threat narrative* explaining how the board should get involved. First, they said, the board needs to determine the organization's critical business activities and risks. This would involve interviewing company leaders, examining statements of company risk tolerance, looking at company potential sources of

Author α: Department of Business Information Technology Virginia Tech, Blacksburg, VA 24061 USA. e-mail: jdeane1@vt.edu
Author σ: Department of Business Information Technology Virginia Tech, Blacksburg, VA 24061 USA. e-mail: wbaker@vt.edu

major revenue, etc. Then the board must ascertain essential systems that support these critical activities; this involves getting IT to catalogue computer systems and the functionality they supply for each critical activity or risk. Thirdly, they should determine the types of cyber attacks that might harm these support systems; this involves studying and coming to understand what an adversary needs in order to pull off an attack. And finally, the board should have generated for them a list of firms or individuals most likely to be possible cyber adversaries. Parenty and Domret note that company leaders and operations staffers involved in critical business activities are best at identifying potential adversaries.

Thus, we specify that the first step in a Board recipe to minimize cyber risk in a supply chain is just Parenty and Domret's first step, namely, *as certain the threats to your organization's key activities*.

Our second step regarding cyber risk in a supply chain is for the board to have determined for it *who is in the organization's first tier of supply-chain partners*. If you are in a supply chain, you are exposed to three additional types of threats beyond the *direct threats* you are subjected to when not belonging to a chain. We have observed that the biggest by far of the three new types of threats you face beyond the direct attack when you join a chain is the *partner vector* threat. The board should be aware, however, that even more significant than the new partner vector threat is the (old) direct threat. This direct threat still will constitute most of your risk, so you must continue to follow the Parenty-Domret advice as a first step. But a vector threat occurs because you are electronically connected to your supply-chain partners, and so you may experience the results of an attack because you are just connected to some other firm with a whole different set of critical business activities and risks, cybersecurity types, and cyber adversaries.

Depending on how big a supply chain you belong to, you may have first-tier partners, who are in turn connected to *their* first-tier (and your second-tier) partners, who in turn are connected to *their* first-tier (and your third-tier) partner. We have observed over the years that focusing on just your first-tier of partners will mitigate much of your risk.

Therefore, the board must expand its focus beyond just the *organization's* four aspects of its own cyber narrative (its set of key activities, associated essential support systems, associated collection of types of possible cyber-attacks, and finally its cyber adversaries). The board must also attempt to gain insight either directly from its supply-chain partners if they are willing and able to do so; or the board must have generated for it an in-house estimate of each first-tier partner's cyber narrative. Then, with these inputs, the board should focus to the extent possible on the set of four factors for each of its first-tier suppliers as for itself.

In short, an organization should first establish an extended context consisting of itself and its first-tier partners.

b) Reduce Vector Attacks

If an organization has a breach of any type or source, there is a probability that the breach will "propagate" to all partners in the network connected to the original victim. Thus, by connecting in a supply chain, a firm may incur the "side-effects" of any of its partners being breached; this type of breach is called a *partner vector breach*, or a *vector breach* for short.

There are quite a few factors that influence an organization's monetary loss from a vector attack, including its *IT* integration level; information sharing: scope/confidentiality; information sharing: degree; *its* security posture to each partner; and its partners' security postures facing them. However, we have found from our forensic analyses that, *of all these factors*, in general the most effective way to mitigate vector loss is to establish a *strong security posture* that blocks possible interference from each partner due to the electronic conduit between you two. In the many cases we examined, we found that cyber loss can vary from 1.8 times the normal value down to 0.5 times the normal risk due to this one factor alone.

A well-known example illustrating a vector attack is the case of Target and an HVAC supplier that Target also made a connected partner. In short, Target allowed an HVAC supplier in 2013 to connect electronically to it, and as a result, Target was hacked after Thanks giving and before Christmas by a third party that got into Target via the HVAC connection. The personal information (including credit card numbers) of approximately 40 million customers led to losses to Target estimated as high as $300M [Krebs, 2014] [Lynch, 2017].

In summary, *a corporate board should make sure, particularly for its supply-chain partners for whom it has inadequate information on their cyber narratives, that its security posture facing each of those partners is strong.* This is an organization's best first step in reducing partner vector breaches.

There is one more issue regarding reducing vector attacks that should provide a general caveat to a board: *The industry to which a partner belongs will affect the type of attack you experience*.

We have plotted in Figure 1 the types of cyber-attacks *experienced* over the years in various industries. Each dot in Figure 1 represents an industry subsector identified by a three-digit North American Industry Classification System (NAICS) code. Subsectors within the same higher-level sector are grouped by color (i.e., several retail (44x) subsectors in the upper right are all grey). The size of the dot corresponds to the number of breaches recorded for that subsector (larger = more). The distance between the dots shows how breaches in one subsector compare to that of another. If dots are close together, it means breaches in those subsectors share similar A4 Threat Model characteristics (in terms of actors, actions, assets, and attributes). If far away, it means the opposite. In other words, subsectors with similar breach profiles appear closer together.

Now, for example, suppose you are an organization in the industry *Manufacturing* and that you have insured that you are well protected against the type of threats experienced by firms in the center of Figure 1. Then if you join a supply chain with a firm that provides *Transportation and Warehousing (Distribution)*, you have now become exposed to a whole new potential category of threats and attacks because, as the figure shows, Transportation and Warehousing is in the upper left corner of the cluster plot of threat types.

As an organization, you most likely will *not* be able or even want to exclude another organization because of the industry to which it belongs; in fact, its industry is probably why you want that organization in your chain. So the caveat we offer here is that, as a board, you should be aware that if you have supply-chain members in portions of Figure 1 distant from your industry, you will want to pay extra attention to those members and determine the types of attacks more common to them than to you.

c) Simplify Electronically the type of Chain to which you belong

The next step in the recipe to cyber-risk success is that boards should insist that the information sharing structures of organizations in the chain, i.e., the electronic connections between its own organization and all partners, should be simplified as much as possible.

In our experiences, we have observed cyber-attacks on supply chain members connected electronically in many different configurations. The literature lists and names some common connectivity schemes, and we have shown three of the most common in Figure 2. From left to right in that figure are examples of "linear (sequential)," "hub-and-spoke," and "reciprocal" connectivity strategies. [See, e.g., Liu and Kumar (2003)]. Note for example, that in the reciprocal connectivity chain, essentially everyone is connected to everyone else; this results in way more connections than in, say, a simple linear (sequential) arrangement. Of course, it must be recognized that oftentimes the type of connectivity must be specified due to business purposes other than cyber considerations. But what we have observed over the years from our forensics is that the way firms connect, taken together with their security postures, greatly affects cyber loss. For example, we have seen five firms connected reciprocally with poor security posture experiencing over one billion dollars more loss over five years than five similar firms connected with strong security.

In short, *a corporate board should thus, to the extent possible, reduce the number of inter-firm electronic connections.* If it is absolutely necessary to connect everyone to almost everyone else, the board must insist to IT that *its security posture facing every such partner is as strong as possible.*

d) Force your Partners to be Responsible

There is a somewhat surprising piece of evidence that makes this final measure of the board recipe not only an important step, but in fact, an essential one. The action? to the extent you are able, *force your partners to improve their security posture toward you in particular, and also toward the world in general*. Our experience has clearly demonstrated that, when I am in a supply chain, my risk as a firm is *not* the same as all my partners' risk. In fact, we have seen over and over that *risk in a chain is not commensurate with culpability*. Our findings clearly indicate that the firm that causes most of the risk does *not* necessarily incur the most risk. That is, in some cases, some other firms incur more risk than even the "weakest link."

It thus is worthwhile for a firm to help-or even demand that (if possible)-its partners obtain a strong security posture. This recommendation is not unlike what occurred in the early dot-com era when large firms like Wal-Mart required and/or incentivized suppliers to modernize IT systems to reduce overall risk.

III. Conclusions

As Parenty and Domret [2019] and Deane et al. [2022] have argued, historically, corporate management has *not* been involved, but now can and *should get involved*, in managing corporate cyber risk in general. This present work shows that extending the Parenty-Domret work to supply chains is also an activity that corporate boards can and should be involved in.

In particular, this paper suggests the manner in which boards should take leadership in order to reduce cyber attacks on its organization due to its membership in a supply chain:

First, Eextend your Parenty-and-Domret Context

Now you must also include your first-tier partners in your "context."

Next, Reduce your Vector Threats

The way to do this is to establish a *strong security posture* that blocks possible interference from each partner due to the electronic conduit between you two. Also watch out for industries distant from yours in an A4 sense (see Figure 1).

Third, Simplify Electronically your Information Sharing

Reduce the connectivity (see Figure 2) among chain members as much as practical. When denser connectivity is necessary for other than cyber reasons, be especially careful, once again, to mandate that the appropriate IT groups increase your security facing each firm.

Finally, "force" Partners to be Responsible

Since cyber loss is not proportional to cyber culpability, the board should help and/or force partners to improve their security posture toward both you and the world in general.

References Références Referencias

1. Deane, J., Baker, W. and Rees, L. (2022). "Cybersecurity in Supply Chains: Quantifying Risk,"
2. *Journal of Computer Information Systems*, available online: https://www.tandfonline.com/doi/full/10.1080/08874417.2022.2081882, accessed 14 December 2022.
3. Krebs, Brian. (2014). "Target Hackers Broke in Via HVAC Company, "https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/, accessed 07December 2019.
4. Liu, E. R. and Kumar, A., 2003, "Leveraging Information Sharing to Increase Supply Chain Configurability." In *Twenty-Fourth International Conference on Information Systems*, 523–537.
5. Lynch, Vincent (2017), "Cost of 2013 Target Breach Nears $300 Million, "https://www.thesslstore.com/blog/2013-target-data-breach-settled/, accessed 07 December 2019.
6. Parenty, Thomas J., and Domret, Jack J., 2019, "Sizing up Your Cyber Risks, "*Harvard Business Review*, November-December.

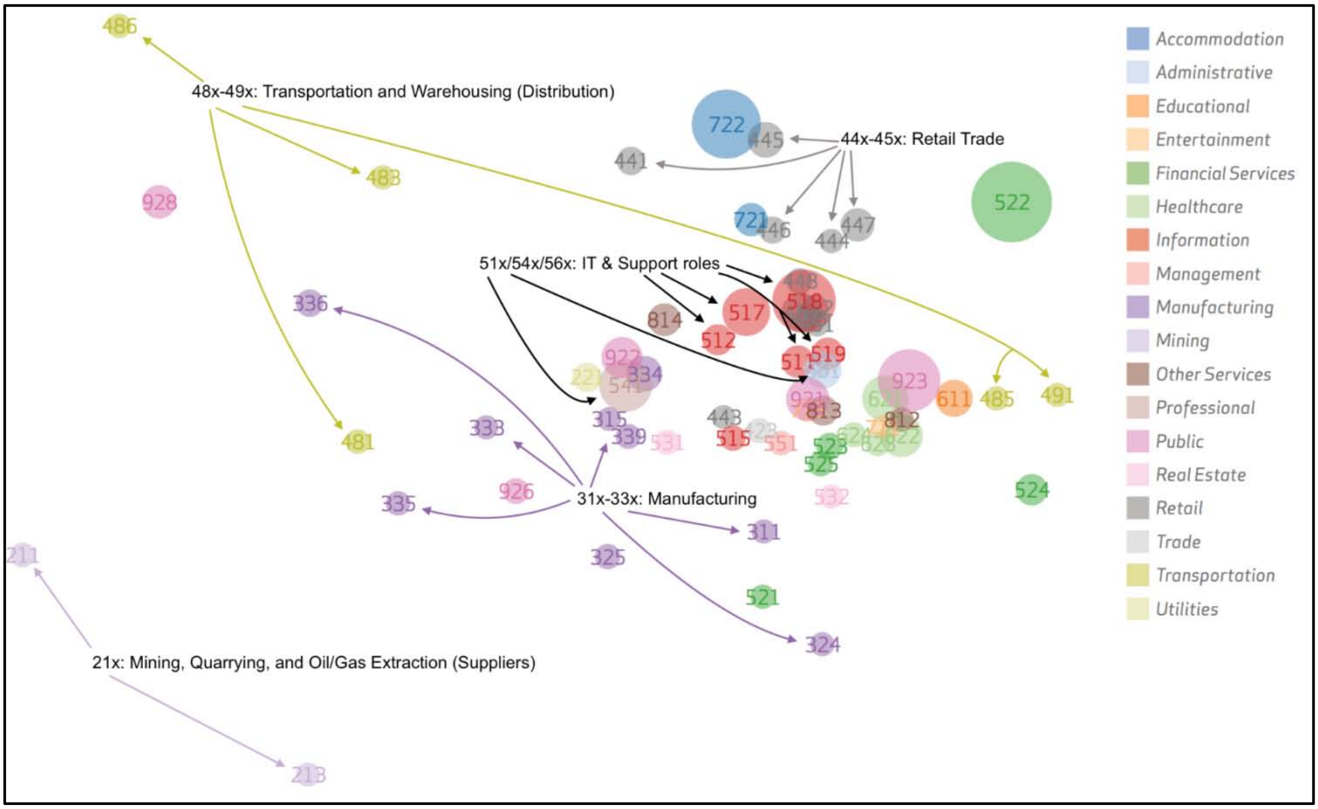


Figure 1: Cluster Analysis Showing Risk Profiles by Industry

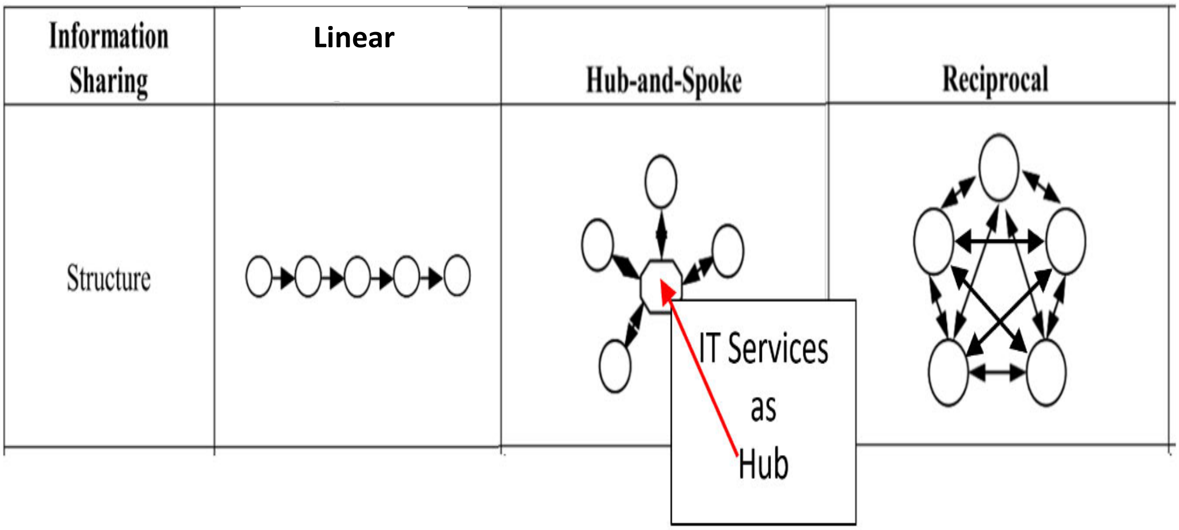


Figure 2: Three Basic Information Sharing Structures Commonly Recognized in the Supply Chain Management Literature. Taken from Liu and Kumar (2003)

This page is intentionally left blank

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 23 Issue 2 Version 1.0 Year 2023
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Database Security

By Vineel Patel & Akanksha Kulkarni

Ajeenkya DY Patil University

Abstract- A database management system is frequently used by users to handle data protection, which is at the core of many security systems. The security of database management systems is the main topic of this essay, which serves as an illustration of how application security may be planned and implemented for certain tasks. Due to the fact that databases are more recent than programming languages and operating systems, there is currently a lot of interest in DBMS Security. Many commercial and governmental organizations depend on databases because they store data in a way that makes retrieving and maintaining it simple and effective. Because databases are a favorite target for attackers, their structure and contents are regarded as significant company assets that must be carefully protected. Similar to other computing systems, databases have some fundamental security requirements. Access control, excluding erroneous data, user authentication, and reliability are the main issues. The problems and dangers to database security are discussed in this paper.

Keywords: attack, database security. threat, integrity.

GJCST-E Classification: LCC: QA76.9 .A25 D33

Database Security

Vineel Patel α & Akanksha Kulkarni σ

Abstract- A database management system is frequently used by users to handle data protection, which is at the core of many security systems. The security of database management systems is the main topic of this essay, which serves as an illustration of how application security may be planned and implemented for certain tasks. Due to the fact that databases are more recent than programming languages and operating systems, there is currently a lot of interest in DBMS Security. Many commercial and governmental organizations depend on databases because they store data in a way that makes retrieving and maintaining it simple and effective. Because databases are a favorite target for attackers, their structure and contents are regarded as significant company assets that must be carefully protected. Similar to other computing systems, databases have some fundamental security requirements. Access control, excluding erroneous data, user authentication, and reliability are the main issues. The problems and dangers to database security are discussed in this paper.

Keywords: attack, database security. threat, integrity.

I. Introduction

A database management system is frequently used by users to handle data protection, which is at the core of many security systems. In order to be more efficient and in line with new and revised aims, databases are crucial to many commercial and government organizations [1] Any firm should improve database security in order to conduct its operations more efficiently. The different dangers put the organization's integrity of data and access in peril. Threats may be caused a software action that is not permitted [1] or by an external force like a fire or a power failure. The majority of the database contains user-sensitive information that is susceptible to hacking and misuse [3]. In order to preserve the data's accuracy and make sure that their systems are continuously watched to deter malicious intrusions from outsiders, businesses have greater control. Due to the rapid growth of technology, the creation of new forms of communication, the globalization of some aspects of society, and the reliance on networks for the transmission of different types of data, this data is divided into numerous categories, most notably. Information about development: Information on development is another name for it. This category covers knowledge gleaned by reading books and articles, which allows one to pick up a variety of contemporary concepts and information meant to advance one's degree of scientific understanding, and widen his field of thought [7]. Achievement Details: An individual's motivation to finish and complete to the best of his ability-and ultimately to make the right decision-comes from learning new terminology and concepts.

- *Education-Related Information:* This is what students learn while sitting in study chairs during all phases of their education, and the curricula serve as the source of this knowledge. Intellectual data: A collection of presumptions and hypotheses concerning a possible connection between the aspects of an issue.
- *Research Information:* This type of information, which can come from either the scientific or literary fields, depends on doing experiments and research to get the essential data.
- *Systematic Stylistic Data:* This category contains all data pertaining to scientific techniques that provide the researcher the chance to conduct the study with great accuracy. Informative incentives, information about politics. Information for guidance, information about philosophy. All of this has increased the possibility of this data being leaked and being accessed by the wrong persons or rivals, making it vital to maintain information security [8]. Information security is the complete control of information, including deciding who will receive it, deciding who has access to it, and using a variety of technologies to ensure that it is not breached by anyone. Its significance grows as it protects private information as well as crucial information like customer accounts in banks. The Internet frequently has a wide range of vulnerabilities that allow unauthorized users to access this data. These vulnerabilities include programmatic mistakes that programmers make when creating networks or designing various applications, such as mistakes in how the application handles incorrect entries or because of poor memory distribution, as there are many programmers who create programs to penetrate systems and search for their weaknesses.
- *Physical Protection Measures:* There are a number of straightforward measures that must be taken to maintain the security of information, such as keeping the computer in a secure location and setting a password to prevent tampering by intruders. The password should also contain letters, numbers, and symbols. Predict them and modify them frequently.

Author α: School of Engineering Ajeenkya DY Patil University Pune, India. e-mail: vineetp91695@gmail.com

Author σ: Pro. School of Engineering Ajccnkya DY Patil University Pune, India. e-mail: facultyit478@advnu.edu.in

Network filters and servers both use firewalls, which are installed there depending on the requirements of each.

- *Encryption:* There are several protocols created to encrypt data, preventing anybody who gets it from comprehending it. The complexity of this encryption varies. The receiving device for this data is responsible for encryption and, of course, for maintaining the decryption key.
- *Data monitoring (Packet Sniffers):* There are many applications that are able to know the movement of data coining out, and entering the network, and by analyzing it, it is possible to reach the breaches that occurred to this network, and know its location. The greater the importance of data and its confidentiality, the greater the means used to protect it, from material and software, for example, server devices are placed in a place protected in various physical ways, including guards [9, 10],

In this article, we thoroughly examine the information structure threads and give an overview of the network's current security threads. We started by outlining the many kinds of threads that are currently known. We have examined the many approaches that might be used to integrate the database's security threads into the application and identified the tactics that could be used to each approach. Database security dangers and challenges were covered in Section II, and in Section III, we discussed security threats that can come from one or more of the following sources. We discussed the difficulties with database security in section IV. Additionally, we described the various threats to database security in section V and their respective countermeasures.

II. Threats of Database Security

Due to its extensive use, database security challenges have become more complicated. Databases are a company's key resource, thus procedures and regulations need to be in place to safeguard the security and precision of the data they hold. Additionally, because of the internet and intranets, database access has become more commonplace, boosting the risk of unwanted access. Database security's goal is to shield a database against theft or intentional loss. These dangers put the data's dependability and integrity at risk. Database security- permits or prohibits users from making changes to the database.

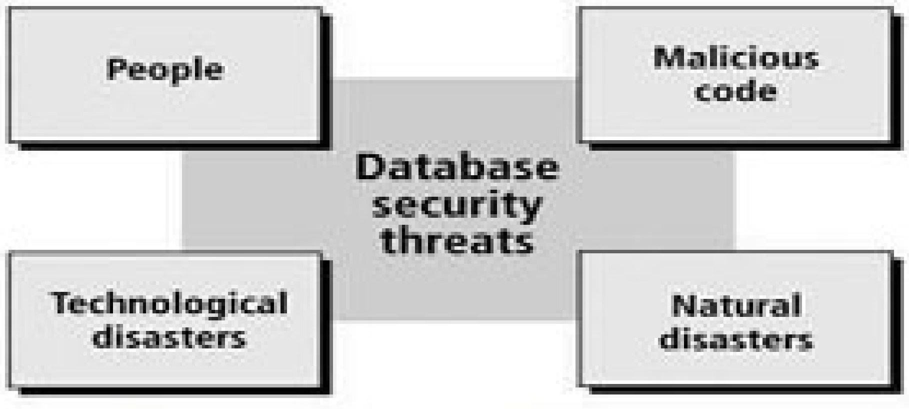


Figure 1: Threats of Database Security

Database systems are at various risks, such as the excessive abuse of privilege Users may abuse their privileges for malevolent purposes if they are given database access rights that go beyond what is necessary for their job function [3], a poor audit trial is another danger. This is a result of internal organizational system weaknesses. This is a result of a weak deterrent system one other issue with database security is the denial of service. On many levels, a weak database audit policy poses a major risk to the firm. The issue of database insecurity is also posed by inadequate authentication systems and techniques. By stealing or otherwise gaining login credentials, attackers can pretend to be authorized database users thanks to weak authentication systems. Therefore, in order to overcome these issues, strong authentication is necessary. [4]

III. Database Security Requirments or Challenges

There are three different degrees of abstraction available for the database. An internal dimension, which represents the actual storage of the database and the physical processing of the data, is typically introduced, along with a three-level viewpoint.

An objective level (or view level), establishes the perspectives that various users or programs have on the stored data, and a logical (or conceptual level) level that gives users a high-level understanding of the physical reality that the database reflects. At this time, just a portion of the complete database is specified. The internal dimension converts the data model's abstract structures into representations of the real operating system structures. Given that all hazards are external, it is standard practice for enterprises to secure the enterprise at the network level. But up to 50% of network intrusions, according to CERT's yearly report, originate within. In fact, this is the reason why many firms arc installing a second layer of protection that uses cutting-edge technology to protect databases. The quality of the data is thought to be a sign of the importance placed on it by its user while protecting data privacy from security assaults. Data responsiveness should be considered for a number of reasons [12].

- A data's meaning itself may be so sensitive or secret that it gets exposed.
- The source of a piece of data may point to the requirement for secrecy.
- The particular quality or history could have been viewed as weak.
- Any data may become vulnerable in the presence of additional data even when it is not vulnerable on its own.

The primary technological components that have a big impact on organizations today arc the specifics and the general concerns with cyber management. The safely of the server might be jeopardized by accessing or changing private data, etc. Reducing the website's functionality or seriously tarnishing the client’s and industry's credibility.

Database systems have similar fundamental security needs as other computer systems. Access control, excluding erroneous data, user authentication, and dependability are the main issues.

a) *Physical Database Integrity:* A database's data arc resistant to physical issues like power outages, and if the database is destroyed by a disaster, it may be rebuilt.
b) *Logical Database Integrity:* The database's structure has been maintained. A database's logical integrity ensures that changing the value of one field won't change the values of any different fields.
c) *Audit Capability:* It is possible to keep tabs on what or who has accessed the database's components.
d) *Access Management:* Only permitted data may be accessed by a user, and different people could only be able to view certain channels
e) *User Authentication:* User authentication ensures that each user can be positively recognized I or both the audit trail and access to specific data.
f) *Availability:* The full database is accessible to users, as well as the information for which they have been given authorization.

IV. Databasc Security Guidelines

Users must have confidence in the veracity of the data values if a database is to act as a central repository for data. This requirement indicates that the database administrator must be certain that only authorized users are carrying out modifications. The DBMS could need stringent user authentication, A DBMS may, for instance, demand that a user passes both the required password and time-of-day checks. The operating system's built-in authentication is supplemented by this one [I]. By using user access credentials, databases are frequently conceptually divided. The general data, for instance, may be made available to all users, but only the personnel department could access wage information, and only the marketing division could get sales information. The storage and upkeep of data arc centrally managed via databases, which makes the mincredibly helpful. When a disc drive fails or the master database index becomes faulty, the database us a whole is safeguarded from damage, according to database integrity. Operating system integrity safeguards and recovery processes address these problems [2], when sensitive information is encrypted, a user who unintentionally obtains ii cannot decipher it. As a result, It is possible to store each level of sensitive data encrypted in a separate table with its own unique key.

V. Levels of Database Security

We must put security measures in place on all levels.

1. *People:* To reduce the possibility that any individual user may offer access to an intruder in exchange for money or other favors, users must be thoroughly authorized.
2. *Operating Systems:* Regardless of how secure the database system is, an operating system security flaw could compromise it.
3. *Network:* Network software security is necessary since almost all database systems allow remote access via terminals or networks.
4. *Database System:* Some users of the database system could only be permitted to view a small area of the database. It's possible that other users can issue. If database security is to be secured, security must be maintained at each of these levels.

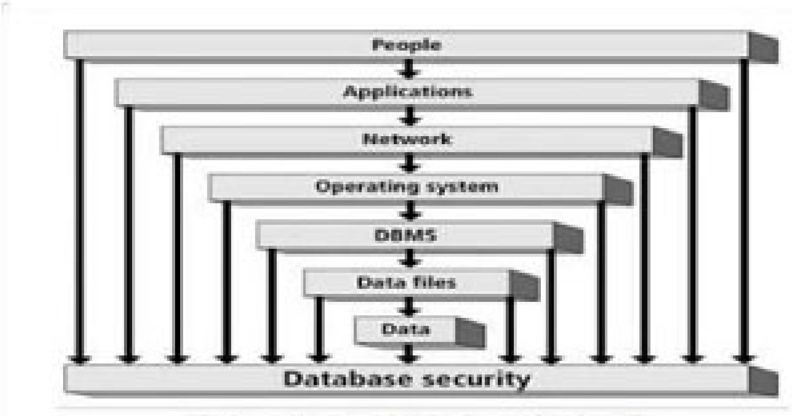


Figure 2: Database Security levels

VI. Techniques for Database Security

Authentication is one of the most fundamental ideas in database security. It is basically the method by which a user's identification is verified by the system. A user can respond to a request for authentication by showing identity papers or an authentication token.

Authorization, the second security layer, is passed through by an authenticated user. The process of obtaining information about the authenticated user, such as the database actions and data objects they are permitted to access, is known as authorization. A secure system guarantees data confidentiality. This implies that it enables users to view only the information that is intended for them. Aspects of confidentiality include user authentication, safe data storage, user authorization, and the privacy of communications. Access control is another method that may be used to safeguard databases [1], Here, access to the system is granted only once the user's credentials have been confirmed, and then and only after that has been done. Another technique that might aid in database security is the audit trial. To discover the history of activities on the database, an audit trial must be conducted [4].

Using a DBMS for numerous users with diverse interests and the ability to build a unique view for each user is one method for establishing security.

VII. Database Management System Advantages

Using a front end, sometimes referred to as a database manager or database management system {DBMS), the user communicates with the database. The rules that govern how the data is organized arc determined by a database administrator, who establishes who should have access to which data *areas* [1] J. A database provides several advantages over a simple file system. It improves data sharing so that end users may more readily access properly managed data. Since security and privacy are guaranteed, data security has increased of the data is upheld [4]. Database management has the effect of ensuring that there is the promotion of data integration across the board, allowing for a more comprehensive view of all operations [2], Furthermore, it is likely that data access is facilitated and might be utilized to deliver prompt responses to questions posed. Because the information supplied is accurate, timeless, and valid, better decisions maybe made.

VIII. Principal of Integrity Reliability in Database Security

Users expect a DBMS to give access to the data in a trustworthy manner since databases combine data from several sources, software is developers refer to a piece of software as reliable, they indicate that it can operate for very long periods of time. Since the data are usually necessary to satisfy organisational or business requirements, users expect a DBMS to be trust worthy. Additionally, customers expect DBMSs to protect their data from loss or damage because they have faith in them to do so. Data integrity is defined as the data that is stored and used in the business is accurate and reliable. A company should use data to help it decide wisely and steer clear of contradictions. Element integrity refers to the idea that only authorized users are allowed to write to or modify the value of a particular data element. A database is shielded from corruption by unauthorized users by effective access restrictions [5], Integrity problems are crucial to database security because users rely on the DBMS to preserve their data accurately.

IX. Conclusion

Because the data kept in databases is frequently extremely sensitive and valuable, security is a crucial concern in database administration. Consequently, the information in a database management system needs to be safeguarded against misuse as well as against illegal access and modifications. The purpose of this article on database security was lo investigate potential vulnerabilities in database systems. Loss of integrity and loss of secrecy are two examples of this. The article also covered topics related to perspectives and authentication-based strategics for dealing with threats of any kind. Another approach is using backup techniques, which make sure that the data is kept elsewhere and may be recovered in the event of assaults and failure. The various prerequisites for database security and the various levels of security have also been covered in this paper.

X. Future Scope

The many enterprises that create their own security standards and fundamental security controls for their database systems will find this review paper to be beneficial. It will have a better understanding of the numerous threats that might affect the database system's integrity and dependability. Future database security applications will make use of this review article to develop cutting-edge solutions that ensure that deployed data management systems satisfy their security and privacy requirements during the design, implementation, and usage of data management systems.

References Références Referencias

1. ""Security in Computing" 4th edition Mr. Charles, P. Pfleeger-Pfleeger Consulting Group, Shari Lawrence Pileeger.
2. Bertino et al Database Security-Concepts, Approaches and challenges IEEE Transactions on dependable and secure computing, 2005.
3. http://www.impcrva.eom/down1oads/TopTen Database Security Threats.
4. S. Singh, Database System: Concepts, Design and applications New Delhi: Pearson Education India, 2009.
5. S. Sumanthi, Fundamentals of relational database management systems Berlin: Springer, 2007.
6. http://wwwnosecinc.com/downloads/Risksto Database Security in 2012.pdf.
7. Emil Rurtescu, "DATABASE SECURITY ATTACKS AND CONTROL MET] IODS". Journal of Applied Quantitative Methods, Vol. 4, no. 4, Winter 2009.
8. M. Murray, Coffin, "Database Security: What Students Need to Kpow." Journal of Information Technology Education, vol. 9, pp 61-77, 2010.
9. A. Furmanyuk, M. Karpinskyy and B. Borowik, "Modern Approaches to the Database Protection," 2007 4th IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Dortmund, pp. 590-593, September 2007.
10. A. Asmawi, Z. M. Sidek, and S. A. Razak , "System Architecture for SQL Injection and Insider Misuse Detection System for DBMS", In 2008 International Symposium on Information Technology, vol. 4, pp. 1-6. June 2008.
11. Applications (SERA 2007), Busan, vol. 7, pp. 359-365, 2007.
12. Mariupi, "Principles of security and integrity of databases." Procedia Economics and Finance, Targul din Vale, Romania, vol. 15, pp. 401-405, October 2014.
13. M. Karabatak and T. Mustafa, "Performance comparison of classifiers on reduced phishing website dataset," 2018 6th International Symposium on Digital Forensic and Security (1SDFS), Antalya, vol. 5, pp. 1-5, 2018
14. R. Agrawal, R. Srikant, and Y. Xu. "Database technologies for electronic commerce." Proceedings of the 28th International Conference on Very Large Databases. Morgan Kaufmann, vol .2, pp. 1055-1058, January 2002.
15. P. R. Ambhore, B. R. Meshram, and V. B. Waghmare, "A Implementation of Object Oriented Database Security," 5th ACIS International Conference on Software Engineering Research, Management.

This page is intentionally left blank

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 23 Issue 2 Version 1.0 Year 2023
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Socio-Technical Power System Resilience

By Jaber Valinejad, Lamine Mili, C. Natalie Van Der Wal & Yijun Xu

Harvard University

Abstract- Power systems serve social communities that consist of residential, commercial, and industrial customers. The social behavior and degree of collaboration of all stakeholders, such as consumers, prosumers, and utilities, affect the level of preparedness, mitigation, recovery, adaptability, and, thus, power system resilience. Nonetheless, the literature pays scant attention to stakeholders' social characteristics and collaborative efforts when confronted with a disaster and views the problem solely as a cyber-physical system. However, power system resilience, which is not a standalone discipline, is inherently a cyber-physical social problem, making it complex to address. To this end, in this paper we develop a socio-technical power system resilience model based on neuroscience, social science, and psychological theories and using the threshold model to simulate the behavior of power system stakeholders during a disaster.

Index Terms: *resilience; social science; power systems; social computing; cyber-physical-social system; data science; social media; natural language processing.*

GJCST-E Classification: *DDC Code: 940.547252092 LCC Code: D805.J3*

SOCIOTECHNICALPOWERSYSTEMRESILIENCE

Strictly as per the compliance and regulations of:

Open Association of Research Society, USA

Research | Diversity | Ethics

Socio-Technical Power System Resilience

Jaber Valinejad [α], Lamine Mili [σ], C. Natalie van der Wal [ρ] & Yijun Xu [ω]

Abstract- Power systems serve social communities that consist of residential, commercial, and industrial customers. The social behavior and degree of collaboration of all stakeholders, such as consumers, prosumers, and utilities, affect the level of preparedness, mitigation, recovery, adaptability, and, thus, power system resilience. Nonetheless, the literature pays scant attention to stakeholders' social characteristics and collaborative efforts when confronted with a disaster and views the problem solely as a cyber-physical system. However, power system resilience, which is not a standalone discipline, is inherently a cyber-physical social problem, making it complex to address. To this end, in this paper we develop a socio-technical power system resilience model based on neuroscience, social science, and psychological theories and using the threshold model to simulate the behavior of power system stakeholders during a disaster. We calibrate and validate our model using Tenfold cross-validation on datasets of hurricane Harvey of Category 4 that hit Texas in August 2017 and hurricane Irma of Category 5 that made landfall on Florida in September 2017. We retrieve these datasets from Twitter and Google Trend and then apply natural language processing and language psychology analysis tools to deduce the social behavior of the end-users.

Index Terms: resilience; social science; power systems; social computing; cyber-physical-social system; data science; social media; natural language processing.

I. Introduction

The 2021 winter storm in Tex as, which included three severe storms between 10 and 20 February, resulted in widespread power generation failure and blackouts. As a result, over 4.5 million homes and businesses lost power, leaving them without heat, water, or food for several days. Remarkably, during the storms numerous grocery stores have closed and some critical loads, such as hospitals, were short of electricity while experiencing power outages. Thus, the 2021 Texas power crisis had a detrimental effect on people's mental and physical health, resulting in a wave of widespread anger. On the other hand, because the power system managed by the Energy Reliability Council of Texas (ERCOT) is disconnected from the US Eastern and Western interconnections, importing power from these interconnections was impossible during the winter storm. ERCOT issued bills to customers as high as $17,000 for less than a month of service, compared to prestorm prices of less than $60 per month. The power outages and high electricity prices were exacerbated by a lack of cooperation and empathy and inadequate winterization of the power infrastructure. This example demonstrates the effect of cooperation on the resilience of the power system.

A power system is inextricably linked to the social communities it serves. Indeed, making a power system resilient requires that all stakeholders, e.g., utilities, consumers, and prosumers, work together. The ultimate goal of the power system is to balance supply and demand. With the advent of the Internet and the energy of things, consumers can play a critical role in achieving the grid's objectives and assisting the generation side in increasing its operational efficiency, reliability, and resilience. For instance, the consumers may take an active role in demand management by reducing their consumption during disasters. Additionally, prosumers may store their electricity for use during times of peak demand, support critical loads, and share it with their neighbors during power outages. End-users willingness to assist the power utilities during and in the aftermath of a disaster is contingent upon their satisfaction and cooperation. Without collaboration, a power system may struggle to respond to and recover from a disaster as it was the case of the 2021 Texas winter storm. In the literature, a number of papers have proposed a variety of models for power system resilience. Although there are papers that discuss the effect of social factors on resilience, they have not modeled these social factors. The mathematical models focus exclusively on the cyber-physical aspects while ignoring the social aspects of resilience. Mili [1] elucidates the concept of the resilience of a power system and discusses its robustness, stability, reliability, and homeostasis. Panteli et al. [2] define operational metrics for power system resilience from an infrastructure perspective. Watson et al. [3] and Panteli et al. [4] provide an event-based fragility model for the electric grid's components in order to assess the vulnerability of the critical components to extreme events. To enhance power system resilience, Huang et al. [5] propose to integrate in the power system model generation re-dispatch, load shedding, and topology switching; Ma et al. [6] develop a model for backup

Author α: Student member, IEEE. Data and System Science in Public Health Lab, Medical School, Harvard University, Cambridge, MA, USA.
e-mail: JValinejad,@mgh.harvard.edu
Author σ ω: Student member, IEEE, Senior Member, IEEE L. Mili, and Y. Xu are with the Bradley Department of Electrical and Computer Engineering, Virginia Tech, Northern Virginia Center, Greater Washington D.C., VA 22043, USA.
e-mail: lmili,yijunxu@vt.edu
Author ρ: Natalie van der Wal is with the University of Delft, Technology, Policy and Management, dept. Multi-Actor Systems, Netherlands.
e-mail: C.N.vanderWal@tudelft.nl

distributed generators and automatic switches; and Mili et al. [7] and Panteli et al. [8] propose to utilize adaptive islanding.

Obviously, all the papers in the literature overlook the importance of mathematical modeling of the social component of power system resilience since they view the latter as a cyber-physical system, not as a cyber-physical-social system. The primary reasons for this lack of attention is the complexity of modeling the social component of power systems. To overcome this weakness, in this paper we present a socio-technical framework for modeling output-oriented power system resilience. To do so, we consider and model the behavior of consumers, prosumers, and utilities through the lens of computational social science. Additionally, we quantify socio-technical resilience characteristics for cross-validation purposes. Specfically, we propose a new method for assessing the social behaviors of power system stakeholders and then we calibrate and validate that model by extracting the social behavior characteristics from large-scale data sets, such as Twitter, while using the natural language processing and the text mining techniques.

The Main Contributions of the Paper are as follows:

- We propose a socio-technical model for power system resilience that leverages social science theories and computational social science to model the social behaviors of consumers, prosumers, and utilities during times of crisis. The proposed multi-agent-based model has the potential to be beneficial for detecting emergent patterns.
- We develop a new method to assess the consumer and presumed social behavior through the use of Natural Language Processing (NLP) and language psychology analysis tools, such as Linguistic Inquiry and Word Count (LIWC), as well as new approaches used in contemporary social science.
- We propose to use the threshold model based on the logistic function to consider the inter dependence between socio-technical resilience-related features. This model is based on the theory of morphic resonance and formative causation initiated by Sheldrake [9].
- We investigate the impact of Hurricanes Irma and Harvey on socio-technical power system operation as real-world case studies. We retrieve tweets from Twitter's streaming API by leveraging hashtag search on the terms #electrcity, #power systems, #electric, #power utility, #electric utility, #power grid, from hurricane Harvey's 18,336,283 tweets and hurricane Irma's 17,227,935 tweets. Additionally, Google Trends is used as another social sensing.
- We apply M-estimators [10] to calibrate the proposed model by processing spatial-temporal data sets. Then, this model is validated using Tenfold cross-validation.

The remainder of this paper is organized as follows. Section II develops a socio-technical model of power system resilience through the application of computational social science. Section III provides a framework to validate the proposed model that makes use of modern social science and explains how consumers' and prosumers' behaviors can be quantified using spatial-temporal data sets. Section IV calibrates and validates the proposed socio-technical power system model using two real-world events, Hurricane Harvey and Hurricane Irma. Finally, Section V concludes the paper.

II. Socio-Technical Power System Resilience

To capture the dynamical change in consumer, prosumer, and utility behaviors in response to a disaster, we develop a multi-agent-based dynamical model. This socio-technical model is beneficial for capturing emergent processes and for analyzing the multi-dimensional aspects of power system resilience. Figure 1 illustrates the interdependence between disasters, generational factors, and end-user behavior. We consider dissatisfaction, cooperation, and physical health to be end-user social behaviors. Additionally, we consider two distinct types of electricity generation, namely, (1) severity dependent type as exemplified by electricity generated by utilities and cooperation-dependent type as exemplified by electricity generated by Microgrids (MGs) and Distributed Energy Resources (DERs). Indeed, the performance of the utility power system to serve the load decreases with the severity of the disaster since the latter typically damages part of the electric infrastructure. As for the MGs and DERs, they are less affected by the disaster and therefore, can cooperate with electric stakeholders and share electricity during time of shortages.

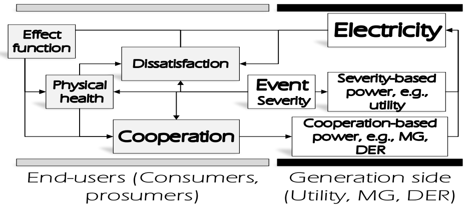

Effect function
Dissatisfaction
Electricity
Physical health
Event Severity
Severity-based power, e.g., utility
Cooperation
Cooperation-based power, e.g., MG, DER
End-users (Consumers, prosumers)
Generation side (Utility, MG, DER)

Fig. 1: Interdependence between Disasters, Generational Factors, and end-user Behavior

Prior to discussing the socio-technical power system resilience model, we will introduce next the threshold model using logistic function to consider the socio-technical effect, which is widely used in sociology, medicine, biology, ecology and neural networks [11], [12].

a) Threshold Model using Logistic Function

The threshold model using logistic function allows us to set up thresholds beyond which the socio-technical behavior changes [13], [14]. For instance, a power outage can result in consumer and prosumer dissatisfaction if the level of outages exceeds a given threshold, ***φ(X)***. The logistic value, ***ψ(X),*** of each factor on the resilience-related feature, X, is expressed as

$$\psi(X) = \frac{1}{1 + e^{-\sigma^X (X_{ti} - \phi^X)}} \tag{1}$$

Additionally, we define $\psi^{'}(X) = 1 - \psi(X)$

b) The Socio-Technical Power System Model

Eqs. 2-10 describe the dynamical changes in socio- technical behaviors. Note that all variables, parameters, and functions defined thus far take values between 0 and 1.

$$\Delta(X^E_{ti}) = \alpha'^E_{ti}(f(\hat{X}^E_{ti}, X^E_{ti}) - X^E_{ti})\Delta t, \tag{2}$$

$$\alpha'^E_{ti} = \frac{\sum_j \alpha^E_{ij} X^E_{tj}}{\sum_j \alpha^E_{ij}}, \tag{3}$$

$$f(\hat{X}^E_{ti}, X^E_{ti}) = \eta^E[X^O_{ti}(1 - (1 - X^E_{ti})(1 - \hat{X}^E_{ti})) \tag{4}$$

$$+(1 - X^O_{ti})(\hat{X}^E_{ti} X^E_{ti})] + (1 - \eta^E)\hat{X}^E_{ti},$$

$$\hat{X}^E_{ti} = w^{EE}(\frac{\sum_j \alpha^E_{tij} X^E_{tj}}{\sum_j \alpha^E_{tij}}) + W^E(1 - X^C_{ti} \quad (X^C_{ti})) \tag{5}$$

$$(1 - X^P_{ti} \quad (X^P_{ti}))\ (1 - Q^e_{ti} \quad (Q^e_{ti}))(X^S_{ti} \quad (X^S_{ti}))$$

$$\Delta(X^P_{ti}) = \eta^P \psi^{'}(X^E_{ti})[Q^e_{ti}(1 - X^S_{ti}) - P_{ti}]\Delta \tag{6}$$

$$\Delta(X^C_{ti}) = \eta^C \psi(X^E_{ti}) \psi(X^P_{ti}) \psi(X^S_{ti})[X^O_{ti}(1 - Q^e_{ti}) - X^C_{ti}]\Delta \tag{7}$$

$$\Delta(Q^{DER}_{ti}) = \alpha^{DER}_{ti}(\alpha^{DER}_{ti} - Q^{DER}_{ti})\Delta t, \tag{8}$$

$$\alpha^{DER}_{ti} = \frac{\sum_j \alpha^E_{ij} X^C_{tj} Q^{DER}_{tj}}{\sum_j \alpha^E_{ij} X^C_{tj}} \tag{9}$$

$$Q^e_{ti} = \varpi Q^{DER}_{ti} + (1 - \varpi) X^S_{ti} \quad (X^S_{ti}) Q^U_{ti}. \tag{10}$$

Eqs. 2- 5 are related to the dynamical changes in enduser dissatisfaction levels, where X^E_{ti} associated with the i-*th* consumer/prosumer dissatisfaction at time t with an incremental change, $\Delta(X^E_{ti})$. Note that a value of 0 or 1 for X^E_{ti} indicates a low or a high level of dissatisfaction, respectively. Here, $f(\hat{X}^E_{ti}, X^E_{ti})$ denotes the magnitude of the absorption and amplification's effect on the end-user emotion [15]; $\hat{X}^E_{ti}$ denotes the magnitude of the effect of dissatisfaction diffusion among consumers, prosumers, and external features on the end-user dissatisfaction. Additionally, α'^E_{ti} denotes the strength of the link between two consumers/prosumers i and j. A value of 1 for α^E_{ij} indicates a strong connection. In Eq. 3 X^O_{ti} denotes an agent's optimism. A X^O_{ti} value of 1 indicates that the consumer/prosumer is optimistic. The first term (with coefficient of η^E represents the amplification effect while the final term (with coefficient of $(1 - \eta^E))$ represents the absorption effect. The former effect is based on Fredrickson's broaden-and-build theory, and includes upwards and downwards spirals [15], [16]. If there is no external disaster within the group, the bottom-up absorption effect may be used. On the other hand, when an unexpected event occurs, the amplification effect should be considered as well. Combining the two effects makes sense for disaster resilience and planning. Eq. 5 consists of two components, namely the social diffusion and the impact of external factors. Social contagion or diffusion implies that end-users' dissatisfaction is contingent on the dissatisfaction of other consumers and prosumers. Additionally, the dissatisfaction is influenced by external factors, i.e., cooperation, X^C_{ti}, [17] physical health, X^P_{ti}, [18], and accessibility to electricity, Q^e_{ti}, [19] and severity of a disaster. X^S_{ti}. Eq. 6 is related to the dynamical changes in physical health, $\Delta(X^P_{ti})$ where η^P denotes the dynamical coefficient of physical health. The latter is influenced by the level of dissatisfaction, the severity of a disaster, X^S_{ti} and the access level to electricity, Q^e_{ti}, [20]. Eq. 7 is related to the dynamical changes in the level of consumer and producer cooperation, $\Delta(X^C_{ti})$ The level of cooperation is a function of the positive or negative emotion level based on the narrowing hypothesis of Fredrickson's broaden-and-build theory [21]. Indeed, cooperation is conditional on dissatisfaction [17], physical health [22], and the level of optimism among end-users [23], and access level to electricity by the end-users, Q^e_{ti}.

Eqs. 8-10 model the dynamical changes of accessibility to electricity by the end-users. The primary energy sources that supply electricity to consumers include utilities, MG, and DERs. Utilities are the primary suppliers of the demand of electricity. However, during disasters, some communities may lose access to utility-provided electricity. In this case, depending on their level of cooperation, end-users who own DERs, namely prosumers, may wish to share their electricity with consumers and critical loads that are not connected to the grid, but they are connected to them. Here, $\Delta(Q^{DER}_{ti})$ denotes the dynamical changes in accessibility to DER generated electricity. A value of 1 for Q^{DER}_{ti} indicates that the consumer/prosumer makes full use of the DERs' capacity to meet its demand. Additionally, available electricity, Q^e_{ti} is the total amount of electricity supplied by utilities and consumers, whereas Q^U_{ti} is the amount of electricity generated by utilities, which varies according to the severity of a disaster. A value of 1 for Q^U_{ti} indicates that utilities are fully utilizing their capacity to meet consumer/prosumer demand. Additionally, ϖ is the fraction of an end-user's total electricity consumption that is supplied by DERs.

In this section, we have presented a mathematical model of the socio-technical power system resilience. In the following section, we discuss how to calibrate and validate that model using Tenfold cross-validation.

III. Active Demand-Side Management as Ancillary Service

Meteorology organizations predict the weather. However, in general, weather is so nonlinear and impacts the power system states. There are five power system operation states: normal, alert, emergency, in extremes, and restoration. In an emergency condition, where the system starts to lose its stability, there is a requirement for corrective steps where consumers' roles and level of collaboration are inevitable to retain grid resilience.

In case of an approaching disaster, emergency services are informed and transmit a signal and required information to both utilities and consumers. In conventional power systems, the generation side deals with numerous issues, whereas in modern power systems, by grid modernization, the generation side is not alone anymore. Consumers can participate in active demand-side management and minimize their consumption during disasters in a decentralized power system. Decentralization is one of the main foundations for grid resiliency. In addition, the prosumers can share their electricity with their neighbors and assist critical loads. To have a resilient electricity system, the demand side plays a significant role. The consumer's desire to help power providers overcome a crisis hinges on customer satisfaction and cooperation. In addition, sharing electricity is interwoven with the level of cooperation of the community. There are four scenarios to keep grid resilience, voltage, and transient stability.

1. In real-time, it can send a signal through a communication system to consumers to turn off some of their devices, e.g., a computer, refrigerator during the event. One reason that motivates consumers to participate in active demand-side management is to prevent the automatic cutoff of electricity by utilities. In this circumstance, the level of collaboration and flexibility of consumers can affect grid resilience. Plus, numerous policies might be enacted to attract customers to engage. In this scenario, the consumers a day ahead (although it can be real-time) select they want to participate in active demand-side management and which devices they only use to aid the utility to address grid resilience.
2. In the planning mode, the utility has a contract with consumers to turn off their devices during an event. Every device has a sensor and can be controlled by utilities. Here, the level of collaboration of consumers can help the utility to manage the incident.
3. In real-time, utilities can evaluate the risk of occurrences and turn off the electricity of consumer devices automatically without letting them know. In this instance, the consumer's satisfaction diminishes. In addition, some consumers like hospitals, while they are in desperate need of electricity, may be disconnected.
4. In addition, in the planning mode, prosumers and consumers can share their electricity with their neighborhoods and critical loads. We suppose that demand is 20 MW. In this scenario, if each home shares its electricity with only one neighborhood, the electricity demand reduces dramatically to 10 Mw. In this scenario, the customers can respond to the utility signal that they share their electricity with n number/ KW of neighborhoods/consumers.

In all scenarios, a utility may set the level of disconnection based on different desired frequency thresholds. Utilities may view the 59-61 as a normal range of frequency fluctuations. In the case of three thresholds, we have the following scenarios:

a) If the frequency is lower than 59 HZ, the utility decrease the10 percent load to keep grid resilience.
b) If the frequency is lower than 55 HZ, the utility drops the 30 percent load to keep grid resilience
c) If the frequency is lower than 50 HZ, the utility drops the 50 percent load to keep grid resilience.

Valinejad et al. [24] pioneered the development of an artificial society based on a power system's social demand response. They assumed that consumers could engage in demand response to achieve one of two goals: cost savings or increased system sustainability. Different communities and societies have distinct cultures and characteristics, which influence both dissatisfaction and cooperation. When the enduser's level of dissatisfaction and cooperation is as low as 0.5 and 0.1 in case 4, the proposed motivation price cannot meet the marginal level of load shaving of 20%. To achieve their goal in this situation, utilities must either increase the marginal level of load shaving to 30%, i.e., Case 5, or increase the motivation price by 20%, i.e., Case 6. Case 6 is more expensive for utilities. As can be seen, end-user behavior has an effect on utility costs and, consequently, on the reliability of power systems. When people's level of dissatisfaction is high, the situation becomes even worse. To accomplish its objectives, the utility must increase the motivation price by at least 40% (appropriate level of load shaving).

IV. Calibrating and Validating the Socio-Technical Power System Resilience Model

The process for calibrating and validating the sociotechnical power system resilience model proposed in Section II is depicted in Figure 2. Prior to validating the model, we measure the social behavior of the end-users. Social scientists and cognitive, personality, clinical, and social psychologists use surveys and direct qualitative questions to measure social behavior in conventional social science. While the surveys provide us with an appropriate dataset, they exhibit several significant drawbacks. In practice, they are costly and time consuming to execute. Typically, they are only composed of subsets of the society. Last but not least, individuals have varying interpretations of the level of social behavior. On the other hand, in the new era of language psychology, utilizing community communication via social media platforms such as Twitter and Facebook can circumvent survey limitations and provide a rich dataset. This social media platform is being used to deduce linguistic and psychological patterns associated with social behavior. Due to the strong correlation between linguistic patterns and personality and psychological state in contemporary social science, social behavior is estimated using linguistic patterns. The words and language we use on a daily basis reflect our internal thoughts, our quality of life, our personality, our cognitive styles, our emotions, and our psychological and social behavior. Now, let us utilize the Twitter and Google Trend datasets in order to analyze the resiliency during Hurricanes Irma and Harvey. We retrieve tweets about the power system byfiltering them and utilizing the hashtag search for #electricity, #power system, #electric, #DER, #power plant, #distributed generation, #micro grid, #power utility, #electric utility, #renewable energy, #blackout, #power grid, #power network.

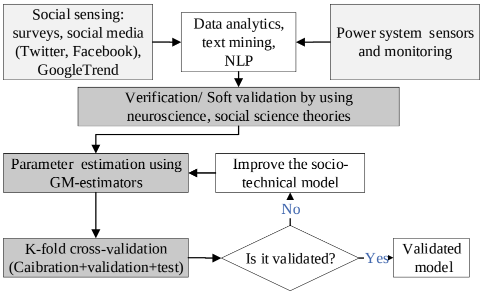

Social sensing: surveys, social media (Twitter, Facebook), GoogleTrend
Data analytics, text mining, NLP
Power system sensors and monitoring
Verification/ Soft validation by using neuroscience, social science theories
Parameter estimation using GM-estimators
Improve the socio-technical model
No
K-fold cross-validation (Caibration+validation+test)
Is it validated?
Yes
Validated model

Fig. 2: Validation of the Cyber-Physical-Social Power System

Following the collection of the raw dataset, we employ psychology-based natural language processing, specifically the Linguistic Inquiry and Word Count (LIWC), to extract endusers social behavior, including dissatisfaction, cooperation, and physical health.

- *Dissatisfaction:* Disasters such as the 2021 Texas winter storm, Hurricane Irma, and Hurricane Harvey result in end-user dissatisfaction. The latter is caused by negative emotional traits, such as anxiety, sadness, and anger [25]– [27]. Using the Twitter dataset, we quantify spatial-temporal dissatisfaction by quantifying these features. The measure of dissatisfaction is calculated by averaging the normalized values of anxiety, sadness, and anger. By using the categories of the LIWC, the level of fear is obtained by -

$$S^E = LIWC['anx']/LIWC[`WC']$$

  where $LIWC['anx']$ means the category of "anx" from outputs of LIWC.

- *Cooperation:* According to psychological research on language, the more words used in communication, the greater the level of agreement and cooperation. The increased use of complex words and words with more than six letters implies a decrease in communication efficiency, cooperation, and social interaction [28]. Additionally, the plural form of thefirst person indicates group interaction and cohesion [29]. Increasing the use of social process languages, such as family and friend-related terms, implies an increase in social interaction, engagement, and cooperation [30], [31]. Finally, assent-related language promotes group consensus, interaction, and cooperation [32]. Hence, the level of cooperation is obtained by

$$X_C = (LIWC['WC'] - LIWC\,['Sixltr'] + LIWC\,['we'] + LIWC\,['social'\,]\ \ LIWC\,['family']\ \ LIWC['friend'] + LIWC['assent'])/(LIWC['WC'])$$

- *Physical Health:* According to psychological research on language, increased use of the first -person singular can imply physical pain [33]. Individuals who are physically ill frequently draw attention to themselves. The increased use of motion, leisure, and work-related terms reflect an increase in physical activity and health. Additionally, the more health-related words a person uses, the better their physical health. The increased use of positive body-related terms implies physical health

[34]–[37]. By using the categories of the LIWC, the level of physical health is obtained by

$$S^P = (-LIWC['i'] + LIWC['health'] + LIWC['leisure'] + LIWC['work'] + LIWC['body'] + LIWC['motion'])/LIWC[`WC']$$

The Calibration and Validation Process can be Summarized as follows.

Step1) Amassing disaster-related data on power systems: First, we collect all tweets about the considered disaster. Then, we retrieve tweets about the power system via a hashtag or related word search. Additionally, we utilize Google Trend as a second social sensing tool.

Step 2) Resilience-related text cleaning: To improve the effectiveness of the result for linguistic and behavioral patterns, we use natural language processing to remove URLs, email addresses, dates, punctuation, and stop words from retrieved tweets about power system response and recovery. After that, we tokenize all tweets for the purpose of word stemming.

Step 3) Measuring Social Behavior: We leverage language psychology analysis tools, such as LIWC, to assess social behavior from the cleaned text. We look for social patterns associated with resilience using the following categories: anxiety, sadness, anger, First-person singular, health, leisure, work, body, motion, word count, words >6 letters,first -person plural, social process, family, friends, exclusive, and assent.

By using the categories of the LIWC, the level of fear is obtained by

$$S^E = LIWC['anx']/LIWC[`WC']$$

where $LIWC['anx']$ means the category of "anx" from outputs of LIWC.

Hence, the level of cooperation is obtained by-

$$X_C = (LIWC['WC'] - LIWC['Sixltr'] + LIWC['we'] + LIWC['social'] + LIWC['family'] + LIWC['friend'] + LIWC['assent'])/(LIWC['WC'])$$

By using the categories of the LIWC, the level of physical health is obtained by

$$S^P = (-LIWC['i'] + LIWC['health'] + LIWC['leisure'] + LIWC['work'] + LIWC['body'] + LIWC['motion'])/LIWC[`WC']$$

Step 4) Concluding Social Behavior: We begin this step by dealing with missing values via an interpolation approach. In order to fairly consider each category to estimate community resilience, we normalize the measure of each category using min-max scaling. Given a feature *x(t),* an arbitrary interval of values, i.e., *[α, β]* based on min-max scaling, a normalized measure is obtained by:

$$x'(t) = \alpha + \frac{(x(t) - x_{\min}(t)))(\beta - \alpha)}{x_{\max} - x_{\min}}, \tag{11}$$

where we set $\alpha = 0$ and $\beta = 1$ and $x_{\max}$ and $x_{\min}$ are the maximum and minimum measure collected during the period considered, and is $x'(t)$ a normalized measure as a real number in [0,1]. After that, we deduce spatial-temporal trends in end-user social behavior during a disaster.

Step 5) Soft validation: We verify the model using soft validation.

Step 6) Parameter estimation: We calibrate the model using a Huber M-estimator. The Huber loss are as follows:

$$\theta = argmin(\sum log(f(x))) = argmin(\sum \rho(x_i, \theta))$$

and

$$\rho(x_i, \theta) = \begin{cases} \frac{1}{2}x_i^2 & |x_i| \leq \sigma \\ \sigma(|x_i| - \frac{1}{2}\sigma) & \text{otherwise} \end{cases} \tag{12}$$

Step 7) Validation by cross-validation: We validate the model using tenfold cross-validation. We classify 60% of data as calibration data, 20% as validation data, and 20% as test data.

Step 8) Updating the Model: If the proposed socio-technical power system resilience model does not perform well after cross-validation, we modify the model accordingly.

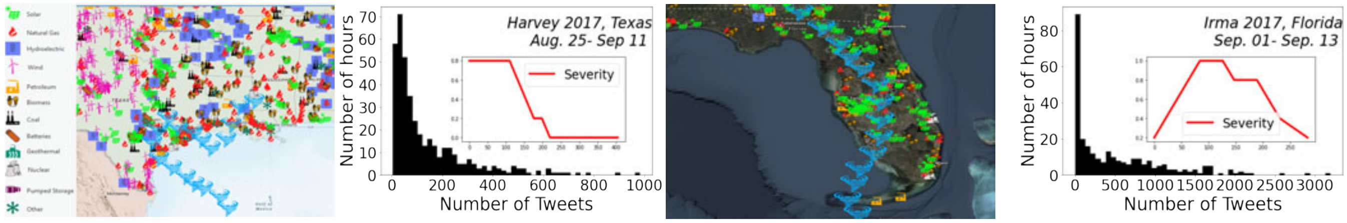
V. Calibrating and Validation the Model by using Datasets from Hurricanes Harvey and Irma

We collect a variety of data samples for Hurricanes Harvey and Irma. We retrieve power-system-related tweets from Twitter's streaming Application Programming Interface (API) by leveraging hashtag search on the hashtag search on #electricity, #power system, #electric, #DER, #power plant, #distributed generation, #micro grid, #power utility, #electric utility, #renewable energy, #blackout, #power grid, #power network, from 18,336,283 tweets of Hurricane Harvey and 17,227,935 tweets of Hurricane Irma for validation purpose. We use the same words as hashtags for word-related searches. We also use Google Trend as another social sensing. Table I provides a summary of 5 samples for each hurricane.

Hurricane Harvey and Irma's tracks, in-hurricane power plants, Tweets, and severity are depicted in Figure 3.

The following is a summary of the impact of these hurricanes.

Hurricane Harvey in Texas: Between 08/25/2017 and 09/11/2017, Hurricane Harvey struck Texas and the ERCOT



(a) Harvey track

(b) Harvey Tweets

(c) Irma track

(d) Irma Tweets

Fig. 3: Hurricane Harvey and Irma's Tracks, in-Hurricane Power Plants, Tweets Frequency, and Hurricane Severity

Table I: The summary of samples for Hurricanes Harvey and Irma

Sample	Social sensing	Type of search	Harvey Tweets IDs	Irma Tweets IDs
1	Twitter	Hashtag	217	271
2	Twitter	Word related	11500	54100
3	Twitter	Event related	20000	30000
4	Twitter	Word related	82000	245000
5	GoogleTrend	Word related	-	-

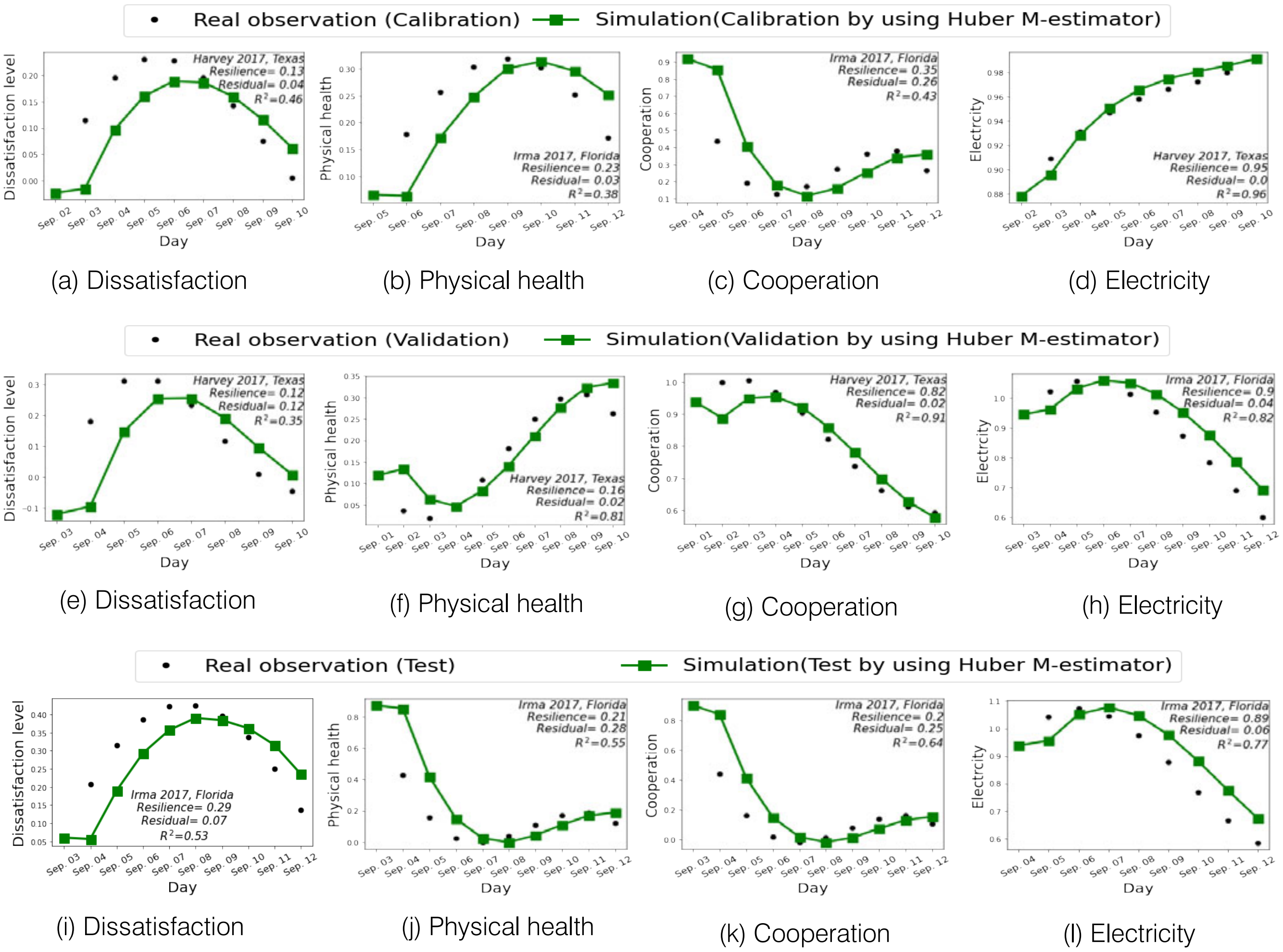
territory. On 08/25/2017, it strengthened to Category 4. Like Hurricane Katrina, this hurricane is the most expensive tropical cyclone in the US history. In Texas, 1168 MW of wind energy capacity and 5679 MW of solar energy capacity in ERCOT became unavailable and energy production fell by 21%. As a result, power systems throughout ERCOT's territory experienced outages between 08/25/2017 and 08/29/2017, leaving many people without power or water. The maximum number of outages reached 309204, which affected two of ERCOT's major utilities, namely AEP Texas North Company (#20404) and AEP Texas Central Company (#3278). For these power utilities, the total number of meters, including smart and nonsmart meters, is 1028900. It took about two weeks, namely from 08/29/2017 to 09/12/2017, for the power system to be restored. We extract various samples of tweets about Hurricane Harvey from the Table I. Between 2:00 p.m. and 11:00 p.m. on 08/30/2017, the customer outage dataset contains missing values due to the loss of an entity website.

Hurricane Irma in Florida: Between 09/01/2017 and 09/13/2017, Hurricane Irma made landfall primarily in Florida and to a lesser extent in Georgia and South Carolina. Between 09/06/2017 and 09/08/2017, this storm was a Category 5 hurricane. Hurricane Irma was downgraded to a Category 3 storm before making landfall in Florida on 09/09/2017. However, on 09/10/2017, it was upgraded to a Category 4 hurricane. Hurricane Irma was then downgraded to Category 1 status on 09/11/2017. Between 09/09/2017 and 09/11/2017, power systems faced outages. It damaged several utilities, including the City of Tallahassee (TAL#18445), the Jacksonville Electric Authority (JEA#9617), Gainesville Regional Utilities (GVL#6909), the City of New Smyrna Beach (NSB#13485), Florida Power Corp. (FPC#6457), Tampa Electric Co. (TEC#18454), Seminole Electric Cooperative (SEC), Florida Municipal Power (FMPP#19804), and Florida Power & (SOCO). The recovery of the power system began on 09/11/2017 and lasted 12 days.

a) Results for the First Sample

The results of a 10-fold cross-validation of the socio technical power system resilience model using the Huber Mestimator for thefirst sample are displayed in Fig. 4. This graph depicts consumer/prosumer dissatisfaction, physical health, cooperation, and the cooperation/severity-dependent electricity using real datasets. The figure also show simulation results related to various scenarios used for calibration, validation, and testing of multi-agent-based model. Each sub figure contains information about the type of event, its resilience level, value of $R^2 = 1 - (RSS/TSS)$ where $RSS = \sum(y - \bar{y})^2$, and $TSS = \sum(y - \bar{y})^2)$ We calibrate and validate the model using data obtained from both Hurricanes Irma and Harvey. Additionally, we calibrate and validate the model for Hurricanes Irma and Harvey separately. The estimated threshold level at which cooperation among end-users has an effect on diss at is factionise qualto 0.5. Similarly, the estimated threshold levels are 0.500002, 0.500017, and 0.500071 for the effects of physical health, electricity, and disaster severity on consumer/ prosumer dissatisfaction, respectively. The estimated threshold levels of electricity and severity on dissatisfaction among Florida end-users are equal to 0.499355 and 0.501454, respectively. These estimated threshold levels for ERCOT areas are equal to 0.500039 and 0.499944, respectively. Additionally, the amplification and absorption effects on the level of dissatisfaction are 0.501797 and 0.498203, respectively. The end users in the ERCOT area and Florida have an optimistic attitude of up to 0.502206. Florida end-users and utilities are less optimistic than their counterparts in Texas with an optimistic level estimated to 0.478854 versus 0.498893 for Texas. For both areas, the estimated threshold level for the effect of dissatisfaction on physical health is equal to 0.415647. Additionally, this threshold is equal to 0.494225, 0.493983, and 0.495111 for the effect of dissatisfaction, physical health, and severity on cooperation, respectively. The estimated threshold level for the effect of severity on electric utility services is equal to 0.458197. This means that if the hurricane is a category three or higher, it has a detrimental effect on the utility's performance. Additionally, approximately 100% of electricity services are cooperatively provided. The estimated threshold level for the effect of severity on ERCOT is 0.457566, while that of Florida is 0.479339. Additionally, 76% of electricity services in ERCOT is of a cooperative-type while 24% are severity-type. Indeed, ERCOT is more vulnerable to hurricane damage than Florida utilities.

Fig. 5 illustrates the QQ-plot for the test dataset's various socio-technical resilience-related features. It demonstrates that the simulation and the real datasets have a similar distribution. The distributions of dissatisfaction and cooperation/severity dependent electricity for the simulation case are more similar to the real case than the physical health and cooperation of the end-users.

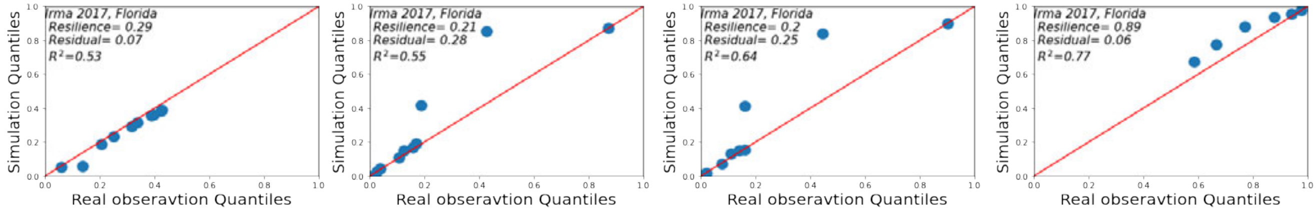


(a) Dissatisfaction (b) Physical health (c) Cooperation (d) Electricity

(e) Dissatisfaction (f) Physical health (g) Cooperation (h) Electricity

(i) Dissatisfaction (j) Physical health (k) Cooperation (l) Electricity

Fig. 4: Consumers' and Prosumers' Level of Dissatisfaction, Physical Health, Cooperation, and the Cooperation/Severity-Dependent Level of Electricity. These are Determined using 10-Fold Cross-Validation, which Included Calibration, Validation, and Test. The Socio-Technical Power System Resilience Model is Calibrated using a Huber M-Estimator and Data Obtained from Hurricanes Irma and Harvey



(a) Dissatisfaction (b) Physical health (c) Cooperation (d) Electricity

Fig. 5: The QQ-Plot Depicts the Level of Dissatisfaction, Physical Health, and Cooperation of Consumers, Prosumers, and the Level of Cooperation/Severity-Dependent Electricity of Socio-Technical Power Systems Resilience for the Test Data Set

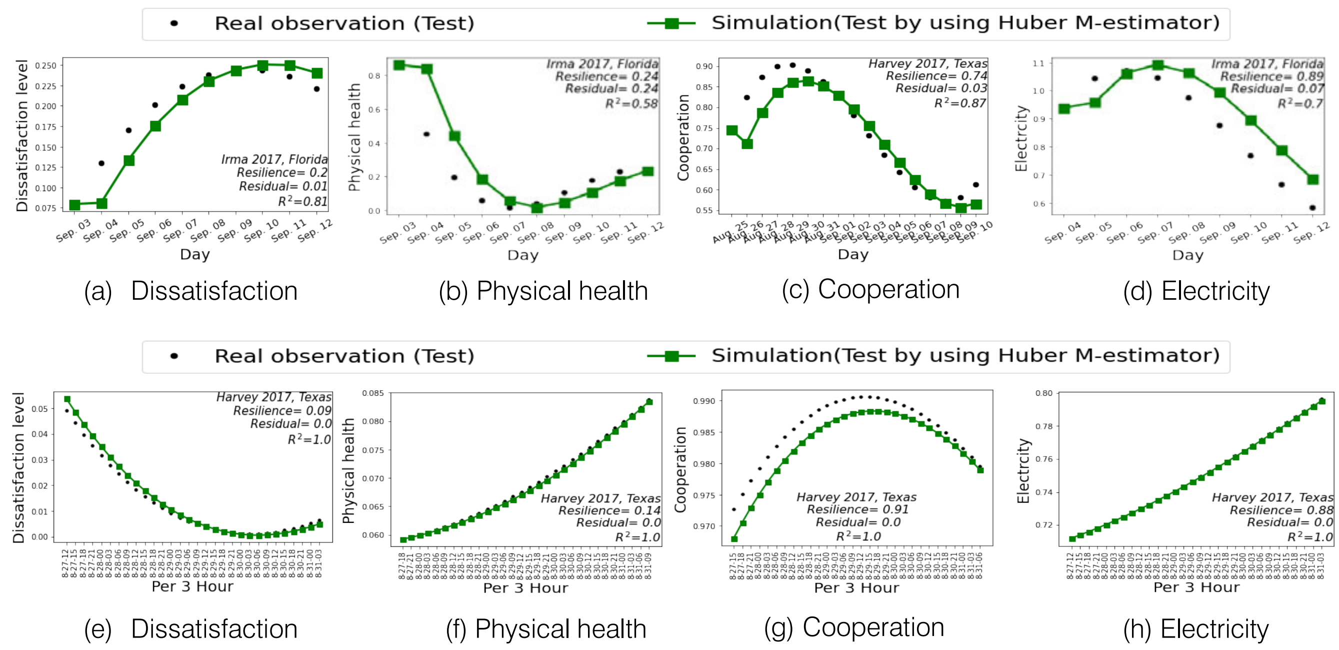
Table II shows the results of the statistical analysis using real-world and simulation datasets for calibration, validation, and test scenarios. The Shapiro-Wilk normality test demonstrates that the majority of cases follow the normal distribution except for cooperation during calibration and testing, as well as the physical health of end-users in the test scenario. Indeed, 0.75 of features exhibit normal distribution behavior. Additionally, the Pearson and Kendall tau correlations demonstrate the high degree of correlation between the simulation and the real datasets. Additionally, Student's t-test p-values (as parametric statistical hypothesis test) and Mann-Whitney U test p-values (as non-parametric statistical hypothesis test) indicate that the distribution of the socio-technical resilience-related features obtained from the real data set and simulation outputs are similar in all cases.

b) *Summary Results for all Samples*

Fig. 6 provides the graphs of the tenfold cross-validation of the socio-technical power system resilience model using the median estimated values of five samples and a three-hourly based dataset for the real and simulated datasets. The results indicate that the socio-technical resilience-related features in the three-hourly-based dataset have a higher R2 value. In other words, the 10-fold cross-validation produces more precise results than the daily datasets. This is because we calibrate the model with more data for the former case. Using the median estimated values of five samples, we found that the level of optimism is equal to 0.537192. The estimated threshold levels for the effect of electricity and disaster severity on the level of dissatisfaction among power system stakeholders are respectively 0.499162 and 0.498763. Additionally, the estimated threshold level of the effect of severity on electricity is equal to 0.45721. On the other hand, using 10-fold cross-validation on a three-hourly basis, the estimated level of optimism among the end-users is equal to 0.594039. The estimated threshold levels for the effect of electricity and disaster severity on dissatisfaction among stakeholders in the power system is 0.475009 and 0.538839, respectively. The amplification effect, as defined by the broaden-and-build theory, accounts for 67% of the dissatisfaction level, while the absorption effect, as defined by the bottom-up emotion theory, accounts for 33%. When we use a daily-based dataset, these values are 50% and 50%. The estimated threshold values for the effect of severity on electricity is equal to 0.458702 in three-hourlybased analyses. Additionally, 76% of electricity services are cooperation-based while 24% are severity-based. As illustrated in Fig. 7, there is a greater similarity in the distributions of three-hourly-based datasets than in the daily-based dataset.

Table II: Results of The Statistical Analysis of Socio-Technical Power Systems Resilience Including Shapiro-Wilk Normality Test, Pearson Correlation, Kendall Tau Correlation, Parametric Statistical Hypothesis Tests (Student's T-Test), and Non-Parametric Statistical Hypothesis Tests (Mann-Whitney U Test). Note that in the Table, the Gaussian Probability Distribution is Denoted as ”Gauss.” and the Dependence Between the Simulation and Real Datasets is Denoted as ”Dep.”.

10-fold Cross-validation	Calibration				Validation				Test			
Statistic test	X_{ti}^{E}	X_{ti}^{P}	X_{ti}^{C}	Q_{ti}^{e}	X_{ti}^{E}	X_{ti}^{P}	X_{ti}^{C}	Q_{ti}^{e}	X_{ti}^{E}	X_{ti}^{P}	X_{ti}^{C}	Q_{ti}^{e}
Real data set p-value	0.3 (Gauss.)	0.24 (Gauss.)	0.012 (not Gauss.)	0.45 (Gauss.)	0.52 (Gauss.)	0.22 (Gauss.)	0.16 (Gauss.)	0.15 (Gauss.)	0.27 (Gauss.)	0.002 (not Gauss.)	0.002 (not Gauss.)	0.28 (Gauss.)
Simulation P-value	0.17 (Gauss.)	0.07 (Gauss.)	0.036 (not Gauss.)	0.16 (Gauss.)	0.34 (Gauss.)	0.21 (Gauss.)	0.09 (Gauss.)	0.16 (Gauss.)	0.07 (Gauss.)	0.007 (not Gauss.)	0.006 (not Gauss.)	0.32 (Gauss.)
Pearson corr	0.74 (Dep.)	0.77 (Dep.)	0.81 (Dep.)	0.99 (Dep.)	0.67 (Dep.)	0.91 (Dep.)	0.96 (Dep.)	0.96 (Dep.)	0.8 (Dep.)	0.88 (Dep.)	0.89 (Dep.)	0.93 (Dep.)
kendalltau corr	0.61	0.43	0.5	1	0.57	0.73	0.82	0.78	0.64	0.64	0.68	0.77
Student's t-test p value	0.54 (same)	0.72 (same)	0.69 (same)	0.9 (same)	0.68 (same)	0.84 (same)	0.95 (same)	0.55 (same)	0.61 (same)	0.59 (same)	0.63 (same)	0.57 (same)
Mann-Whitney U Test p value	0.2 (same)	0.26 (same)	0.48 (same)	0.38 (same)	0.34 (same)	0.33 (same)	0.38 (same)	0.27 (same)	0.22 (same)	0.41 (same)	0.5 (same)	0.22 (same)



(a) Dissatisfaction (b) Physical health (c) Cooperation (d) Electricity

(e) Dissatisfaction (f) Physical health (g) Cooperation (h) Electricity

Fig. 6: Graphs of the Level of Dissatisfaction, Physical Health, and Cooperation of Consumers and Prosumers, and the level of Cooperation/Severity-Dependent Electricity in the Socio-Technical Power Systems Resilience Model for two Scenarios: 1) Median of All Samples and 2) Three-Hourly-Based Data Set

VI. Conclusions

In this paper, we use neuroscience and social science theories to model the complex collective behavior of consumers and prosumers during a disaster. The proposed socio-technical power system resilience model is beneficial for observing emergent processes and developing new hypotheses that can be tested in real-world scenarios. We propose an approach for assessing the behavior of power system stakeholders through the use of social sensing tools such as Twitter and Google Trend. We increase the proposed model's reliability by validating it using cross-validation and data sets related to Hurricanes Harvey and Irma. It should be noted that the approach proposed in this paper for model validation can be applied to a wide variety of socio-technical power system problems.

References Références Referencias

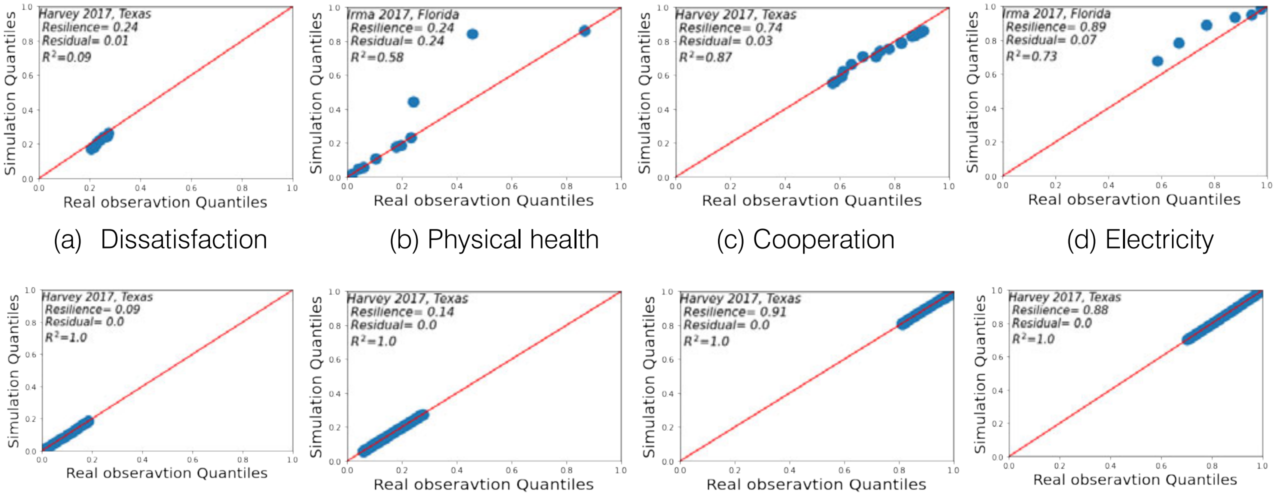
1. L. Mili, “Taxonomy of the characteristics of power system operating states,” pp. 13–15, 2011.
2. M. Panteli, P. Mancarella, D. N. Trakas, E. Kyriakides, and N. D. Hatziargyriou, “Metrics and quantification of operational and infrastructure resilience in power systems,” IEEE Transactions on Power Systems, vol. 32, no. 6, pp. 4732–4742, 2017.
3. E. B. Watson and A. H. Etemadi, “Modeling electrical grid resilience under hurricane wind conditions with increased solar and wind power generation,” IEEE Transactions on Power Systems, vol. 35, no. 2, pp. 929–937, 2020.
4. M. Panteli, C. Pickering, S. Wilkinson, R. Dawson, and P. Mancarella, “Power system resilience to extreme weather: Fragility modeling, probabilistic impact assessment, and adaptation measures,” IEEE Transactions on Power Systems, vol. 32, no. 5, pp. 3747–3757, 2017.
5. G. Huang, J. Wang, C. Chen, J. Qi, and C. Guo, “Integration of preventive and emergency responses for power grid resilience enhancement,” IEEE Transactions on Power Systems, vol. 32, no. 6, pp. 4451–4463, 2017.
6. S. Ma, L. Su, Z. Wang, F. Qiu, and G. Guo, “Resilience enhancement of distribution grids against extreme weather events,” IEEE Transactions on Power Systems, vol. 33, no. 5, pp. 4842–4853, 2018.
7. L. Mili, K. Triantis, and A. Greer, “Integrating community resilience in power system planning,” Power Engineering: Advances and Challenges Part B: Electrical Power, 2018.
8. M. Panteli, D. N. Trakas, P. Mancarella, and N. D. Hatziargyriou, “Boosting the power grid resilience to extreme weather events using defensive islanding,” IEEE Transactions on Smart Grid, vol. 7, no. 6, pp. 2913–2922, 2016.
9. R. Sheldrake, The presence of the past: Morphic resonance and the habits of nature. Icon Books Ltd, 2011.
10. L. Mili, M. Cheniae, N. Vichare, and P. J. Rousseeuw, “Robust state estimation based on projection statistics [of power systems],” IEEE Transactions on Power Systems, vol. 11, no. 2, pp. 1118–1127, 1996.

11. F. L. Gaol, Interdisciplinary Behavior and Social Sciences: Proceedings of the 3rd International Congress on Interdisciplinary Behavior and Social Science 2014 (ICIBSoS 2014), 1-2 November 2014, Bali, Indonesia. CRC Press, 2015.
12. D. J. Champion, Basic statistics for social research. Chandler Publishing Company Scranton, 1970.
13. B. D. Haig and C. W. Evers, Realist inquiry in social science. Sage, 2015.
14. T. Bosse, M. Hoogendoorn, M. C. A. Klein, J. Treur, N. van der Wal, and A. van Wissen, "Modelling collective decision making in groups and crowds: Integrating social contagion and interacting emotions, beliefs and intentions," Autonomous Agents and Multi-Agent Systems, vol. 27, no. 1, pp. 52–84, 2013.
15. M. Hoogendoorn, J. Treur, C. N. van der Wal, and A. van Wissen, "Modelling the emergence of group decisions based on mirroring and somatic marking," In: Yao, Y., Sun, R., Poggio, T., Liu, J., Zhong, N., and Huang, J. (eds.), Proc. of the Second International Conference on Brain Informatics, BI'10, LNAI, Springer Verlag, Heidelberg, 2010.
16. J. Valinejad, L. Mili, C. N. van der Wal, M. von Spakovsky, and Y. Xu, "Multi-dimensional output-oriented power system resilience based on degraded functionality," 2021 IEEE Power and Energy Society, General Meeting (PESGM), Washington, D.C., USA (Accepted), 2021.
17. D. Rand, G. Kraft-Todd, and J. Gruber, "Positive emotion and (dis) inhibition interact to predict cooperative behavior," Available at SSRN 2429787, 2014.
18. J. Ohrnberger, E. Fichera, and M. Sutton, "The relationship between physical and mental health: a mediation analysis," Social Science & Medicine, vol. 195, pp. 42–49, 2017.
19. A. Ibrahim, G. C. Aryeetey, E. Asampong, D. Dwomoh, and J. Nonvignon, "Erratic electricity supply (dumsor) and anxiety disorders among university students in ghana: a cross sectional study," International journal of mental health systems, vol. 10, no. 1, p. 17, 2016.
20. C. Liddell and C. Guiney, "Living in a cold and damp home: frameworks for understanding impacts on mental well-being," Public Health, vol. 129, no. 3, pp. 191–199, 2015.
21. B. L. Fredrickson and T. Joiner, "Positive emotions trigger upward spirals toward emotional well-being," American psychological society, vol. 13, no. 2, 2002.
22. R.-M. H¨am¨ al¨ainen, A. R. Aro, C. J. Lau, D. Rus, L. Cori, and A. M. Syed, "Cross-sector cooperation in health-enhancing physical activity policymaking: more potential than achievements?" Health research policy and systems, vol. 14, no. 1, p. 33, 2016.
23. S.-E. Byun, S. Han, H. Kim, and C. Centrallo, "Us small retail businesses' perception of competition: Looking through a lens of fear, confidence, or cooperation," Journal of Retailing and Consumer Services, vol. 52, p. 101925, 2020.
24. J. Valinejad, L. Mili, C. N. van der Wal, and Y. Xu, "Environomic-based social demand response in cyber- physical-social power systems," IEEE Transactions on Circuits and Systems II: Express Briefs, 2021.
25. A. C. Krendl and B. L. Perry, "The impact of sheltering in place during the COVID-19 pandemic on older adults' social and mental well-being," The Journals of Gerontology: Series B, vol. 76, no. 2, pp. e53–e58, 2021.
26. L. Faelens, K. Hoorelbeke, B. Soenens, K. Van Gaeveren, L. De Marez, R. De Raedt, and E. H. Koster, "Social media use and well-being: A prospective experience-sampling study," Computers in Human Behavior, vol. 114, p. 106510, 2021.
27. M. R. Paredes, V. Apaolaza, C. Fernandez-Robin, P. Hartmann, and D. Ya˜nez-Martinez, "The impact of the COVID-19 pandemic on subjective mental well-being: The interplay of perceived threat, future anxiety and resilience," Personality and Individual Differences, vol. 170, p. 110455, 2021.
28. M. R. Mehl, S. D. Gosling, and J. W. Pennebaker, "Personality in its natural habitat: Manifestations and implicit folk theories of personality in daily life." Journal of Personality and Social Psychology, vol. 90, no. 5, p. 862, 2006.
29. R. A. Simmons, P. C. Gordon, and D. L. Chambless, "Pronouns in marital interaction: What do you and i say about marital health?" Psychological Science, vol. 16, no. 12, pp. 932–936, 2005.
30. E. Lazega et al., The collegial phenomenon: The social mechanisms of cooperation among peers in a corporate law partnership. Oxford University Press on Demand, 2001.
31. M. L. Newman, C. J. Groom, L. D. Handelman, and J. W. Pennebaker, "Gender differences in language use: An analysis of 14,000 text samples," Discourse Processes, vol. 45, no. 3, pp. 211–236, 2008.
32. J. B. Sexton and R. L. Helmreich, "Analyzing cockpit communications: the links between language, performance, error, and workload," Human Performance in Extreme Environments, vol. 5, no. 1, pp. 63–68, 2000.
33. S. Rude, E. M. Gortner, and J. Pennebaker, "Language use of depressed and depression-vulnerable college students," Cognition & Emotion, vol. 18, no. 8, pp. 1121–1133, 2004.
34. G. W. Wendel-Vos, A. J. Schuit, M. Tijhuis, and D. Kromhout, "Leisure time physical activity and health-related quality of life: cross-sectional and longitudinal associations," Quality of Life Research, vol. 13, no. 3, pp. 667–677, 2004.

35. N. Mutrie and G. Faulkner, “Physical activity: Positive psychology in motion,” Positive Psychology in Practice, pp. 146–164, 2004.

36. L. Cer´on-Lorente, M. C. Valenza, J. M. P´erez-M´armol, M. del Carmen Garc´ıa-R´ıos, A. M. Castro-S´anchez, and M. E. Aguilar-Ferr´andiz, “The influence of balance, physical disability, strength, mechanosensitivity and spinal mobility on physical activity at home, work and leisure time in women withfibromyalgia,” Clinical Biomechanics, vol. 60, pp. 157– 163, 2018.

37. J. W. Pennebaker, “Putting stress into words: Health, linguistic, and therapeutic implications,” Behaviour Research and Therapy, vol. 31, no. 6, pp. 539–548, 1993.



(a) Dissatisfaction (b) Physical health (c) Cooperation (d) Electricity

(e) Dissatisfaction (f) Physical health (g) Cooperation (h) Electricity

Fig. 7: The QQ-Plot of Consumers’ and Prosumers’ Level of Dissatisfaction, Physical Health, and Cooperation, as Well as Cooperation/Severity dependent Level of Electricity, Using the Median of All Samples (Figures A-D) and Three-Hourly-Based Data (Figures E-H).

Global Journals Guidelines Handbook 2023

www.GlobalJournals.org

Memberships

FELLOWS/ASSOCIATES OF COMPUTER SCIENCE RESEARCH COUNCIL

FCSRC/ACSRC MEMBERSHIPS

Introduction

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

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

FCSRC

FELLOW OF COMPUTER SCIENCE RESEARCH COUNCIL

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

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

Benefit

To the institution

Get letter of appreciation

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

Exclusive Network

Get access to a closed network

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

Career | Credibility | Exclusive | Reputation

Certificate

Certificate, LoR and Laser-Momento

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

Career | Credibility | Exclusive | Reputation

Designation

Get honored title of membership

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

Career | Credibility | Exclusive | Reputation

Recognition on the Platform

Better visibility and citation

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

Career | Credibility | Reputation

Future Work

Get discounts on the future publications

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

Career Financial

GJ Account

Unlimited forward of Emails

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

Career Credibility Reputation

Premium Tools

Access to all the Premium Tools

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

Financial

Conferences & Events

Organize seminar/conference

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

Career Credibility Financial

Early Invitations

Early invitations to all the symposiums, seminars, conferences

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

Exclusive

Publishing Articles & Books

Earn 60% of sales proceeds

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

Exclusive Financial

Reviewers

Get a remuneration of 15% of author fees

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

Financial

Access to Editorial Board

Become a member of the Editorial Board

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

Career Credibility Exclusive Reputation

And Much More

Get access to scientific museums and observatories across the globe

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

ACSRC

ASSOCIATE OF COMPUTER SCIENCE RESEARCH COUNCIL

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

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

Benefit

To the institution

Get letter of appreciation

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

Exclusive Network

Get access to a closed network

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

Career | Credibility | Exclusive | Reputation

Certificate

Certificate, LoR and Laser-Momento

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

Career | Credibility | Exclusive | Reputation

Designation

Get honored title of membership

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

Career | Credibility | Exclusive | Reputation

Recognition on the Platform

Better visibility and citation

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

Career | Credibility | Reputation

Future Work

Get discounts on the future publications

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

Career Financial

GJ Account

Unlimited forward of Emails

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

Career Credibility Reputation

Premium Tools

Access to all the Premium Tools

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

Financial

Conferences & Events

Organize Seminar/Conference

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

Career Credibility Financial

Early Invitations

Early invitations to all the symposiums, seminars, conferences

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

Exclusive

Publishing Articles & Books

Earn 30-40% of sales proceeds

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

Exclusive Financial

Reviewers

Get a remuneration of 15% of author fees

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

Financial

And Much More

Get access to scientific museums and observatories across the globe

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

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

Preferred Author Guidelines

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

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

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

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

Before and during Submission

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

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

Declaration of Conflicts of Interest

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

Policy on Plagiarism

Plagiarism is not acceptable in Global Journals submissions at all.

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

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

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

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

Authorship Policies

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

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

Changes in Authorship

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

Copyright

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

Appealing Decisions

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

Acknowledgments

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

Declaration of funding sources

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

Preparing your Manuscript

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

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

Manuscript Style Instruction (Optional)

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

Structure and Format of Manuscript

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

A research paper must include:

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

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

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

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

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

Format Structure

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

All manuscripts submitted to Global Journals should include:

Title

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

Author details

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

Abstract

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

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

Keywords

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

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

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

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

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

Numerical Methods

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

Abbreviations

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

Formulas and equations

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

Tables, Figures, and Figure Legends

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

Figures

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

Preparation of Eletronic Figures for Publication

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

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

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

Tips for writing a good quality Computer Science Research Paper

Techniques for writing a good quality computer science research paper:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Informal Guidelines of Research Paper Writing

Key points to remember:

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

Final points:

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

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

The discussion section:

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

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

General style:

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

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

Mistakes to avoid:

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

Title page:

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

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

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

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

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

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

Approach:

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

Introduction:

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

The following approach can create a valuable beginning:

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

Approach:

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

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

Procedures (methods and materials):

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

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

Materials:

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

Methods:

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

Approach:

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

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

What to keep away from:

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

Results:

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

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

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

Content:

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

What to stay away from:

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

Approach:

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

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

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

Figures and tables:

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

Discussion:

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

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

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

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

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

Approach:

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

Describe generally acknowledged facts and main beliefs in present tense.

The Administration Rules

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

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

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

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

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

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

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

INDEX

save our planet

Global Journal of Computer Science and Technology

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

ISSN 9754350