International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 07 | July - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

Cyber Security Unveiled: Trends and Protections in the Digital World

Haripriya M P [1] , Aleena Jolly[2] , Venkadesh P[3]

[1]*Department of Computer Science, Kristu Jayanti College, Bengaluru*
[2]*Department of Computer Science, Kristu Jayanti College, Bengaluru*
[3]*Department of CSE, V.S.B. College of Engineering, Coimbatore*

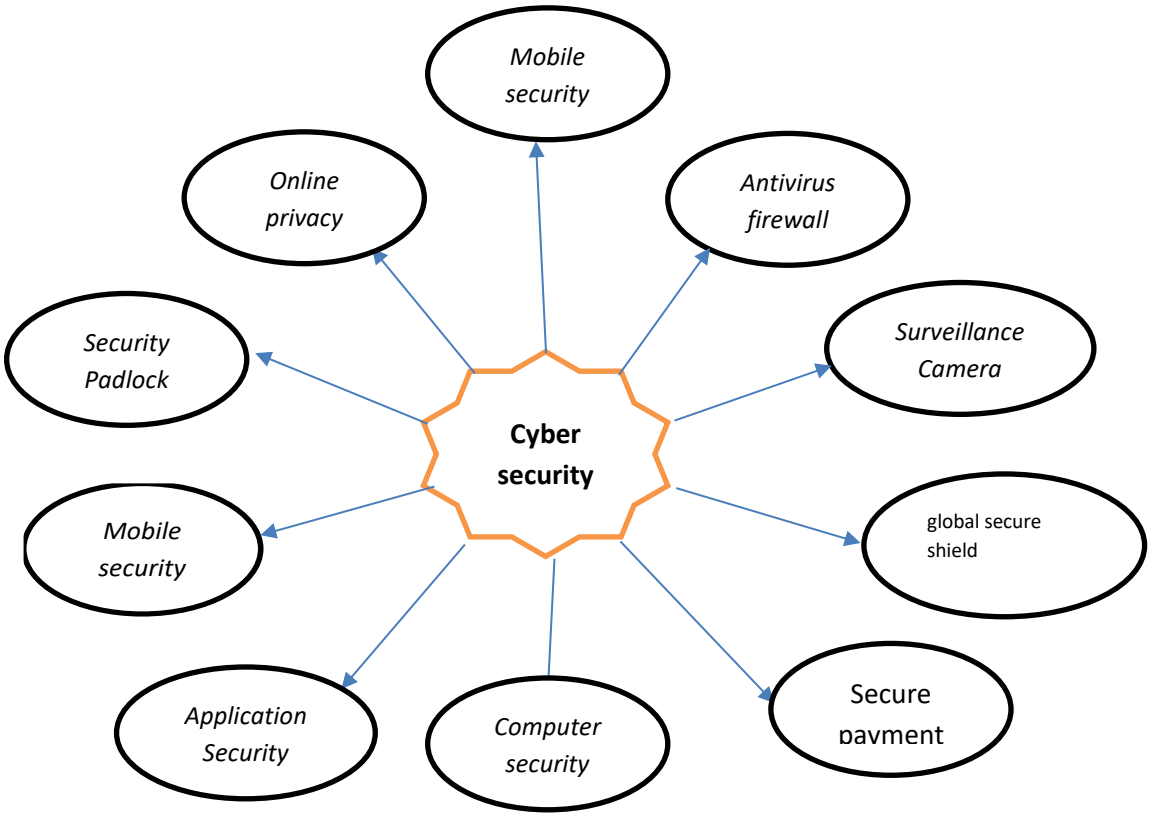
Abstract—

Cybersecurity is the practice of protecting our systems, networks, and programmes from cyber attackers and it aims to access, alter, or destroy sensitive information that affects normal processes. Cybersecurity specialists are constantly searching for new, cutting-edge strategies, where the various methods that cybercriminals can use to attack. According to the Cyber Security & Infrastructure Security Agency (CISA), "Cyber security is the art of protecting networks, devices and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity and availability of information". Cybersecurity protects against theft and loss of all forms of data, including sensitive data, protected health information (PHI), personally identifiable information (PII), intellectual property, personal information, data, and systems used by governments and businesses hence it is essential. One of the most important aspects of cybersecurity is End-user Protection. All software and hardware used by end users must be scanned at regular intervals as there can be malicious threats. The attackers do not fall behind as a result of the advancement of new cyber security systems. They use improved hacking methods and target the weaknesses of numerous companies worldwide. Aside from other things, many people are still very concerned about cyber security. At present cyber security faces, many challenges and this study focuses on user security for the most recent technologies that encountered difficulties.

Keywords— Cyber Security, Cyber Attacks, Defects, Technologies, Hacking.

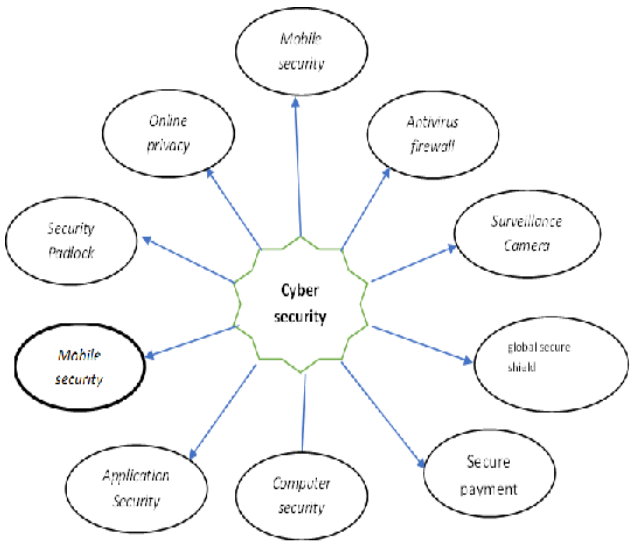
Introduction

Cyber security is the application of technology for defending computers, servers, mobile devices, electronic systems, networks, and data from cyberattacks. It is also known as information technology security or electronic information security. It can be applied in many



varieties context from business to mobile computing. Cyber security is an authority that acts against scandalous actors such as hackers, spammers and cybercriminals to shield devices and services. Although some parts of cyber security are

Fig1: Cyber Security Elements



prepared to strike first, nowadays most of the professionals focus more on finding the best way to protect all assets, from computers and smartphones to networks and databases, from attacks. Medias are using cyber security across the board to aware the process of protection against every form of cybercrime, which is from identity theft to international digital weapons. But some fails to capture the true nature of cyber security for those who don't have a computer science degree or experience in this digital field.

Cisco Systems, a combination of tech specializing in networking, the cloud, and the security defines cyber security as the practice of protecting systems, networks and programs from digital attacks. These cyberattacks are usually

aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. The Scale of Cyber Security Threat According to Forbes,2022 is going to be a pack of various and terrifying cyber security challenges, everything from supply chain disruption to increased smart device risks to a continued cyber security talent drought.

According to Cybercrime Magazine, by 2025 it will cost the world around $10.5 trillion for cybercrime. Moreover, it is predicted that the cost of cybercrime will rise by 15 percent yearly over the next four years. For creating a target rich environment concept such as pandemic, cryptocurrency, and the rise in remote working are coming together so that criminals can take the advantage.

Working of Cyber Security and the Challenges of Cyber Security an overview

The encompassment of technology, processes, and methods to secure computer systems, data, and networks from attacks is the major work cyber security does. To understand what cyber security is and how it works it is divided into a series of subdomains:

Application security: Application security balances the execution of different defenses in an organization's software and services against a various reach of threats. To write secure code, design secure application architectures, implement robust data input validation and more, to minimize the chance of unauthorized access or modification of application resources this sub domain requires cyber security experts.

Cloud security: Cloud security pertain to creating secure cloud architectures and application of companies that use cloud service providers such as Amazon Web Services, Google, Azure, Rackspace, etc.

Identity Management and Data Security: This security system balances the activities, frameworks, and processes that enable authorization and authentication of legalized individuals to an organization's information system. For implementing powerful information storage mechanisms that protects data these measures are involved, whether in transition or residing on a server or computer. Besides, this security system makes greater use of authentication protocols, whether two-factor or multi-factor.

Mobile security: As people rely on mobile devices more nowadays mobile security is considered as a big deal. It is to secure organizational and personal information stored on mobile devices like cell phone, tablet and laptops from threats such as unauthorized access, device loss or theft, malware, viruses etc. To amplify security mobile security employs authentication and education.

Network security: Network security covers hardware and software mechanism which can

secure the network and infrastructure from disruptions, unauthorized access, and other abuses. To protect organizational assets against a vast range of threats from within or outside the organization an effective and strong network security is needed.

Disaster recovery and business continuity planning: This subdomain maintains processes, alerts, monitoring, and plans designed to help organizations make ready for keeping their business-critical systems running whenever any sort of incident happens like massive power outage, fires, natural disasters, and resuming and recovering lost operations and systems in the incident's aftermath.

User definition: Awareness of cyber threats by staff is very important in the cyber security puzzle. Providing training to business staff on the fundamentals of computer security is essential to bring up awareness about industry best practices, organizational procedures and policies, monitoring, and reporting suspicious, malicious activities. It covers cybersecurity-related classes, programs, and certifications.

Types of Cyber Security Threats

Computer-assisted crimes, crimes where the computer itself is a target, and crimes where the computer is incidental to the crime rather than directly related are the three generally recognized classification of cybercrimes.

- **Cyberterrorism**-this a politically-based attack to create harm and widespread social disruption on computer and information technology.
- **Malware**-this threat enclose ransomware, spyware, viruses, and worms. It can install harmful software, block access to your computer resources, disrupt the system, or covertly transmit information from your data storage

- **Trojans**-Like the mythology of legendary Trojan Horse, this attack is in the form a trick which make users think that they are opening a harmful file. Once it is in the place it attacks the system, it is like establishing a backdoor that allows access to cybercriminals.
  - **Botnets**-this attack involve large scale cyberattacks which is conducted by remotely controlled malware infected devices. It is like one coordinating cybercriminal controls a string of computers, later compromised computers become part of the botnet system.
  - **Adware**-it is in the form of malware. It is also known as advertisement-supported software. This virus is a potentially unwanted program (PUP) installed without your permission and automatically generated unwanted online advertisements.
  - **SQL injection**-a structured query language attack inserts malicious code into a SQL-using server.

- **Phishing**- Through false communication, especially e-mail, hackers fools the recipient into opening it and led them to follow instruction that typically ask for their personal information.

- **Man**- In-the-middle attack in this attack hackers insert themselves into two-person online transaction. Hackers can filter and steal desired data. This attack usually happens on unsecured public Wi-Fi network.
- **Denial of service**- This is a cyber attack that floods a network or computer with an overwhelming amount of "handshake" processes, effectively overloading the system and making it incapable of responding to user requests.

Advantages of Cyber Security:

Cyber security is mainly focused on protecting devices and systems from cybercriminals. Every bits and bytes of this process is hard to visualize, its much better to focus on the effects. Without this hard work many websites would be impossible to enjoy due to ever-present denial-of-service attack attempts. Without cyber security defense, it is possible to destroy modern-day essentials like the power grid and water treatment facilities that keep the world running smoothly. Cyber security is very important that it is what helps to prevent the lifestyles we have come to know and enjoy.

CIA Triad: Security of any organization start with three principle which are, confidentiality, integrity, availability. This is called CIA, which has served as the industry standard for computer security since the time of first mainframes.

- **Confidentiality**: The principle of this asserts that only authorized parties can access sensitive information and function. Example: Military secrets.
- **Integrity**: Only authorized people and means can alter, add, or remove sensitive information and functions. Example: A user entering incorrect data into the database.
- **Availability**: Systems, functions, and data must be available on-demand according to agreed-upon parameters based on levels of service.

Comparison Analysis

According to Cybersecurity[4] risks can be reduced by constantly monitoring sources of threat information. However, according to them, the sheer amount of written or printed information that needs to be processed by security analysts is huge. It requires everyday work to disentangle the threats from the bluster. They suggested a novel approach to represent the applicability and effectiveness of the cyber-security text that represents subjective importance to the user in quantitative numbers. They introduced the custom Named Entity Recognition (NER) model using over 17 million words and created a Cyber-security Knowledge Graph (CKG) with 221,202 semantic tuples to develop features that would denote and speculate the significance and subjective relevance of the

cyber-security text to the user and generate correlation attributes. The significance of the text is checked in terms of its textual resemblance with different repositories of pre-defined "significant" text. The maximum number of likenesses are calculated. These analyses act as features to generate an effective score with a massive amount of text. The effectiveness of their suggested architecture could not be verified directly on the basic test records. The experimental result showed that the widespread system could choose the importance and relevancy of the unstructured text within a steady environment with 88% accuracy by manipulating. the experimentation has to be improved as it is unimaginable to expect the controlled environment in a real-life situation, to reconcile the fake dataset with real-life data. The entire design would be able to run a full cycle as depicted by them with the help of a relation extractor which continuously improves the Cyber Security Knowledge Graph by extracting the relations from the cyber-security text and constructing a more extensive one.

According to [5], due to the increasing use of Internet of Things (IoT) enabled applications, such as linked electric vehicles, power electronics systems have grown more exposed to cyber-physical dangers. The IEEE Power Electronics Society recently created a cyber-physical security program in response to this growing requirement. Connected electric cars are experiencing higher cyber-physical security difficulties as a result of rising connections brought on by Vehicle-to-everything and the number of electronic control units. This research paper largely concentrates on the network security of internal combustion engine cars and neglects to particularly address the cyber-physical security of EVs. From the perspectives of firmware security, car charging safety, powertrain control security, the issues and potential solutions for connected electric vehicle cyber-physical security are covered in their article. Investigations on the vulnerabilities of EVs are conducted under a range of cyberattacks, from those motivated by energy efficiency to those driven by safety.

To further assess the effects of the cyberattack on device and system levels, simulation findings, including hardware-in-the-loop (HIL) results, are presented. More significantly, a design for the next power electronics systems is put out to solve the cyber-physical security issues with EVs. Finally, future research directions are thoroughly reviewed. These include model-based and data-driven detection and mitigation, as well as detection and migration for firmware security. The cyber-physical security of contemporary EVs has been thoroughly examined in this research, with a focus on three representative parts of the powertrain system in particular: 1) ECU firmware; 2) Vehicle-to-grid in-vehicle charging system; and 3) Powertrain control system, which consists of device-level electric drive systems and system-level energy management systems. Practical

advice is also provided, along with some early security assessment findings for the powertrain control system, which is further broken down into the powertrain control system and the electric drive system. Finally, a thorough discussion of cutting-edge firmware, model-based and data-driven detection, diagnostic, and mitigation prospects are presented. Powertrain systems' cyber-physical security concerns as well as potential upgrades are highlighted.

A cross-layered experimental platform prototype has been created to facilitate cyber security evaluation and upgrading of cyber-physical systems [6]. A modular strategy was used to make the prototype adaptable. There are four parts in total: platform management, security enhancement, security evaluation, and attack scenario generation. The design approach and choice of architecture for this platform have been explored in relation to standard cyber-enabled industrial control systems. A prototype hardware-based cyber security assessment and enhancement platform has been put into place on a lab-scale cyber-physical system to show the usefulness of the proposed platform and to give interested readers more information. To show how the platform operates and to test its features in the case of a security breach, two types of cyber-attacks have been taken into consideration. The outcomes have shown that the design process works well for real-world cyber-physical systems, and the platform is a good resource for finding vulnerabilities, analyzing them, and comparing the efficiency of various security augmentation techniques. This article has looked at issues related to strengthening the cyber-attack endurance of cyber-physical systems and assessing their cyber security.

A platform for security evaluation and upgrading has been created to get an efficient solution. The design philosophies and reasonings for choosing this particular arrangement are also highlighted. This platform was built using a modular approach to simplify the administration of the necessary capabilities and to ease operation. Detecting possible cyberattacks and minimizing their effects, assessing the performance of each functional unit as well as the entire system, and monitoring the platform's overall functioning. Using industrial communication networks and a genuine lab-scale cyber-physical system, a prototype platform has been created and built in order to offer design details and illustrate operating processes. To give readers a thorough understanding of this platform's functionality and use, three case studies have been done on it. It is presumed that other readers in this crucial field of research will find the material in its design, building, and operation to be of great use.

Numerous issues for the effective application of cyber security to crucial digital assets at nuclear power plants as the importance of cyber security for nuclear power plants has recently increased [7]. Analysis and research are

crucial to determine how to implement nuclear cyber security standards and what supporting elements are included in the whole procedure for a nuclear security technology system. Through various cyber security techniques including assurance, evaluations, and the software development life cycle, the complementing aspects of nuclear cyber security technology may be examined. Effective nuclear cyber security technology application is required in line with a nuclear facility's operation, assurance, and system development process. The findings of this investigation might be used to develop technical guidelines for the future cyber security of vital digital assets at nuclear power plants, as well as technologies that will need to be at the right degree of cyber security to provide technical confidence. This research presents a novel way for contrasting and analyzing different approaches in the field of cyber security in order to identify compatible areas for the usage of cyber security in nuclear power plants. Cyber security approaches are used to create, apply, evaluate, and regulate cyber security in nuclear digital critical systems in this research. Infrastructure cyber security is challenging to find techniques for applying, prevention, detection, analysis, reaction, recovery, and risk evaluation, which should be taken into account in nuclear cyber security. Nuclear cyber security has lately been regarded to be also crucial. All the important systems in these digital systems ought to have cyber security features and defences created for these problems in order to guarantee security against cyberattacks. The sections discuss how many organizations and standard publications have published cyber security standards relating to infrastructure. Legal guidelines nuclear cybersecurity-related RGs have also been announced, however, developers, operators, and regulators are concerned about how to successfully implement these criteria for CDAs at NPPs. Because cyber security has been studied and developed in IT for a long time, it is useful to utilize this knowledge to compare and analyse the various strategies used in general cyber security in order to understand the needs necessary in nuclear cyber security. Understanding both the communications technology of NPPs and cyber security is vital for nuclear cyber security. It is not possible to apply conventional cyber security techniques as they are incompatible with nuclear regulations, development, assessment, and operation.

The analysis presented in the work may be applied to comprehend nuclear regulations' needs as well as supplementary nuclear cyber security issues. To improve cybersecurity, which is crucial in infrastructure facilities. Cybersecurity for nuclear weapons should take into account technical advancements that can raise the level of confidence in the future. First, a system that may improve the assurance level of nuclear cybersecurity at a company like a research centre has to be created by adding the elements specified

in this article. The study, methodologies, and complementing points suggested in this research might be applied to improve the cyber security of NPPs. The suggested methodologies, according to the authors, would, for the first time, provide a direction for addressing the nuclear cyber security challenges and aid in the discovery of deficiencies in nuclear cyber security schemes. Additionally, if the suggested complimentary ideas and schemes mentioned in their study are further examined and explored there is a chance of exploring new conclusions.

For cyber-physical systems (CPSs) under denial-of-service (DoS) attacks, where DoS assaults exist in both the sensor-to-controller (S-C) channel and the controller-to-actuator (C-A) channel, an active security control strategy is suggested in this study [8]. The maximum number of continuous DoS assaults in both the S-C and the C-A channels should be seen as being constrained due to the cost restrictions of attacks. Next, a proactive security control approach is developed to guarantee that the control inputs are modified on time throughout each period in order to fight against two-channel DoS assaults. A security control system that includes both the present and future control inputs is being built in the meanwhile. The addressed CPS against two-channel DoS assaults can be asymptotically stable under the active security control method and security controller without sacrificing control performance. Lastly, simulations and tests are provided to show the viability of the suggested active security control strategy. The number of maximum continuous DoS assaults in both the SC and the C-A channels is thought to be constrained due to the cost restrictions of attacks, and an active security control technique has been developed for CPSs under the two-channel DoS attacks. The active security control method in the algorithm has been created to actively fight against two-channel DoS assaults and can guarantee that there are suitable control inputs to be updated in each period. The closed loop system produced by the active security control technique is comparable to the situation without DoS assaults, it can be deduced from the theorem. Another algorithm has provided the security controller design process. However, a lot of the physical processes in CPSs are noisy and nonlinear.

The Cyber Supply Chain (CSC) system is intricate, with several sub-systems carrying out diverse functions [9]. The inherent weaknesses and risks from any portion of the system can be exploited at any point throughout the supply chain, making supply chain security complex. The general business continuity may be severely disrupted by this. Therefore, it is crucial for organizations to comprehend and assess hazards in order to implement the essential control mechanisms for supply chain security. Cyber Threat Intelligence (CTI) uses a variety of features, such as threat actor expertise and motive, tactics, techniques, and procedure (TTP), and

indicators of compromise, to identify unknown to recognized threats (IoC). In order to increase the security of the cyber supply chain, this research analyses and forecasts risks. To analyse and forecast attacks based on CTI features, we combined machine learning (ML) techniques with cyber threat intelligence (CTI). This enables the identification of the innate CSC vulnerabilities so that the proper control measures may be performed to enhance cybersecurity generally. The Microsoft Malware Prediction dataset is used to create predictive analytics utilising a number of ML algorithms, including Logistic Regression (LG), Support Vector Machine (SVM), Random Forest (RF), and Decision Tree (DT), in order to show the applicability of our methodology. Attack and TTP are considered input parameters for the experiment, whereas vulnerabilities and Indicators of Compromise (IoC) are considered output parameters. The outcomes of the forecast show that spear phishing and spyware/ransomware are the most expected dangers in CSC. To counter these concerns, they have also provided pertinent control recommendations. In order to strengthen CSC's overall cyber security, they recommend leveraging CTI data for the ML predicate model. In the fields of transportation, energy, healthcare, manufacturing, and communication, the integration of complex cyber-physical infrastructures and applications in a CSC environment has had an economic, commercial, and societal influence on both the national and international settings. CPS security is still an issue, though, because any vulnerability inside the system might put the entire supply chain at risk. Through the integration of CTI and ML for threat analysis and prediction, this research seeks to enhance CSC security. The results of the experiment demonstrated the accuracy of the LG, DT, SVM, and RF algorithms in Majority Voting and named a number of predicted dangers. They also noted that CTI is efficient in extracting threat information, which may be integrated into ML classifiers for threat prediction. This enables the CSC organization to evaluate the currently in place measures and identify new controls for enhancing overall cyber security [8].

Future Studies

Future studies which give a path to the active security control approach for nonlinear CPSs. To generalize their findings, it is required to take into account the industrial case study and complete automation of the process [9]. On the basis of the outcomes of their predictions, we also intend to evaluate the current controls and any required additional controls in the future [10]. By 2025, India alone is predicted to create more than 1.5 million jobs in the cybersecurity industry, according to global recruiting firm Michael Page.

Conclusion

With a particular emphasis on representative applications, we survey the literature on security and privacy of cyber physical systems for the Internet of Things (ICS), smart grids, medical gadgets, and smart cars. A taxonomy of dangers, weaknesses, known assaults, and available controls is presented in wide range[11][12]. As well as a framework for cyber-physical security that includes Cyber physical system components that affect security. In future the IoT system with these factors may also leads to the security with effective combinations. The long-term network coverage that allows more people to use smart gadgets with strong security. [13]. The structure includes what can happen if a Cyber Physical system is attacked in its physical realm unanticipated repercussions in the online world and vice coupled with suggested remedies, vice versa. It is possible to create efficient controls to get rid of cyber-physical attacks. As an illustration, we discovered that the heterogeneity of Components of cyber physical systems play a crucial role in many attacks.

References

[1] Bhuyan, Soumitra Sudip, et al. "Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations." Journal of medical systems 44.5 (2020): 1-9.

[2] Jin Ye, Lulu Guo, Bowen Yang, Fangyu Li, Liang Du, Le Guan, and Wenzhan Song ,2021,Cyber-"Physical Security of Powertrain Systems in Modern Electric Vehicles: Vulnerabilities, Challenges and Future Visions",2015.

[3] Larsen, Per, et al. "SoK: Automated software diversity." 2014 IEEE Symposium on Security and Privacy. IEEE, 2014.

[4] Abomhara, Mohamed, and Geir M. Koien. "Security and privacy in the Internet of Things: Current status and open issues." *2014 international conference on privacy and security in mobile systems (PRISMS)*. IEEE, 2014.

[5] Xirong Ning and Jin Jiang Design, Analysis, and Implementation of a Security Assessment/Enhancement Platform for Cyber-Physical Systems", *IEEE Access,2017.*

[6] Švábenský, Valdemar, Jan Vykopal, and Pavel Čeleda. "What are cybersecurity education papers about? a systematic literature review of sigcse and iticse conferences." *Proceedings of the 51st ACM* technical symposium on computer science education. 2020.

[7] Shaukat, Kamran, et al. "A survey on machine learning techniques for cyber security in the last decade." IEEE Access 8 (2020): 222310-222354.

[8] Tongxiang Li, Bo Chen, "Active Security Control Approach Against DoS Attacks in Cyber-Physical Systems"," Computational and

mathematical organization theory 26.4 (2020): 365-381.

[9] Otgonpurev Mendsaikhan, Hirokazu Hasegawa, Hajime Shimada," Quantifying the Significance and Relevance of Cyber-Security Text Through Textual Similarity and Cyber-Security Knowledge Graph", 2014, IEEE Access.

[10] Kumar, Rajeev, et al. "Fuzzy-based symmetrical multi-criteria decision-making procedure for evaluating the impact of harmful factors of healthcare information security." Symmetry 12.4 (2020): 664.

[11] Carley, Kathleen M. "Social cybersecurity: an emerging science." Computational and mathematical organization theory 26.4 (2020): 365-381.

[12] Von Solms, Rossouw, and Johan Van Niekerk. "From information security to cyber security." computers & security 38 (2013): 97-102.

[13] Haripriya, M. P., and P. Venkadesh. "Feature Selection Based on IoT Aware QDA Node Authentication in 5G Networks." INTELLIGENT AUTOMATION AND SOFT COMPUTING 33.2 (2022): 825-836.