http://www.inosr.net/inosr-scientific-research/
Eze *et al*
INOSR Scientific Research 9(1):13-24, 2023.

International Network Organization for Scientific Research ISSN: 2705-1706

A Study of Cyber Security Threats, Challenges in Different Fields and its Prospective Solutions: A Review

Val Hyginus U. Eze[1], Chinyere Nneoma Ugwu[1] and Ifeanyi Cornelius Ugwuanyi[2]

[1]Department of Publication and Extension, Kampala International University, Uganda
[2]Department of Electronic Engineering University of Nigeria Nsukka, Nigeria
Email: udoka.eze@kiu.ac.ug, ugwun@kiu.ac.ug, cornelius.ugwuanyi@unn.edu.ng

ABSTRACT

This paper reviewed the implications, challenges and the effects of cybercrimes and cybersecurity in the society. It fully defined cybersecurity based on governmental and national view, industrial view and academic view. From this it was concluded that cyber security and cyber-attack is best defined and prevented based on the field of research. This paper review 27 articles on cyber security and cybercrimes and it showed that cyber security is a complex task that relies on domain knowledge and requires cognitive abilities to determine possible threats from large amounts of network data. This study investigates how knowledge in network operations and information security influence the detection of intrusions in a simple network. This research paper also reviewed different strategies used by different researchers to prevent cyber-attack in different areas of work and also exposed the most recent used cyber security attacks, preventions, future threats and prospective ways to avoid cyber-attacks.
Keywords: Cyber Security, Threats, Challenges and Different Fields

INTRODUCTION

The most widely utilized sources of gathering both information and data in this 21st century is through internet. In the year 2017 the internet usage by the total world population was 48% and it rapidly increased to 81% in the developed countries. The transfer of information from one node to another over the network is the primary aim of internet. The innovation of computer systems, networks, and mobile devices has drastically increased the use of the internet. Internet is a universal collection of millions of distinct interconnected computers, networks, and associated devices for effective data delivery. These data that were transferred from one computer to another contains a very vital information which needs to be protected. Due to this spontaneous increase in the internet usage and the vital and huge amount of data that were conveyed from a computer to the other, it becomes a good target for cybercriminals [1] [2]. The integrity and security of a computer system are compromised when an illegal penetration, unauthorized individual or program enters a computer or network intending to harm or disrupt the normal flow of activities. The Information and Communication Technology (ICT) has brought great convenience in human life and efficacy in governance. With the increasing reliance on ICT and sophistication of attack methods, the trend of cyber-attacks has changed from small-scale intrusion attempts and financial breaches to highly organized state-sponsored attacks [3]. These cyber-attacks led to introduction of cyber security and its strategies to prevent the harmful cyber-attacks. Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights." Articulating a concise, inclusive, meaningful, and unifying definition will enable an enhanced and enriched focus on interdisciplinary cybersecurity dialectics and thereby will influence the approaches

of academia, industry and government and non-governmental organizations to cybersecurity challenges [4].

However, human factor is one of the underlying reasons why many cyber-attacks were successful because the uneducated computer user is the weakest link targeted by cyber criminals using social engineering. Formal cyber security awareness is required to mitigate the exploitation of human vulnerabilities by computer hackers and attackers [5], [6]. Cyber security is the set of security measures that can be taken to protect the cyberspace and user assets against unauthorized access and attacks. It is clear from this point of view that there is every tendency for the cyber criminals to attack any data base that contains a vital information that can lead to exposure of that particular database. Furthermore, all the sectors and areas of human endeavor are now the targets of the cyber-attackers to get access into their privacy, hack, collect vital information and make it prone to the public [7]. It is getting more and more challenging to fight against these cyber security attacks and to keep a match with the speed of security attacks. Currently, researchers are focusing on the urgent need of finding new automated security methods to curb these cybersecurity challenges. This paper mainly focused on reviewing most recent techniques and strategies deployed by researchers to curb this cyber-attacks/menace in the society.

Definitions of Cyber Security

Cyber security can be defined based on the field of study and the contextual area of view from the researcher. It was also observed that there is no uniform definition from the introduction and different reviewed papers in this research work. It is based on these fields such as industrial view, Government and National state view and academic views that cyber security definitions were drawn as follow:

Industry Definitions

This aspect defined cyber security with respect to industrial view. It described cyber security as a security practice that is related to the combination of offensive and defensive actions involving or relying upon information technology and/or operational technology environments and systems. It is also defined as information security based on a short analysis of the 'cyber' component which is described as the use of information technology and computers. In official guidance, ISACA described cyber security as impunities emerging within the fields of information security and traditional security [8]. All these definitions of cyber security are based on industrial perspective of view and it is generally acceptable within the context.

Academic Definitions

Cyber security is academically defined as the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights [4]. Cyber security are techniques generally set forth in published materials that attempt to safeguard the cyber environment of a user or organization. It refers to the body of technologies, processes and information technology security [9]. Cyber security is the set of security measures that can be taken to protect the cyberspace and user assets against unauthorized access and attacks. It is clear from this point of view that there is every tendency for the cyber criminals to attack any data base that contains a vital information that can lead to exposure of that particular database.

Government and Nation State Definitions

Cyber-security has no single definition, it has been defined by different researchers as a branch of information security. It is further defined as information security with jurisdictional uncertainty and attribution issues [8]. It is also defined as the attack on the security of an organization or firm which affects its

normal operation and as well makes the organizations vital information prone to the public. All these are generally acceptable under governmental and nation state view.

Overview of Cyber-Security

This section of the paper reviewed 15 most recent papers in cyber security and its related works. It also compared and contracted the effects and implications of cyber security threats together with the prospective solutions.

Study of Cyber Security on Latest Technologies

In [2], Cyber Security plays an important role in the field of information technology. This reviewed the most important trending areas where the cyber-attackers are more interested to hack as: web servers, cloud computing and services, Advanced Persistent Threats and targeted attacks, mobile networks, IPv6 (new internet protocol) and encrypted codes. These are the new emerging fields where cyber attackers are seriously concentrating to attack. This paper also highlighted on some preventive measures such as the use of Anti- virus software, authentication of data, access control and password security, malware scanners and firewalls. There is no perfect solution for cyber-crimes but this paper has best minimized the Techniques in order to have a safe and secure future in cyber space. The author in [10], reviewed and discussed some cyber-security measures using freeware/shareware.

Cyber Security in blockchain

In [11], this paper discussed cyber security in the field of bitcoin. This research identifies peer-reviewed literature that seeks to utilize blockchain for cyber security purposes and presents a systematic analysis of the most frequently adopted blockchain security applications. Our findings show that the Internet of Things (IoT) lends itself well to novel blockchain applications, as do networks and machine visualization, public key cryptography, web applications, certification schemes and the secure storage of Personally Identifiable Information (PII). This timely systematic review also sheds light on future directions of research, education and practices in the blockchain and cyber security space, such as security of blockchain in IoT, security of blockchain for AI data, and sidechain security.

Cyber Security using Machine Learning

In [1], the reviewer how machine learning can be used to detect and curb cybersecurity in various areas of human life in the society. Cyber security techniques provide enhancements in security measures to detect and react against cyberattacks. The previously used security systems are no longer sufficient because cybercriminals are smart enough to evade conventional security systems. Conventional security systems lack efficiency in detecting previously unseen and polymorphic security attacks. Machine learning (ML) techniques are playing a vital role in numerous applications of cyber security. However, despite the ongoing success, there are significant challenges in ensuring the trustworthiness of ML systems. There are incentivized malicious adversaries present in the cyberspace that are willing to game and exploit such ML vulnerabilities. This paper reviewed the ML techniques for cyber security including intrusion detection, spam detection, and malware detection on computer networks and mobile networks in the last decade. It also provides brief descriptions of each ML method, frequently used security datasets, essential ML tools, and evaluation metrics to evaluate a classification model. It finally discusses the challenges of using ML techniques in cyber security.

Cyber security in New Space

In [12], the security of satellites and its challenges were discussed in this paper. New and proposed constellations will increase the in-orbit satellite population by the order of thousands, expanding the threat landscape of the space industry. This article analyses past satellite security threats and incidents to assess the

motivations and characteristics of adversarial threats to satellites. The ground and radio frequency communications were the most favored targets; however, the boom of satellites constellations in the upcoming years may shift this focus towards the space segment which must be addressed. Key technology advancements and open issues in the satellite industry related to security and operational requirements are also discussed in this paper.

Cyber Security using Artificial intelligence

In [13] the author discussed the active use of artificial intelligence to resolve a number of ethical and legal problems cyber security attack. The ethical framework for the application and use of data today is highly blurred, which poses great risks in ensuring data confidentiality. In the article, the authors analyzed in detail the main problems in the field of cybersecurity in connection with the active use of AI. The study identified the main types of criminological risks associated with the active implementation of AI. The authors argued the position about the need to recognize AI as a source of increased danger. This involved the use of AI to solve the problems of cyber-attack.

Comparative Analysis of Various National Cyber Security Strategies

In [3] the author reviewed the intrinsic vulnerabilities in the cyberspace and ever-escalating cyber-attacks which tends to continuously threaten the national security, economy and daily life of citizens. This reviewed paper analyzes and compares National Cyber Security Strategies of twenty countries based on the documented legal, operational, technical and policy-related measures. The majority of the strategies have described the need of appointing an official body for leading the cyber security tasks at the national level and establishment of Computer Emergency Response Teams (CERT/CSIRT) to fight cyber-attacks targeting national cyberspace. However, disparity lies in the understanding of major key terms (particularly cyber security and cyberspace), characterization of the cyber threats, aims and description of cyber awareness and capacity building programs, legislative measures etc. Based on the comparison, the research specifies and recommends best practices for improving the state of national cyber security and resilience. The countries planning to develop or update their cyber security strategies can use this review paper of [3].

Cyber Security of Critical Infrastructures

In [14] Modern Supervisory Control and Data Acquisition (SCADA) systems are essential for monitoring and managing electric power generation, transmission and distribution. In the age of the Internet of Things, SCADA has evolved into big, complex and distributed systems that are prone to be conventional in addition to new threats. Many security methods can be applied to such systems, having in mind that both high efficiency, real time intrusion identification and low overhead are required. The synergy between the ICS and the IoT has emerged largely bringing new security challenges. The author identified key security issues for ICS and current solutions. Future work should primarily focus on the balance between holistic approaches that can deal with a wide variety of attacks, real time identification of intruders with high accuracy and solutions that impose low overhead to the communication and performance of SCADA/ICS systems.

Cyber Security, Cyber Threats, Implications and Future Perspectives

In [15], the results showed a deeply ingrained preventative mindset, driven by a desire to ensure the availability of technology and services and a general lack of awareness of enterprise security concerns. While other tactics were evident, they were also preventative measures. The article discussed research agenda for deploying multiple strategies across an enterprise and also focused on how to combine, balance, and optimize systems for effective output. This research looked at various topics, including information security and areas where security strategy is likely to be discussed, such as military sources. There are nine security strategies

identified in this reviewed article that will effectively curb cyber security menace. A qualitative focus group approach is used to determine how these security strategies are used in organizations. In focus groups, security managers from eight organizations were asked to discuss their organizations' security strategies. Finally, it was observed from this paper that organizations use a preventive approach to keep technology services available. Some of the other identified methods were used to support the prevention strategy on an operational level.

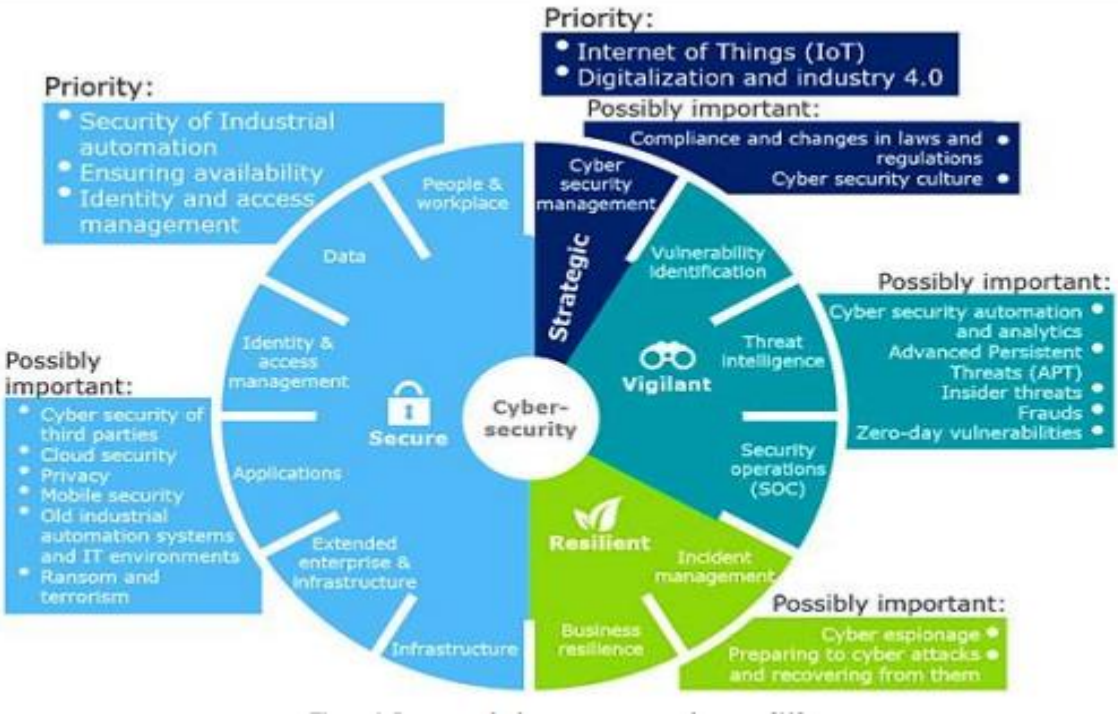

Figure 1: Priorities of cyber security in manufacturing [15]

The evaluation of the articles concentrated on four areas of examination. These areas include: (1) an examination of cybersecurity and Industry (2) an examination of industry types and industrial assets most affected by cybersecurity issues (3) a definition of system vulnerabilities, cyber threats, risks, and countermeasures to be taken in Industry 4.0 scenarios; and (4) the identification of guidelines and more structured solutions to deal with cybersecurity issues. As a consequence, each area's major elements were outlined in a reference framework. The framework gathers and summarizes the most referenced evidence for each area of investigation in order to provide an immediate possibility of synthesis that can be used to guide future research as well as management activities. Although a variety of solutions for dealing with cybersecurity challenges in Industry have been created, none of them take into account the three exposure layers of Cyber-Physical Systems (physical, network, and computer) that might be exploited by cyber-attacks at the same time. Future research can use this study as a platform for addressing industrial investigations and expanding the existing state of the art security cyber techniques.

Cyber Security in Smart Grid (Renewable and Non-Renewable Energy)

In [16] smart grid uses the power of information technology to intelligently deliver energy by using a two-way communication and wisely meet the environmental requirements by facilitating the integration of green technologies. The inherent weakness of communication technology has exposed

the system to numerous security threats. Several survey papers have discussed these problems and their countermeasures. However, most of these papers classified attacks based on confidentiality, integrity, and availability, but they excluded the accountability. In addition, the existing countermeasures focus on countering some specific attacks or protecting some specific components, but there is no global approach to secure the entire system. This paper reviewed the security requirements, provides descriptions of several severe cyber-attacks, and propose a cyber-security strategy to detect and counter these attacks. This also showed how renewable energy can be used as source of energy generation, how to optimize it and finally reviewed different solar photovoltaic systems. The solar photovoltaic optimization which includes maximum power point tracking of solar photovoltaic panels is also part of this review and how to use to generate energy for construction of solar Electric Vehicle (EV) charge stations [17], [18]–[23]

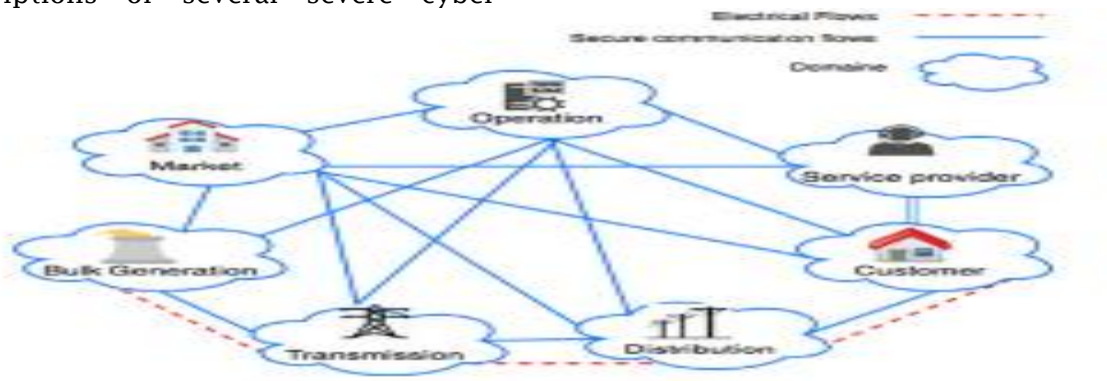

Figure 2: Smart grid's conceptual model based on NIST

According to the National Institute of Standard and Technology (NIST), a smart grid is composed of seven logical domains: bulk generation, transmission, distribution, customer, markets, service provider, and operations, each of which includes both actors and applications. Actors are programs, devices, and systems whereas applications are tasks performed by one actor or more in each domain. Fig. 2 shows the conceptual model of smart grid and the interaction of actors from different domains via a secure channel. Within the customer domain, the main actor is the end user. Generally, there are three types of customers: home, commercial/building, and industrial. In addition to consuming electricity, these actors may also generate, store, and manage the use of energy. This domain is electrically connected to the distribution domain and communicates with the distribution, operation, service provider, and market domains. In the market domain, actors are the operators and participants in the electricity markets. This domain maintains the balance between electrical supply and the demand. In order to match the production with demand, the market domain communicates with energy supply domains which include the bulk generation domain and distributed energy resources (DER). The service provider domain includes the organizations that provide services to both electrical customers and utilities. These organizations manage services such as billing, customer account, and use of energy. The service provider interacts with the operation domain for situational awareness, system control and also communicates with customer and market domain to develop smart services such as enabling customer interaction with market and energy generation at home [2]. The operations domain's actors are the managers of the movement of electricity. This domain maintains efficient and optimal operations in transmission and distribution. In transmission, it uses energy management systems (EMS), whereas in distribution it uses distribution

management systems (DMS). Actors in the bulk generation domain include generators of electricity in bulk quantities. Energy generation is the first step in the process of delivering electricity to the end user. Energy is generated using resources like oil, flowing water, coal, nuclear fission, and solar radiation. The bulk generation domain is electrically connected to the transmission domain and communicates through an interface with the market domain, transmission domain, and operations domain. In the transmission domain, generated electrical power is carried over long distances from generation domain to distribution domain through multiple substations. This domain may also store and generate electricity. The transmission network is monitored and controlled via a supervisory control and data acquisition (SCADA) system, which is composed of a communication network, control devices, and monitoring devices. The distribution domain includes the distributors of electricity to and from the end user. The electrical distribution systems have different structures such as radial, looped, or meshed. In addition to distribution, this domain may also support energy generation and storage. This domain is connected to the transmission domain, customer domain, and the metering points for consumption.

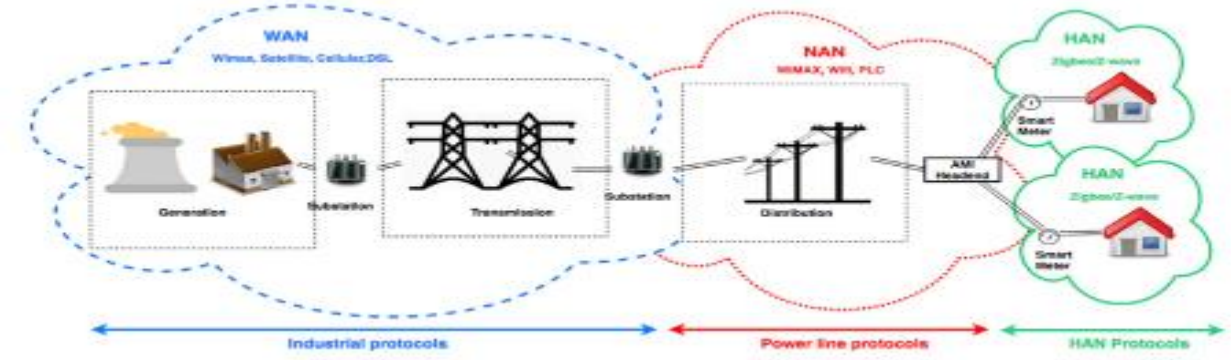

Figure 3: Illustration of the smart grid architecture

Distributed and heterogeneous applications in smart grid require different communication protocols. Figure 3, illustrates the smart grid network architecture and the protocols used within each network. In the home area network (HAN), home appliances use ZigBee and Z-wave protocols. In the neighborhood area network (NAN), devices are usually connected via IEEE 802.11, IEEE 802.15.4, or IEEE 802.16 standards. In the wide area network (WAN) and in supervisory control and data acquisition (SCADA) applications, several industrial protocols are used especially distributed networking protocol 3.0 (DNP3) and Modicon communication bus (ModBus). Some authors have proposed the use of cognitive radio based on the IEEE 802.22 to address the problem of scarcity of wireless resources and improve the smart gird's communication in the wide area network [16].

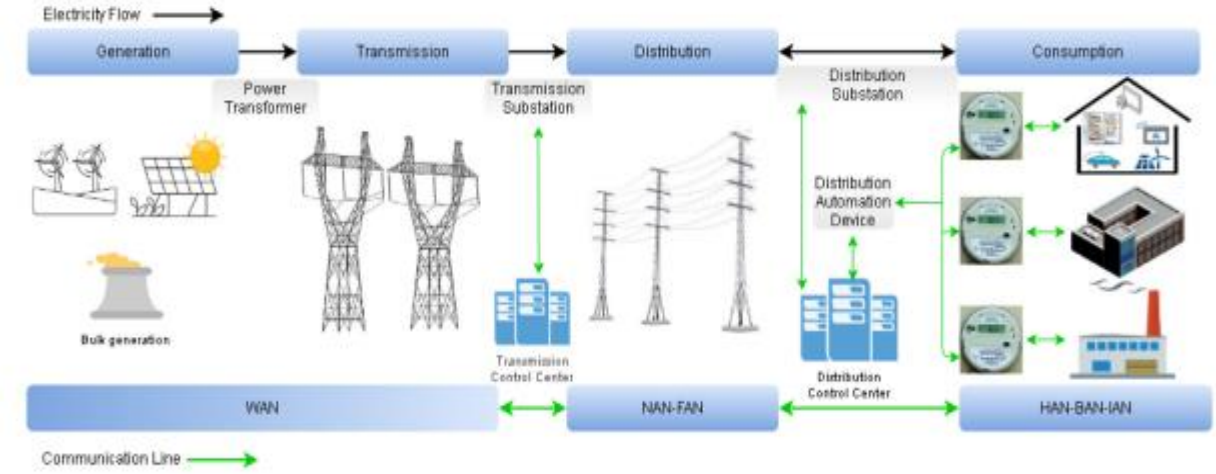

Figure 4: Smart grid electricity transmission process from generation to consumer

The Smart grid applications have four main stages shown as in Figure 4, These are generation, transmission, distribution, and consumption [16, 17, 18, 19, 20, 21, 22]. Energy has different types such as geothermal heat, flowing water, solar radiation, wind, hydro plants, chemical combustion, and nuclear fission [23, 24, 25, 26]. Generation of electricity is the process of producing electricity from these kinds of energy. Bulk generation system is connected to the distribution system via the transmission system carrying electricity to far distances [27,28]. Transmission domain is connected to customer domain by distribution domain which could also supply connection to storage systems and distributed energy resources (DERs) to meet electricity need for customers [17].

Security Requirements of Smart Grid

The National Institute of Standards and Technology (NIST) has defined three criteria required to maintain the security of information in the smart grid and keep it protected, specifically confidentiality, integrity, and availability [18]. According to [19], accountability is another important security criterion. The description of each criterion is given below.

Confidentiality

In general, confidentiality preserves authorized restrictions on information access and disclosure. In other words, the confidentiality criterion requires protecting both personal privacy and proprietary information from being accessed or disclosed by unauthorized entities, individuals, or processes. Once an unauthorized disclosure of information occurs, confidentiality is lost [18]. For instance, information such as control of a meter, metering usage, and billing information that is sent between a customer and various entities must be confidential and protected; otherwise, the customer's information could be manipulated, modified, or used for other malicious purposes.

Availability

Availability is defined as ensuring timely and reliable access to and use of information. It is considered the most important security criterion in the smart grid because the loss of availability means disruption of access to information in a smart grid [18]. For example, loss of availability can disturb the operation of the control system by blocking the information's flow through the network, and therefore denying the network's availability to control the system's operators.

Integrity

Integrity in smart grid means protecting against improper modification or destruction of the information. A loss of integrity is an unauthorized alteration, modification, or destruction of data in an undetected manner [18]. For example, power injection is a malicious attack launched by an adversary who intelligently modifies the measurements and relays them from the power injection meters and power flow to the state estimator [29, 30]. Both nonrepudiation and authenticity of information are required to maintain the integrity. Nonrepudiation means that individuals, entity or organization, are unable to perform a particular action and then deny it later; authenticity is the fact that data is originated from a legitimate source.

Accountability

Accountability means ensuring tractability of the system and that every action performed by a person, device, or even a public authority is recordable so that no one can deny his/her action. This recordable information can be presented as evidence in a court of law in order to determine the attacker. An example of an accountability problem would be the monthly electricity bills of customers. Generally, smart meters could determine the cost of electricity in real-time or day-to-day. However, if these meters are under attack this information is no longer reliable because they have been altered [31, 32]. As a result, the customer will have two different electric bills, one from the smart meter and the other from the utility.

National Cyber-security Strategy

In [24] [25], Cybersecurity risks involve three components namely; threat, vulnerability and consequences.

i. **Threat:** Threat can be technological like malware, geopolitical like adversary nation state, crime like an organized crime group or even environmental like extreme weather conditions.
ii. **Vulnerability**: Vulnerability is often described as a weakness of computer system which can be exploited. In the cyber ecosystem, vulnerability is more complex and can be technological, organizational, administrative and so on are the weaknesses that leave the ecosystem open to cyberthreats.
iii. **Consequence (impact):** Consequence can be assessed combining likelihood of the cyber incident with potential impact to the ecosystem or its components.

Figure 5: flowchart of National Security Threat

Figure 5 showed the flowchart of the risk and the growth stages of cyber attackers before it become a national risk. When a database or a system is threatened and succeeded it will make the system vulnerable to cyber attackers and when allowed again it creates a very big negative impact to the system which may be catastrophic to the nation.

In [26], [27] Ensuring cyber security is a complex task that relies on domain knowledge and requires cognitive abilities to determine possible threats from large amounts of network data. This study investigates how knowledge in network operations and information security influence the detection of intrusions in a simple network. A simplified Intrusion Detection System (IDS) was developed by this author [26], which allows user to examine how individuals with or without knowledge in cyber security detect malicious events and declare an attack based on a sequence of network events. The results indicate that more knowledge in cyber security facilitated the correct detection of malicious events and decreased the false classification of benign events as malicious. However, knowledge had less contribution when judging whether a sequence of events representing a cyber-attack. While knowledge of cyber security helps in the detection of malicious events, situated knowledge regarding a specific network at hand is needed to make accurate detection decisions. Responses from participants that have knowledge in cyber security indicated that they were able to distinguish between different types of cyber-attacks, whereas novice participants were not sensitive to the attack types. This showed that a cyber can be protected to a certain percentage based on the experience and training of workers regards the security threats and its likes.

CONCLUSION

This paper reviewed comprehensively the recent papers on cyber security threats, implications, challenges, recent solutions and prospective solutions. We reviewed and organized this paper based on three major areas or field of life which includes cyber security in academics, in industry and in governmental organizations. From this review, we observed that cyber-attacks and threats cannot be totally eradicated but can be curbed as it was caused by many factors which cannot be avoided such as insider, data transferred using different interfaces, downloading without screening and so on. This paper outlined all the likely threats to be experienced and proposed a prospective solution to the cyber attackers.

REFERENCES

[1] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, "A Survey on Machine Learning Techniques for Cyber Security in the Last Decade," *IEEE Access*, vol. 8, pp. 222310–222354, 2020, doi: 10.1109/ACCESS.2020.3041951.

[2] G. N. Reddy and G. J. U. Reddy, "A STUDY OF CYBER SECURITY CHALLENGES AND ITS EMERGNING TRENDS ON LATEST TECHNOLOGIES."

[3] N. Shafqat and A. Masood, "Comparative Analysis of Various National Cyber Security Strategies," 2016. [Online]. Available: https://sites.google.com/site/ijcsis/

[4] D. Craigen, N. Diakun-Thibault, and R. Purse, "Technology Innovation Management Review Defining Cybersecurity," 2014. [Online]. Available: www.timreview.ca

[5] M. D. Richardson, P. A. Lemoine, W. E. Stephens, and R. E. Waller, "Educational Planning," 2020.

[6] D. Craigen, N. Diakun-Thibault, and R. Purse, "Technology Innovation Management Review Defining Cybersecurity," 2014. [Online]. Available: www.timreview.ca.

[7] FTC, "SMALL BUSINESS."

[8] D. Schatz, R. Bashroush, and J. Wall, "Towards a More Representative Definition of Cyber Security," *The Journal of Digital Forensics, Security and Law*, 2017, doi: 10.15394/jdfsl.2017.1476.

[9] S. P.S, N. S, and S. M, "Overview of Cyber Security," *IJARCCE*, vol. 7, no. 11, pp. 125–128, Nov. 2018, doi: 10.17148/ijarcce.2018.71127.

[10] "Cyber Security Applications Freeware & Shareware".
[11] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K. K. R. Choo, "A systematic literature review of blockchain cyber security," *Digital Communications and Networks*, vol. 6, no. 2. Chongqing University of Posts and Telecommunications, pp. 147–156, May 01, 2020. doi: 10.1016/j.dcan.2019.01.005.
[12] M. Manulis, C. P. Bridges, R. Harrison, V. Sekar, and A. Davis, "Cyber security in New Space: Analysis of threats, key enabling technologies and challenges," *Int J Inf Secur*, vol. 20, no. 3, pp. 287–311, Jun. 2021, doi: 10.1007/s10207-020-00503-w.
[13] Z. I. Khisamova, I. R. Begishev, and E. L. Sidorenko, "Artificial intelligence and problems of ensuring cyber security," *International Journal of Cyber Criminology*, vol. 13, no. 2, pp. 564–577, Jul. 2019, doi: 10.5281/zenodo.3709267.
[14] L. A. Maglaras *et al.*, "Cyber security of critical infrastructures," *ICT Express*, vol. 4, no. 1. Korean Institute of Communication Sciences, pp. 42–45, Mar. 01, 2018. doi: 10.1016/j.icte.2018.02.001.
[15] D. Ghelani, Diptiben Ghelani., "Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review," *American Journal of Science, Engineering and Technology*, vol. 3, no. 6, pp. 12–19, 2022, doi: 10.22541/au.166385207.73483369/v1.
[16] Z. el Mrabet, N. Kaabouch, H. el Ghazi, and H. el Ghazi, "Cyber-security in smart grid: Survey and challenges," *Computers and Electrical Engineering*, vol. 67, pp. 469–482, Apr. 2018, doi: 10.1016/j.compeleceng.2018.01.015.
[17] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Computer Networks*, vol. 169, Mar. 2020, doi: 10.1016/j.comnet.2019.107094.
[18] W. O. Okafor, S. O. Edeagu, V. C. Chijindu, N. Iloanusi, and V. H. U. Eze, "A Comprehensive Review on Smart Grid Ecosystem," *IDOSR Journal of Applied Sciences*, vol. 8, no. 1, pp. 25–63, 2023.
[19] C. C. Ogbonna, V. H. U. Eze, E. S. Ikechuwu, O. Okafor, O. C. Anichebe, and O. U. Oparaku, "Comprehensive Review of Artificial Neural Network Techniques Used for Smart Meter-Embedded forecasting System.," *IDOSR Journal of Applied Sciences*, vol. 8, no. 1, pp. 13–24, 2023.
[20] V. H. U. Eze, M. C. Eze, C. C. Ogbonna, S. A. Ugwu, K. Emeka, and C. A. Onyeke, "Comprehensive Review of Recent Electric Vehicle Charging Stations," *Global Journal of Scientific and Research Publications*, vol. 1, no. 12, pp. 16–23, 2021.
[21] V. H. U. Eze, M. C. Eze, V. Chijindu, E. Chidinma E, U. A. Samuel, and O. C. Chibuzo, "Development of Improved Maximum Power Point Tracking Algorithm Based on Balancing Particle Swarm Optimization for Renewable Energy Generation," *IDOSR Journal of Applied Sciences*, vol. 7, no. 1, pp. 12–28, 2022.
[22] V. H. U. Eze, O. N. Iloanusi, M. C. Eze, and C. C. Osuagwu, "Maximum power point tracking technique based on optimized adaptive differential conductance," *Cogent Eng*, vol. 4, no. 1, pp. 1–13, 2017, doi: 10.1080/23311916.2017.1339336.
[23] V. H. U. Eze, U. O. Oparaku, A. S. Ugwu, and C. C. Ogbonna, "A Comprehensive Review on Recent Maximum Power Point Tracking of a Solar Photovoltaic Systems using Intelligent, Non-Intelligent and Hybrid based Techniques," *Int J Innov Sci Res Technol*, vol. 6, no. 5, pp. 456–474, 2021.
[24] A. N. Mohammad *et al.*, "A NEW TAXONOMY OF INSIDER THREATS; AN INITIAL STEP IN UNDERSTANDING AUTHORIZED

ATTACK," *International Journal of Information Systems and Management*, vol. 1, no. 1, p. 1, 2018, doi: 10.1504/ijisam.2018.10014439.

[25] "DRAFT NATIONAL CYBERSECURITY STRATEGY," 2021.

[26] N. Ben-Asher and C. Gonzalez, "Effects of cyber security knowledge on attack detection," *Comput Human Behav*, vol. 48, pp. 51–61, 2015, doi: 10.1016/j.chb.2015.01.039.

[27] C. T. Do *et al.*, "Game theory for cyber security and privacy," *ACM Computing Surveys*, vol. 50, no. 2. Association for Computing Machinery, pp. 30–37, May 01, 2017. doi: 10.1145/3057268.

[28] W M Masisani and I Adabara (2022).Monitoring with Communication Technologies of the Smart Grid. *IDOSR Journal of Applied Sciences* 7 (1), 102-112.

[29] W M Masisani and I Adabara (2022).Implementation of Smart Grid Decision Support Systems. *IDOSR Journal of Scientific Research* 7 (1), 50-57.

[30] WM Masisani, I Adabara (2022). Overview of Smart Grid: A Review. *IDOSR Journal of Computer and Applied Sciences* 7 (1), 33-44.

[31] M Kalulu (2022).The Smart Grid and Its Security Challenges. *INOSR Applied Sciences* 9 (1), 9-12.

[32] M Kalulu and I Adabara (2022). Developing of A Smart Fraud Detection System in Advanced Metering Infrastructure Using Deep Learning. *INOSR Applied Sciences* 9 (1), 1-8.