IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# SURVEY ON CYBER SECURITY AND CLASSIFICATION OF ATTACKS IN NETWORKS

[1]Sumiyah khaja, [2]Syed Faizuddin Ahmed Quadri, [3]Aleem MOHAMMED.

Coding Instructor, Whitehat jr, Online platform

Technical Lead (SME), IT DEPARTEMENT/ Vertafore, HYDERABAD

Research Associate ACS, Sydney, Australia.

## ABSTRACT

Cyber security is crucial for the safety of those who use the internet regularly from a variety of electronic devices. In many parts of the world, individuals have been experiencing connectivity issues after a number of recent events. Cyber security serves a crucial role in protecting especially delicate information, such as that related to biotechnology and military assets, which are frequent targets of hackers. Internet abuse is a growing problem in many areas of society, including the workplace, educational institutions, and government agencies. Students in universities and workers in a variety of businesses can benefit greatly from using the Internet. People now have the option to get information from online sources, which is very convenient. There must be safeguards in place to prevent theft or illegal access while they are online. Various facets of cyber and network security in the present day have been discussed. In addition, we have worked to include discussion of dangers faced by internal networks.

Keywords—Cyber security; internet; intranet; network security; cybercrime and security alludes

## 1. INTRODUCTION

### 1.1 Introduction

Cybersecurity threats have rapidly developed during the past few years. Attempts by an individual or group to obtain unauthorised access to a computer system in order to steal sensitive information are known as threats in the field of cyber security. Sectors such as healthcare, retail, and government will feel the effects the soonest. The sheer volume of financial and medical data generated by these sectors every day makes them particularly vulnerable. Various factors provide risks to any given system. The rise of remote work and people's reliance on digital services and devices has led to a corresponding rise in the sophistication of cyber threats. Knowing the risks we face and taking measures to lessen our exposure to cyberattacks is now more important than ever.

Across the past decade, there has been a dramatic increase in the number of people with access to ICT all over the globe. The number of people who have access to broadband internet has increased by the billions in recent years. Internet connection has many positive effects, but there are also many obstacles to utilising them. Cybersecurity is one of the main problems that needs to be solved. Achieving the goal of a secure internet is impossible without first ensuring that the CIA objectives (confidential integrity, availability) are met in any given computer network environment. Researchers have discovered that DDoS attacks based on the Internet of Things have been labelled "death of the internet" in recent years. If you want to limit your exposure to the internet, you can do so with relative ease now. They'll begin harassing the service's providers [Newman, S. (2017)].

In this paper, we explore the various forms of internet security threats now in existence. In this article, we'll go over the most common types of assaults that can compromise a system's safety. We can also discuss measures to protect our network from these assaults. As we all know, the internet also provides IaaS, or Internet as a Service, making internet security one of the greatest challenges of the computer age (IAAS). Computer

networks are integral to our daily lives, and as such, their security is just as crucial as our ability to protect ourselves from various web attacks, which is becoming increasingly more difficult for both internet users and internet service providers. The CIA trio is being implemented to improve network and internet security. This approach was created to prevent the compromise of network security and the abuse of personal information. If proper network security measures aren't put in place, many potential dangers will remain.

The Internet is a global system of interconnected computer networks and other devices that communicate using both directed and undirected media (such as phone lines, satellites, and connections). Internet connectivity is available across the board, from desktop computers to mobile phones to power grids to televisions and other electrical devices. People all around the world are increasingly turning to the internet as a reliable resource for a wide range of activities. The worldwide use of the internet, both in developed and emerging nations, is expanding on a worldwide graph. Likewise, as time goes on, people's demands for internet connectivity and instantaneous access to information rise. Internet was used in the armed forces, in security duty, and in the administration of exams at specialised universities. In the 21st century, it has flourished in every facet of modern life, from the world of information and business to that of society and entertainment and shopping. Both the benefits and the drawbacks are numerous. Negative aspects of the internet include the ease with which any person, wherever in the world, can commit crimes including fraud, cyber terrorism, identity theft, and other forms of cybercrime. Because of this, users of the internet place a premium on cyber security, and as a result, they expect to feel safe while surfing the web [Weber, R. H., 2016].

**1.2 Types of cyber security**

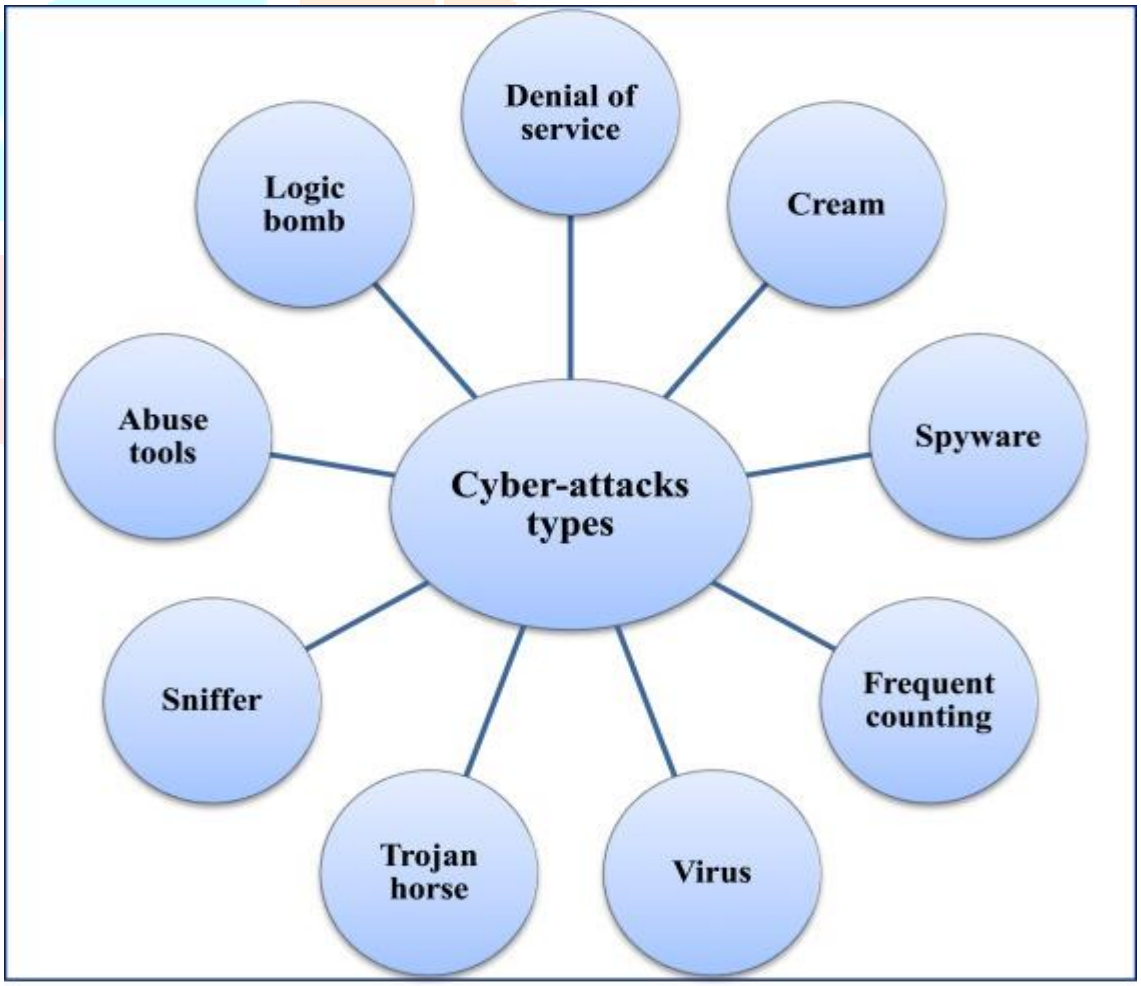


Fig. 1. Main cyber-attacks types.

Common forms of cyberattacks include denial of service, logical bombs, abuse tools, sniffers, Trojan horses, viruses, worms, spamming, and botnets. The most common forms of cyberattacks are shown in Fig 1. Denial-of-service attacks are used to prevent authorised users and administrators from accessing the system. As a matter of fact, the attacker will immediately begin bombarding the compromised machines with messages in an

effort to impede the normal flow of data. So, no gadget can access the internet or share information with others (Topping et al., 2021). Distributed denial of service assaults are another option, in which several infected systems work together to knock down the target. Worms are typically used to accomplish this goal by propagating themselves across an online network. The general public has easy access to abuse tools that can probe for and exploit vulnerabilities in a network's defences. Another sort of malicious software is the "logic bomb," which is programmed to carry out a damaging action upon the occurrence of a certain condition (Li et al., 2021). By inspecting each data packet for specified information like passwords, Sniffer is another tool that may be used to eavesdrop on routed information (Patel et al., 2021). Trojan horses are malicious programmes that trick users into installing and running them because of their benign appearance (Al Shaer et al., 2020).

## 2. REVIEW OF LITERATURE

### 2.1 Emerging trends and recent developments

Internet use has increased dramatically and become ubiquitous over the past two decades, making it an integral part of people's daily lives everywhere. As a result of advancements in technology and decreases in price, there are now more than 3 billion people connected to the Internet around the world (Tan et al., 2021). In creating a wide global network, the Internet has contributed annually to the world economy in the form of billions of dollars (Judge et al., 2021).

The majority of today's economic, commercial, cultural, social, and governmental activities and exchanges take place online, facilitated by individuals, businesses, NGOs, and government and governmental agencies (Aghajani and Ghadimi, 2018). Most important and sensitive data travels to or is created in cyberspace, and crucial infrastructures and systems may be located there or managed, exploited, or even created there as well (Akhavan-Hejazi and Mohsenian-Rad, 2018).

The majority of residents' time and energy is spent interacting in this space, and the majority of their media consumption and financial transactions also take place here (Priyadarshini et al., 2021). There has been a dramatic rise in the proportion of national income attributable to cybersector activities, and cybersector indicators now play a substantial role in measuring national growth. Most of the nation's and its people's money and faith flow into this region, and many of their material successes and spiritual breakthroughs may be traced back to or are profoundly influenced by what happens here (Amir and Givargis, 2020). That is to say, many people's lives depend on this area, and the effects of any instability, insecurity, or difficulties in this area will ripple outside (Li et al., 2020). While this is true, internet has presented new security challenges for nations.

Cyberspace's low entry barrier, anonymity, lack of clarity regarding the potentially dangerous geographical region, dramatic impact, and lack of public transparency make it a battleground for powerful and weak actors alike. Governments, organised and terrorist groups, and even individuals all fit into this category (Niraja and Srinivasa Rao, 2021).

This is precisely what has challenged and rendered ineffectual traditional national security in this area, as cyber dangers are more opaque in nature and whose participants include governments and nations that can be identified by their location (Sarker, 2021). Potential repercussions of cyber attacks have been a topic of discussion for analysts for over a decade (Shin et al., 2021).

Severe and sometimes widespread physical or economic damage can result from the function of a virus that, for example, attacks the financial documents of an economic system or disrupts a country's stock market, or that sends an incorrect message that causes the country's power plant to stop and fail, or that disrupts the air traffic control system and leads to air accidents. Viruses that compromise a country's financial records or cause stock market instability (Snehi and Bhandari, 2021).

Therefore, it will be very difficult for professionals to address the complex and many dimensions and features of the issue and provide legal counsel and analysis until governments agree on a precise definition of a cyber-attack that is recognised and acknowledged by the international community. This will be a very difficult challenge for professionals to address (Cao et al., 2021).

This raises the issues, what constitutes a cyber-attack, what features it must have, and whether or not any act of violence committed in cyberspace can be categorised as a "attack" in the conventional sense. (Gupta Bhol, et al., 2022). It is crucial to have a clear definition of what a cyber-attack is in order for legal frameworks to continue addressing and recognising the consequences of this type of attack (Furnell et al., 2020).

There is no doubt that the lack of a clear and comprehensive definition not only obscures the main legal road, but also leads to variations in interpretation and practise, and, eventually, results in the actualization of legal conclusions that are sometimes in direct opposition to one another (Alhayani et al., 2021). Because of this, it is crucial to do a comprehensive inquiry and settle on a mutually agreeable description, at the very least for the purpose of introducing the problem and providing some initial context for explaining, adapting, and analysing it.

## 3. UNITING CYBER SECURITY AND MACHINE LEARNING

### 3.1. Machine learning in cyber security

The interconnected systems that make up cyberspace can be attacked in many different ways. Some of these include replay, man-in-the-middle (MiTM), impersonation, credential leakage, password guessing, session key leakage, unauthorised data update, malware injection, flooding, denial of service (DoS), and distributed denial of service (DDoS), among others. As a result, we need a security protocol that can identify intrusion attempts and take appropriate action to prevent further damage. Machine learning models, also known as ML algorithms, have the ability to make use of the pre-processed dataset in order to acquire knowledge regarding various categories of cyber risks in either an offline or an online environment. In online, real-time mode, ML algorithms can spot the telltale signs of an incursion (a cyber assault, for example). Fig. 2 depicts a potential "machine learning in cyber security" scenario. Here, we have an Internet-connected system (e.g., laptops, desktops, smartphones, IoT devices) that may be utilised for a variety of online functions, such as making monetary transactions, gaining access to medical records, confirming identity, etc. Hackers are constantly on the lookout for weak points in such systems, and if they find one, they immediately start an attack. Detecting and preventing cyber attacks can be accomplished with the help of a variety of machine learning strategies, including supervised learning, unsupervised learning, reinforcement learning, and deep learning, to name a few. These strategies can be applied in a variety of settings. The communication context of a specific system as well as the resources it has access to will determine which of the four learning methods—supervised learning, unsupervised learning, reinforcement learning, and deep learning—is the most effective for that system. Given their large computational and storage capacities, cloud servers are well-suited for the training and testing of cyber attack models.

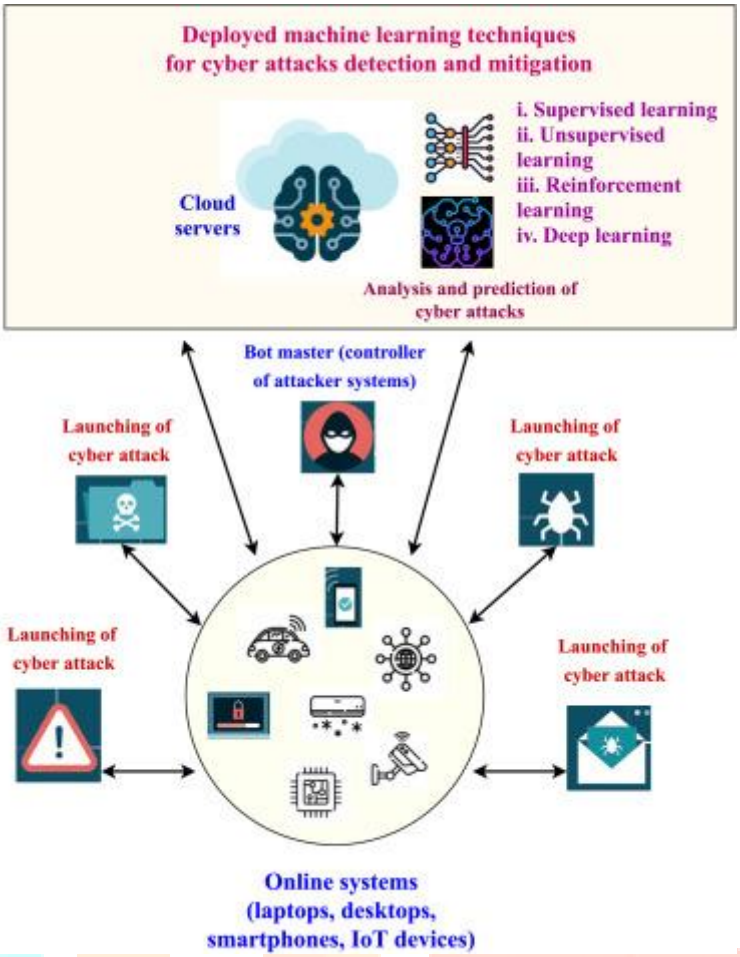


Fig. 2. Scenario of machine learning in cyber security.

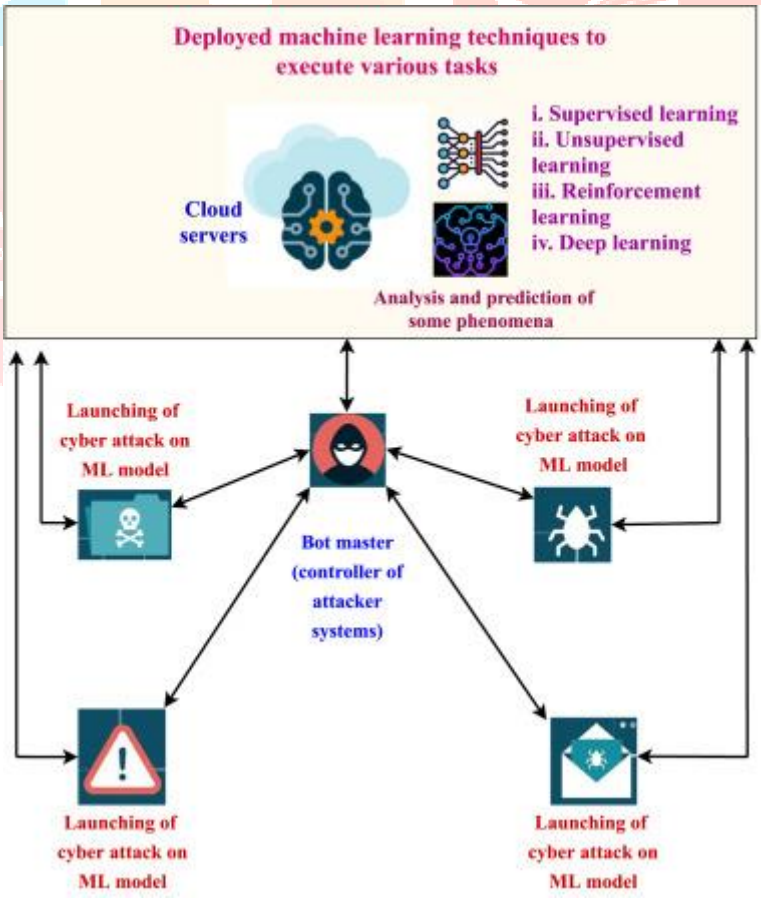


Fig. 3. Scenario of cyber security in machine learning.

### 3.2. **Cyber security in machine learning**

Figure 3 illustrates the "cyber security in machine learning" situation, which can also be referred to as "machine learning (ML) security." ML models can be utilised in a wide variety of contexts, including the investigation and forecasting of events. Attacks such as dataset poisoning, model poisoning, privacy breach, membership inference, runtime disruption, and others can all have an effect on the performance of machine learning models [Sun.Y. et. al., 2021]. ML models vulnerable to these assaults may make inaccurate predictions about the phenomena they are trying to anticipate. The adversarial examples (updated values) inserted by the attacker in the dataset during the "dataset poisoning attack" cause the ML model to make inaccurate predictions. In addition, during a "model poisoning attack," the attacker focuses on tampering with the models' inner workings and manipulating the parameters in an effort to corrupt them. When an attacker conducts a "privacy breach attack," he or she aims to disclose private information and retrieve valuable model data. The invasion of privacy is due in part to membership inference attacks. In addition, an attacker can disrupt the execution of an ML model, known as a "runtime disruption attack," and so corrupt the workflow, thereby affecting the accuracy of the prediction results. Cyber security procedures (such as encryption methods, signature creation and verification methods, and hashing mechanisms) are necessary to prevent such assaults. By implementing these safeguards, we can rest assured that our ML models and the data they use will produce reliable results and predictions.

## 4. CYBER-SECURITY OF SMART GRIDS

Conventional power grids are no longer practical for transmitting and distributing electricity because of their many flaws, such as frequent blackouts, difficulties with energy storage, high asset costs, and substantial carbon emissions. In summary, multiple examples show that the current electricity grid has much room for improvement in terms of its ability to meet consumer demand. In February of 2020, for instance, the storm Ciara knocked off power to about 130,000 residences in France. A similar number of Bavarian houses lost power that month due to the storm Sabine. At least 70 million people in Turkey were without power in March 2016. These are just a few of the glaring reasons why the old electrical grid isn't a good choice anymore [M. S. Al-kahtani, 2019].

Microgrid was developed as a solution to conventional grid weaknesses. Microsources can come from a wide variety of technologies, including but not limited to microturbines, fuel cells, solar panels, wind turbines, and capacitors. A microgrid is comprised of all of these different types of microsources. In addition to functioning autonomously, it can also be linked to a larger grid. An increase in efficiency, a decrease in pollutants, and cheaper and cleaner power are just a few of the advantages provided by microgrids. Some difficulties are overcome by this technology, such as the resynchronization with the main grid, which might cause issues in the network because of the inconsistency of the network. Smart grid was offered as a comprehensive answer to these problems and constraints [Y. Yoldaş, 2017]. The modern electrical grid contains a wide variety of energy-saving technologies as well as technologies that generate energy. Technologies such as smart meters, smart appliances, renewable energy sources, and energy-efficient resources are all good examples. Power grid efficiency, scalability, reliability, and interoperability are all impacted when information technology is used to distribute energy to end-users in the form of a two-way flow of communications. These changes are brought about by the adoption of smart grids.

By integrating a number of different technologies, the "smart grid" is meant to facilitate the delivery of energy that is secure, efficient, and environmentally friendly. It's a cheap, efficient, and reliable way to distribute power that won't break the bank. In addition to providing customers with clean, economical, and efficient energy, it also helps reduce greenhouse gas emissions [A. Gopstein, 2021]. Nonetheless, cyberattacks on this infrastructure pose a threat to the reliability, privacy, and transparency that are essential components of a secure smart grid. In March 2018, for instance, hackers struck the United States electrical infrastructure, aiming for multiple nuclear power plants and water facilities. When it comes to cyber attacks, Ukraine was once again the target in December of 2015. At least 230,000 people lost power for up to six hours as attackers shut down 30 substations. The US Department of Energy (DOE) and the National Electric Sector Cybersecurity Organization (NESCOR) have teamed up to strengthen the safety of the country's power grid. They worked together with the Federal Energy Regulatory Commission and the Cybersecurity for Energy Delivery Systems (CEDS) to accomplish this (FERC). In order to ensure the safety of the electrical grid, they enlisted the help of specialists, developers, and end users. They worked together to improve smart and mitigation techniques for security concerns. Their research showed that protecting against cyber-security threats in the context of this cutting-edge technology calls for a more comprehensive approach. Although smart grids have made significant strides, further work is needed to ensure that sophisticated

cyberattacks are thwarted before any damage is done [G. Bedi, 2018]. Table 1 displays the results of many surveys conducted over the past decade that provide an overview of smart grid cyber-security.

Table 1. Existing Surveys Related to the Cyber-security of Smart Grids.

| Related Work | Topic | Cyber-Attacks Mentioned | Concepts Covered | Concepts Not Covered |
|---|---|---|---|---|
| Gunduz et al. | Survey on cyber-security solutions of IOT-based smart grids. | There were multiple types of cyberattacks performed targeting the CIA tirade and the five OSI communication layers. | • Cyber-attack types and the general importance of countermeasures.<br>• An examination of a variety of cyberattacks, including the requirements for their protection, as well as the directions for the future. | Countermeasure methods and detection techniques. |
| Peng et al. | Survey on security communications in smart grids. | Analysis of traffic, social engineering, scanning an IP address, scanning a port, scanning for vulnerabilities, worms, denial of service attacks, forward data interceptions, replays, violations of privacy, and backdoors | • Cyber-physical security of smart grids as well as prospective scenarios of assaults based on information technology<br>• Methods of prevention and detection, as well as the issues posed by threats posed by smart grids. | Accountability as a security requirement in smart grids. |
| He et al. | Survey on cyber-physical attacks and solutions in smart grids. | Attacks on the generation system, attacks on the transmission system, attacks on the distribution system and on the customer side, and attacks on the energy market | • Critical cyber-physical attacks and the defence mechanisms employed against them.<br>• Performing an investigation of the effects that cyber-physical attacks have had on smart grids. | Detection techniques for cyber-physical attacks in smart grids. |
| Gupta et al. | Survey of cyber-security in smart grids. | DoS/ DDoS attacks | • The smart grid and its components.<br>• Methods and procedures for existing forms of electronic communication.<br>• The effects of DoS and DDoS attacks on smart grids. | Existing cyber-attacks that targets smart grids, their countermeasures, and |

| | | | | |
|---|---|---|---|---|
| | | | | detection techniques. |
| Elmrabet et al. | Comprehensive review of cyber-attacks and their solutions in smart grids. | Methods such as traffic analysis, social engineering, IP scanning, port scanning, vulnerability scanning, worms, Trojan horses, denial of service, forged data injection, forged integrity, backdoor, MITM, jamming, and popping the HMI are all examples of malicious network activity. masquerade. | • Smart grid cyberattacks and their consequences.<br>• Smart grids' cyber security concerns can be addressed in a number of ways. | Detection techniques and countermeasure approaches. |
| Komninos et al. | Survey on cyber-security in smart homes and smart grids. | Cyberattacks of various types targeting data privacy, data availability, data authorisation, and data validity. | • The most typical threats to smart homes and smart grids.<br>• Cases of cyberattack and the steps taken to stop them.<br>• Strategies to counter or prevent cyberattacks. | Smart grid cyber-attacks, countermeasures, and detection techniques. |
| Sakhnini et al. | Survey on cyber-security aspects of IOT aided smart grids. | MITM, jamming, FDI, spoofing, DoS, malware, replay attacks. | • Journal content evaluation using bibliographic data.<br>• Threats to the safety of smart grids from a variety of cyber sources.<br>• Cybersecurity in the smart grid is an area that will continue to develop in the future. | Countermeasure techniques. |
| Kumar et al. | Survey of cyber-security and privacy of smart grid metering networks. | There have been numerous attacks against the energy sector, its renewable resources, and its metering infrastructure. | • Cyberattacks on conventional energy systems are a real threat.<br>• Smart grid metering networks need to address concerns about privacy, including the need for restrictions on unauthorised access.<br>• Perspectives and challenges for future research. | Countermeasures and detection methods. |

## CONCLUSION

Internet access is now considered essential in almost every country. The list of pros and cons is long. The most important benefit is that criminals may use the internet with ease due to unrestricted access and resources. They are pleading for a safe and protected internet platform. Internet users are able to use the safe and secured source and path thanks to cyber security. Intranets are private networks used primarily by the government and the armed forces. Some problems do arise with this network, but overall it's safer than the local internet. The entire system is then under the direction of intelligent agents and protected via onion routing from any potential attacks. The anonymity, exposure, and asymmetry inherent to the online world have led to a diffused distribution of power. Since governments appear to have already allocated roles in the game of power among themselves, it follows that private enterprises, organised terrorist and criminal groups, and people must be involved. This phenomena will not compromise government efforts to ensure national security, of course. The magnitude of its impact can be measured in various ways. To begin, let's talk about safety. Today, a danger to national security is not just the possibility of a decline in people' quality of life, which means that military issues and internal and external boundaries are no longer sufficient definitions. The second is that there is no longer a physical distance between people who can potentially pose a cyber threat. There used to be a clear physical place associated with military dangers. Therefore, it was easy to deal with, at least in terms of spotting. There can be no successful rollout of smart grid infrastructure without first guaranteeing the safety of the associated network infrastructure. However, previous research has revealed only a limited function in assessing cyber-security solutions for smart grid networks. In light of the limitations of previous surveys, this article presents a detailed overview of possible attacks against smart grids and an evaluation of various security solutions. Using the Open Systems Interconnection (OSI) communication layers as a basis, this research proposes a classification scheme for cyberattacks and a ranking scheme that accounts for the damage done to privacy, accessibility, and responsibility during an attack.

## REFERENCES


1. Newman, S. (2017). Service providers: the gatekeepers of Internet security. Network Security, 2017, 5-7.
2. Weber, R. H., & Studer, E. (2016). Cybersecurity in the Internet of Things: Legal aspects. Computer Law \& Security Review, 32, 715- 728.
3. Topping C., *et al.* Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks Comput. Secur., 108 (2021), Article 102324
4. Li J., Sun C., Su Q. Analysis of cascading failures of power cyber–physical systems considering false data injection attacks Glob. Energy Interconnect., 4 (2) (2021), pp. 204-213
5. Patel D.C., *et al.* Paradoxical motion on sniff test predicts greater improvement following diaphragm plication Ann. Thorac. Surg., 111 (6) (2021), pp. 1820-
6. Al Shaer D., *et al.* Hydroxamate siderophores: Natural occurrence, chemical synthesis, iron binding affinity and use as Trojan horses against pathogens Eur. J. Med. Chem., 208 (2020
7. Tan S., *et al.* Attack detection design for dc microgrid using eigenvalue assignment approach Energy Rep., 7 (2021), pp. 469-476
8. Judge M.A., *et al.* Price-based demand response for household load management with interval uncertainty Energy Rep. (2021)
9. Aghajani G., Ghadimi N. Multi-objective energy management in a micro-grid Energy Rep., 4 (2018), pp. 218-225
10. Aghajani G., Ghadimi N. Multi-objective energy management in a micro-grid Energy Rep., 4 (2018), pp. 218-
11. Akhavan-Hejazi H., Mohsenian-Rad H. Power systems big data analytics: An assessment of paradigm shift barriers and prospects Energy Rep., 4 (2018), pp. 91-
12. Priyadarshini I., *et al.* Identifying cyber insecurities in trustworthy space and energy sector for smart grids Comput. Electr. Eng., 93 (2021), Article 107204
13. Amir M., Givargis T. Pareto optimal design space exploration of cyber–physical systems Internet Things, 12 (2020), Article 100308
14. Li N., *et al.* Early validation of cyber–physical space systems via multi-concerns integration J. Syst. Softw., 170 (2020), Article 110742

15. Niraja K.S., Srinivasa Rao S. A hybrid algorithm design for near real time detection cyber attacks from compromised devices to enhance IoT security
16. Mater. Today: Proc. (2021)
17. Sarker I.H. Cyberlearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks Internet Things, 14 (2021), Article 100393
18. Shin J., *et al.* Application of STPA-SafeSec for a cyber-attack impact analysis of NPPs with a condensate water system test-bedNucl. Eng. Technol. (2021)
19. Ahmed Jamal A., *et al.* A review on security analysis of cyber physical systems using machine learning Mater. Today: Proc. (2021)
20. Cao J., *et al.* Hybrid-triggered-based security controller design for networked control system under multiple cyber attacks Inform. Sci., 548 (2021), pp. 69-84
21. Gupta Bhol S., Mohanty J.R., Kumar Pattnaik P. Taxonomy of cyber security metrics to measure strength of cyber security Mater. Today: Proc. (2021)
22. Furnell S., *et al.* Understanding the full cost of cyber security breaches Comput. Fraud Secur., 2020 (12) (2020), pp. 6-12
23. Alhayani B., *et al.* Best ways computation intelligent of face cyber attacks Mater. Today: Proc. (2021)
24. Sun Y., Bashir A.K., Tariq U., Xiao F. Effective malware detection scheme based on classified behavior graph in IIoT Ad Hoc Netw., 120 (2021), Article 102558
25. M. Z. Gunduz, and R. Das, "Cyber-security on Smart Grid: Threats and Potential Solutions," Computer networks, vol. 169, pp.107094, 2020.
26. C. Peng, H. Sun, M. Yang and Y. Wang, "A Survey on Security Communication and Control for Smart Grids under Malicious Cyber Attacks," Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 8, pp. 1554-1569, 2019.
27. H. He, and J. Yan, "Cyber-physical Attacks and Defenses in the Smart Grid: a survey," IET Cyber-Physical Systems: Theory & Applications, vol.1, no.1, pp.13-27, 2016.
28. B. B. Gupta, and T. Akhtar, "A Survey on Smart Power Grid: Frameworks, Tools, Security Issues, and Solutions," Annals of Telecommunications, vol. 72, no. 9, pp.517-549, 2017.
29. N. Komninos, E. Philippou and A. Pitsillides, "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures," Communications Surveys and Tutorials, vol. 16, no. 4, pp. 1933-1954, 2014.
30. X. Li, X. Liang, R. Lu, X. Shen, X. Lin and H. Zhu, "Securing Smart Grid: Cyber-attacks, Countermeasures, and Challenges," Communications Magazine, vol. 50, no. 8, pp. 38-45, 2012.
31. J. Sakhnini, H. Karimipour, A. Dehghantanha, R. M. Parizi, and G. Srivastava, "Security Aspects of Internet of Things Aided Smart Grids: A Bibliometric Survey," Internet of things, p.100111, 2019.
32. P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong and A. Martin, "Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues," Communications Surveys and Tutorials, vol. 21, no. 3, pp. 2886-2927, 2019.
33. M. S. Al-kahtani, and L. Karim, "A Survey on Attacks and Defense Mechanisms in Smart Grids," International Journal of Computer Engineering and Information Technology, vol. 11, no. 5, pp.94-100, 2019.
34. Y. Yoldaş,A. Önen, S. M. Muyeen, A. V. Vasilakos, A.V. and İ. Alan, "Enhancing Smart Grid with Microgrids: Challenges and Opportunities," Renewable and Sustainable Energy Reviews, no. 72, pp.205-214, 2017.
35. Gopstein, C. Nguyen, C. O'Fallon, N. Hastings, and D. Wollman, "NIST Framework and Roadmap for Smart Grid Interoperability Standards," National Institute of Standards and Technology Special Publication (NIST SP), release 4.0, 2021.
36. G. Bedi, G. K. Venayagamoorthy, R. Singh, R. R. Brooks and K. Wang, "Review of Internet of Things (IoT) in Electric Power and Energy Systems," Internet of Things Journal, vol. 5, no. 2, pp. 847-870, 2018