International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 6 Volume No.7 November - December – 2023
DOI:10.46647/ijetms.2023.v07i06.029 ISSN: 2581-4621

A Review of Cyber Security and its Approaches with Recent Progress and Challenges

Amisha Sharma[1], Dhairya Verma[2], Neha Sharma[3], Neeru Jindal[4]
[1] UG - Computer Science and Engineering, Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India
[2] UG - Computer Science and Engineering, Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India
[3] Assistant Professor, Computer Science and Engineering, Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India
[4] Associate Professor, Electronics and Communication Engineering, Thapar Institute of Engineering and Technology, Patiala, Punjab, India.
***Corresponding Author Orcid ID**: https://orcid.org/0009-0001-4848-6594*

ABSTRACT

Cyber security is a practice to protect internet-based systems including software, hardware, and data such as networks, computers, mobile devices, electronics systems, and data from illegal attacks or cyber threats. One of the most focused and sensitive areas in today's world is cybersecurity. The main objective of this study is to emphasize the several cyber security attacks and threats under one umbrella. The goal of this work is to examine the literature review on cyber security approaches, datasets, threats, attacks, research trends, challenges, performance metrics, and software used to promote further research in this field. Based on a comprehensive review SWOT analysis is also performed on cyber security. The presented review paper aid researchers in both academia and industry in making advancements in their work in relevant application fields.

Keywords— Cyber security constraints, Computer privacy, Information security, Intrusion detection, Artificial intelligence, IoT

1. Introduction

Numerous factors have caused an increase in interest in expanding the potential use of cyber security: (i) The rise of cyber dangers, (ii) Growing dependency on technology (iii) Regulation and compliance requirements (iv) Education and training initiatives: (v) Employment opportunities. The "cyber" problem has evolved over 50 years. Long before the public and many senior executives realized its value in the mid-1990s, it existed. The conclusions of those earlier discussions thus influenced the official responses to the emergence of the cyber crisis in the late 1990s [1]. The practices employed to protect a user's online environment are referred to as cyber security. The user, devices, networks, apps, all software, and other elements are all included in this ecosystem. The objective is to minimize the risk of cyberattacks. However, information security states the preservation of data with importance on its availability, truthfulness, and privacy aspects [3, 4]. The fact that information security is a continual process rather than a one-time occurrence is the most crucial fact about it. There are various methods for reducing internet security risks and stopping online assaults. Cyberattacks are becoming more prevalent as internet activities and mobile applications grow in popularity [2]. Recent trends in cyber security are presented in Fig. 1. and Fig. 2 represents the AI-based cyber security work as per Google Scholar statistics.

The following is the review paper's main contributions:

1. This paper provides a relevant discussion of cybersecurity, and cyber trespass, as well as its applications and necessity.

2. In addition, a review of various cybersecurity approaches is provided, along with a comprehensive discussion of various cybersecurity datasets, threats, and attacks.
3. The review paper substantially describes present research and issues in cyber security. As well as potential future paths in the field of cybersecurity that could aid researchers in both academia and industry in making advancements in their work in relevant application fields.
4. From a literature review, a SWOT analysis is performed on cyber security broadly considering the various aspects.

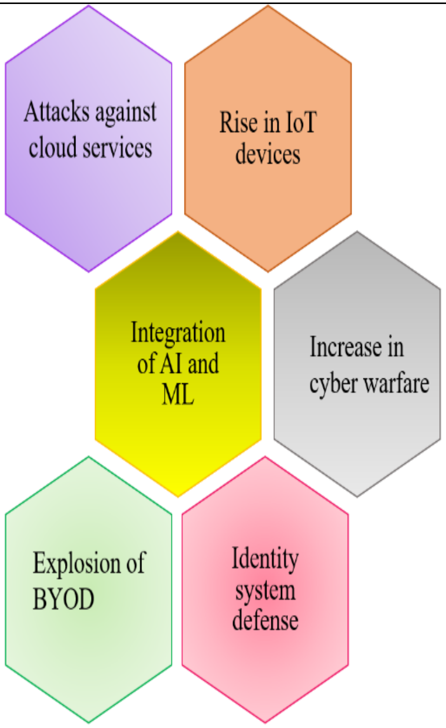

Fig. 1 Some major trends in cyber security.

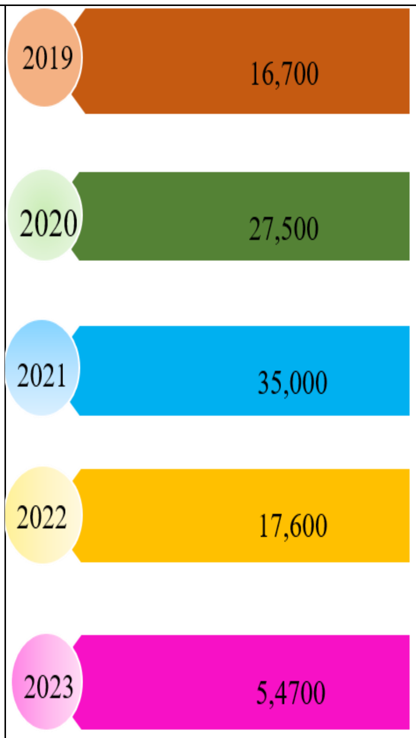

Fig. 2 AI-based cyber security work as per Google Scholar statistics.

2. Related work

The explicit and contented literature review is presented in this paper with some of the recently released works. Cybersecurity's future will be difficult as compared to the present in that it will become hard to define and possibly endless, as digital skills converge with other technologies. There are humans in almost every element of laws, society, the family, and the outside world. The foundation of this work [3] was the idea that the "cyber" and "security" professions as a concept of "cybersecurity" would coexist in a rapidly changing context in the second period of 2010. Even though the way it was used varies greatly depending on the situation, that action was more likely to quicken than slow. So, that cannot be the part of research task instead it served as the core of the investigation. Cybersecurity will be probably regarded as a "master challenge" in the age of the internet eventually. Considering this, it would appear first on any list of difficulties that civilizations encounter and technology companies must deal with the work [5,6]. Organizations had difficulties in 2022 concerning cybersecurity [8]. Ransomware became a common hazard for most enterprises as attackers targeted numerous government entities. Cybersecurity solutions now frequently use Machine Learning (ML), a subset of AI, to quickly analyze massive data sets in search of normal and abnormal data as well as to quickly and effectively categorize suspicious data [7, 9].

The robotics sector is adopting ROS 2, requiring security for robots and ROS computational graphs. This paper provides SROS2, library sets, and developer tools for integrating safety in ROS 2 graphs, adhering to DevSecOps model, and demonstrating graph protection using TurtleBot3 [10]. The author discusses that cyber-physical systems security modeling is not effectively applied due to weak design aspects, lack of overlap between security and safety, and the potential for mishaps [11].

This work investigates the Bluetooth system in an automobile display system, identifying threats to privacy restrictions, grading attacks, and suggesting defenses. The study uses the Android Open-Source Project to discover vulnerabilities in a real vehicle [12].

The author of this study used DNNs (Deep neural networks) to foresee Network Intrusion Detection System attacks (N-IDS). The network has been trained and benchmarked using the KDDCup-'99 dataset. Upon comparing the findings, it was seen that a deep neural network (DNN) consisting of three layers outperformed all other standard machine learning (ML) techniques [13].

The author introduces active fuzzing, an automated method for detecting packet-level CPS network intrusions. It uses online active learning to update models, and the technique is tested on a water purification facility to determine its effectiveness [14].

To provide flexible control of network traffic, software-defined networking (SDN), a unique network paradigm, splits the control plane and data plane into independent pieces of network equipment. It is strong programmability and global perspective open up a lot of new possibilities. DDOS detection in the context of SDN (Software-Defined Networking) was a significant and difficult research field focus to provide flexible control of network traffic. As a result, the author presented FORT, a straightforward DDoS detection system that distributed the rule-based detection algorithm at edge switches and determines when to activate it by routinely gathering the port condition data. Representative tests showed that FORT can significantly decrease controller load while delivering accurate detection. The following were the results of the survey. Additionally, by including an alarm mechanism, this design can, under normal circumstances, lower the load on the southbound channel by more than 60% [15].

3. Approach

Nations now face new security challenges as a result of the internet. Aside from administrations, extremist groups, and even people, cyberspace is home to both strong and weak actors as well as due to its low entrance barrier, anonymity, significant influence, and lack of public transparency, cyberspace poses hazards such as cyberwarfare, cybercrime, cyberterrorism, and cyber espionage. Fig. 3 depicts the anatomy of a cyber-attack and its strategy. It is clear that the hacker first starts with the target identification which means to whom device or organization where it wants to attack to gain access. Then, data collection by researching and gaining information in this context and finally performing the cyber-attack. All this can be stopped at any stage if the companies and particular user is aware of the cyber-attack and know how to protect from it.

Cyberattacks can cause severe physical or financial harm, such as virus attacks, stock market crashes, power plant failures, and air traffic control system disruptions. Organizations use cybersecurity to avoid unauthorized access to databases and systems, and various attacks, contribute to these security issues [16, 17].

3.1 Dataset used in cyber security

The significance of cybersecurity is discussed in the above sections of this review paper. It is shown that to address these cyber-security vulnerabilities, unique machine-learning challenges must be overcome. It can provide new datasets that accurately explain the difficulties, allowing the academicians to explore the issues and make recommendations for solutions such as solving the common problem of labels being missing in the cybersecurity dataset. Further, the numerous datasets utilized in cyber security research are shown in Fig. 4 [18].

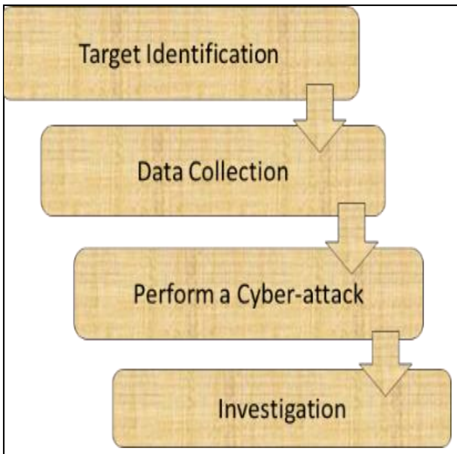

Fig. 3 Anatomy of a cyber-attack and its approach [5].

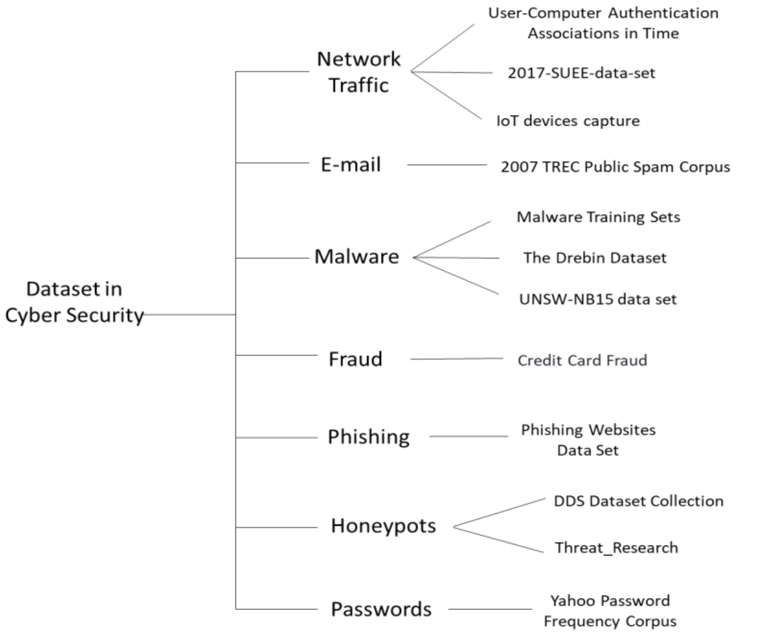

Fig. 4 Various datasets used in cyber security research.

4 Threats

Cyber security threats include illicit internet activity, critical infrastructure security, and insecure computer systems. Crimes like malware, viruses, and denial-of-service assaults target computer networks or services, while fraud, identity theft, phishing schemes, and cyberstalking target non-network or device targets. Various kind of threats are shown in Fig 5.

Cybercrime is the most common type of cyberattack, involving the use of the internet to steal data or resources without user consent. It involves unauthorized access through malicious scripts, such as identity theft, DNS cache poisoning, hacking, piracy, and plagiarism. Cyber vandalism [18] involves destroying or exploiting data by interrupting or terminating network services, causing authorized users to be unable to access the network's data. Web jacking involves unauthorized access to a website, while card information theft involves hacking into an eCommerce server and stealing credit or debit card information. Child pornography involves using computer networks to exploit minors, while spam covers unauthorized transmission of pornographic or illegal product promotions. Cyber trespass involves gaining access to network resources without making changes, while logic bombs operate on events and can be turned on at specific times. Drive-by downloads allow attackers to install harmful software on a victim's computer, allowing them to steal passwords and other sensitive information. Cyber terrorism involves intentional attacks on individuals or organizations using the internet, while cyber-attack by risk involves putting someone in dread for their life or family members. Script kiddies are individuals who breach networks and computer systems, obtain root access, and vandalize websites using scripts or programs.

5 Attacks

The various attacks are depicted in Fig. 6. As technology develops, so do cyber security threats, also referred to as "cyber-attacks," which put users of those systems at risk for a security breach. It can be hard to identify and defend from cyber threats and attacks [19]. Untargeted attacks target individuals or services randomly, while targeted attacks target specific users. Phishing involves sending emails to users asking for sensitive information, while water holing allows access to legitimate websites. Ransomware is used for extortion, and scanning attacks randomly attack the internet. Targeted attacks target specific users, such as spear-phishing and DDOS attacks. Social engineering attacks involve background studies, offering rewards in exchange for breaching security by disclosing private information or granting access to crucial resources.

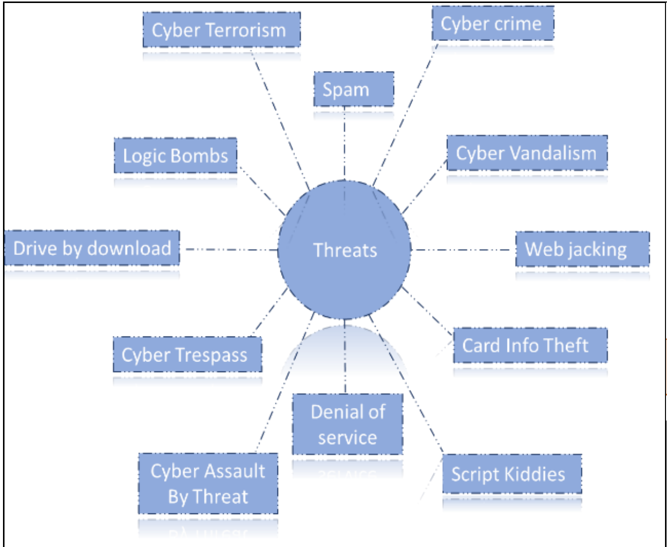

Fig. 5 Various types of threats [17].

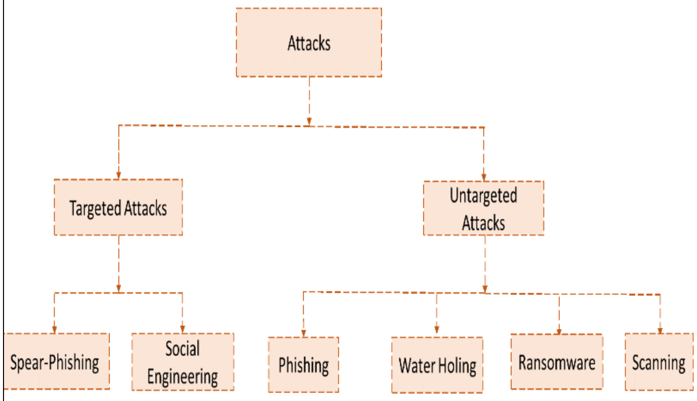

Fig. 6 Classification of attacks [17].

6 Research Trends and challenges

A Visualization for Cyber Security research community (VizSec) reports enduring issues for cyber security by familiarizing and examining information visualization approaches for usage in the cyber security arena. Even though this research effort resulted in a large number of tools and approaches that may be utilized to enhance cyber security, the community has failed to set uniform standards for evaluating these methods to verify their practical validity [20, 21]. The smart grid may be a very appealing target for attackers as a vital infrastructure because internet-based protocols and open-source software are used for controlling and monitoring [22]. The emergence of Smart Grid Cyber-Physical Systems (CPS) is occurring alongside the maturation and integration of Information and Communication Technologies (ICT) within traditional energy systems. Smart grid systems, which are powered by the Internet of Things (IoT), are considered to be critical infrastructures that possess complex architectures and essential components. These communication technologies possess the potential to cause loss of life, disruption of peace, substantial economic damage, or a combination thereof, if their confidentiality, integrity, or availability is compromised. Extracting patterns or insights linked to security incidents from cybersecurity information and creating the right data-driven models is significant to automating and intelligently building security systems [23-24]. Finding insights from data can be made possible by the use of ML. A new scientific paradigm is being guided by ML and data science can drastically alter the state of cybersecurity.

The primary objective of cybersecurity data science involves utilising data-driven methodologies to facilitate intelligent decision-making processes based on security data, hence enabling the development of intelligent solutions for cybersecurity. Partially substituting well-known, conventional security measures like firewalls, user authentication, access control, encryption systems, etc. in light of the goals of the modern cyber organization. Security aims to protect assets from the many threats that result from specific inherent flaws. The underlying technology is the asset that needs to be safeguarded in terms of information and communication security [23]. Cyber security's current progress with some growing fields and attacks is shown in Fig.7.

“The only truly secure system is switched off and unplugged, locked in a titanium safe, buried in a concrete bunker, and surrounded by nerve gas and very highly paid armed guards. Even then, I would not stake my life on it.” **~ Professor Gene Spafford**

Knowing about diverse cyber threats and taking precautions to safeguard the Confidential, Integrity, and Accessibility (or CIA trinity) of the digital world are both components of cybersecurity. If businesses wish to advance successfully and avoid suffering losses at the hands of hackers and other unpleasant destructive attackers, they must defend their assets and ensure that their staff is always prepared to respond to a cyber-attack [25].

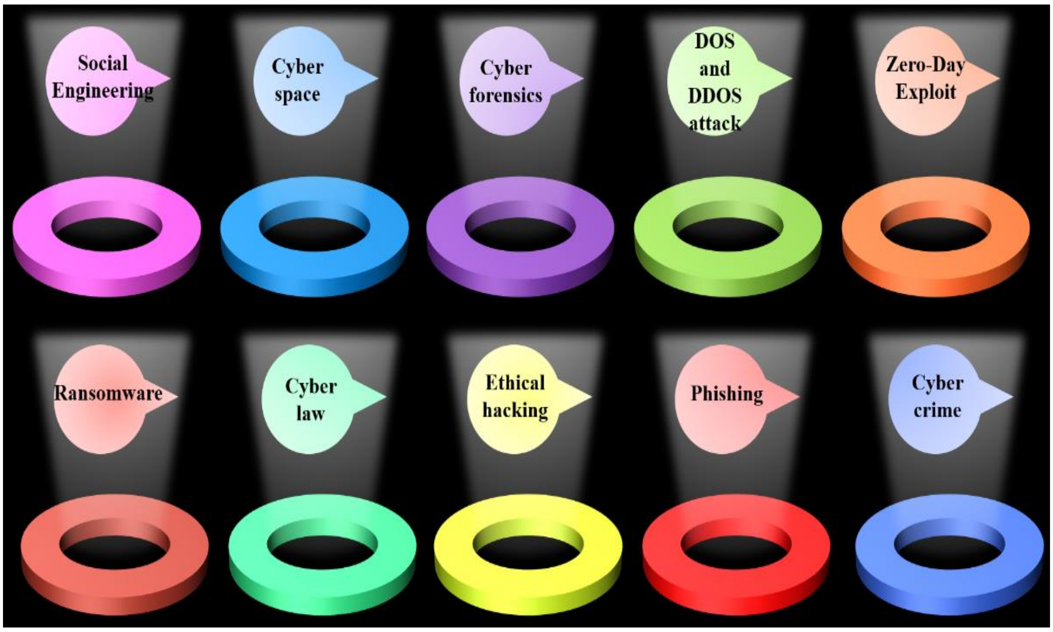

Fig. 7 Information security recent research trends with some growing domains and attacks.

7 SWOT analysis

In this review paper cyber security SWOT analysis is performed as shown in Fig. 9 that comprises strengths, weaknesses, opportunities, and threats. However, there are pros and cons for all technology [8] such as Phishing attacks are now a day become more prominent in various organizations by bad attackers [26-27] and various security risks.

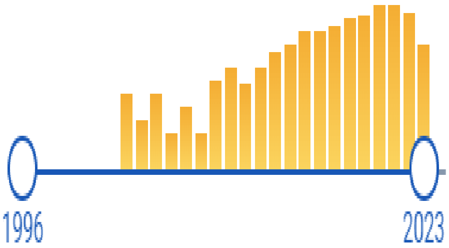

Fig. 8 The number of publications in cyber security.

Conclusion

Considering recently published research, the review makes an effort to assess the enormous threat that cybercrime poses to our daily life. The study highlights the importance of network attacks and cybercrime with their causes and effects. In the future, cyber-attack probability will increase in frequency as 5G, AI, and similar technologies advance such as self-driving automobiles, augmented and virtual reality, smart medical monitoring, etc. Fig. 8 shows the Semantic Scholar search engine with cyber security research publications and is clear from the figure that this field is growing at a very fast speed. We believe that this research paper will support the researchers to find the literature and open issues in cyber security.

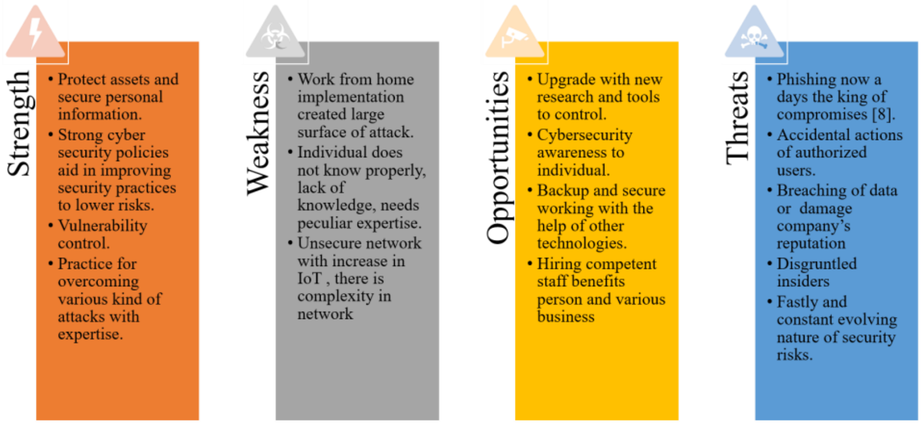
Strength
• Protect assets and secure personal information.
• Strong cyber security policies aid in improving security practices to lower risks.
• Vulnerability control.
• Practice for overcoming various kind of attacks with expertise.
Weakness
• Work from home implementation created large surface of attack.
• Individual does not know properly, lack of knowledge, needs peculiar expertise.
• Unsecure network with increase in IoT , there is complexity in network
Opportunities
• Upgrade with new research and tools to control.
• Cybersecurity awareness to individual.
• Backup and secure working with the help of other technologies.
• Hiring competent staff benefits person and various business
Threats
• Phishing now a days the king of compromises [8].
• Accidental actions of authorized users.
• Breaching of data or damage company's reputation
• Disgruntled insiders
• Fastly and constant evolving nature of security risks.

Fig. 9 SWOT analysis of cyber security.

References

1. Bruce Middleton. “A history of cyber security attacks: 1980 to present.” CRC Press, 2017.
2. Saloni Khurana, "Review paper on cyber security." Int. J. Eng. Res. Technol. (IJERT) ISSN: 2278-0181, 2017.https://www.ijert.org/a-review-paper-on-cyber-security
3. Ashwini Sheth, Sachin Bhosale, and Adnan Bukhari. "A Survey on Cyber Security." Contemporary Research in India, Special Issue, 2021.
4. Muqbil, Cyber security experts warn massive threat activity against SVB following collapse, ETCIO, 2023
5. Alex Andrew, Sam Spillard, Joshua Collyer, and Neil Dhir. "Developing optimal causal cyber-defence agents via cyber security simulation." arXiv preprint arXiv:2207.12355, 2022. https://doi.org/10.48550/arXiv.2207.12355
6. Shah Md Istiaque, Md Toki Tahmid, Asif Iqbal Khan, Zaber Al Hassan, and Sajjad Waheed. "State-of-the-Art Artificial Intelligence Based Cyber Defense Model." In 2021 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), pp. 1-6. IEEE, 2021.
7. Gautam Srivastava, Rutvij H. Jhaveri, Sweta Bhattacharya, Sharnil Pandya, Praveen Kumar Reddy Maddikunta, Gokul Yenduri, Jon G. Hall, Mamoun Alazab, and Thippa Reddy Gadekallu. "XAI for cybersecurity: state of the art, challenges, open issues and future directions." arXiv preprint arXiv:2206.03585, 2022.
8. IANS, 83% organisations in India reported rise in phishing attacks during Covid, ETCIO.com From the Economic Times, September 2021
9. Chuyi, Yan, Chen Zhang, Zhigang Lu, Zehui Wang, Yuling Liu, and Baoxu Liu. "Blockchain abnormal behavior awareness methods: a survey." Cybersecurity 5, no. 1: 5, 2022.
10. Victor Mayoral-Vilches, Ruffin White, Gianluca Caiazza, and Mikael Arguedas. "Sros2: Usable cyber security tools for ros 2." In 2022 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), pp. 11253-11259. IEEE, 2022.
11. Ricardo M. Czekster, Roberto Metere, and Charles Morisset. "Incorporating Cyber Threat Intelligence into Complex Cyber-Physical Systems: A STIX Model for Active Buildings." Applied Sciences 12, no. 10 (2022): 5005.https://doi.org/10.3390/app12105005, 2022
12. Carsten Maple, Matthew Bradbury, Anh Tuan Le, and Kevin Ghirardello. "A connected and autonomous vehicle reference architecture for attack surface analysis." Applied Sciences 9, no. 23: 5101, 2019.
13. Rahul K. Vigneswaran, R. Vinayakumar, K. P. Soman, and Prabaharan Poornachandran. "Evaluating shallow and deep neural networks for network intrusion detection systems in cyber

security." In 2018 9th International conference on computing, communication and networking technologies (ICCCNT), pp. 1-6. IEEE, 2018.

14. Yuqi Chen, Bohan Xuan, Christopher M. Poskitt, Jun Sun, and Fan Zhang. "Active fuzzing for testing and securing cyber-physical systems." In Proceedings of the 29th ACM SIGSOFT International Symposium on Software Testing and Analysis, pp. 14-26, 2020.

15. Elhaam Abdulrahman Debas, Razan Sulaiman Alajlan, and MM Hafizur Rahman. "Biometric in Cyber Security: A Mini Review." In 2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), pp. 570-574. IEEE, 2023.

16. Mohammad Kamrul Hasan, AKM Ahasan Habib, Zarina Shukur, Fazil Ibrahim, Shayla Islam, and Md Abdur Razzaque. "Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations." Journal of Network and Computer Applications 209: 103540, 2023.

17. Aušrius Juozapavičius, , Agnė Brilingaitė, Linas Bukauskas, and Ricardo Gregorio Lugo. "Age and gender impact on password hygiene." Applied Sciences 12, no. 2: 894, 2022. https://doi.org/10.3390/app12020894.

18. https://github.com/shramos/Awesome-Cybersecurity-Datasets#email

19. Tushar P., Parikh, and Ashok R. Patel. "Cyber security: Study on attack, threat, vulnerability." 2017 International Journal of Research in Modern Engineering and Emerging Technology, 2017. https://www.raijmr.com/ijrmeet/wp-content/uploads/2017/12/IJRMEET_2017_vol05_issue_06_01.pdf

20. Youngsun Kwak, Seyoung Lee, Amanda Damiano, and Arun Vishwanath. "Why do users not report spear phishing emails?" Telematics and Informatics 48: 101343, 2020. https://doi.org/10.1016/j.tele.2020.101343

21. Diane Staheli, Tamara Yu, R. Jordan Crouser, Suresh Damodaran, Kevin Nam, David O'Gwynn, Sean McKenna, and Lane Harrison. "Visualization evaluation for cyber security: Trends and future directions." In Proceedings of the Eleventh Workshop on Visualization for Cyber Security, pp. 49-56. 2014. https://doi.org/10.1145/2671491.2671492

22. Muhammed Zekeriya Gunduz, and Resul Das. "Cyber-security on smart grid: Threats and potential solutions." Computer networks 169: 107094, 2020. https://doi.org/10.1016/j.comnet.2019.107094

23. Iqbal H Sarker, A. S. M. Kayes, Shahriar Badsha, Hamed Alqahtani, Paul Watters, and Alex Ng. "Cybersecurity data science: an overview from machine learning perspective." Journal of Big data 7: 1-29, 2020. https://doi.org/10.1186/s40537-020-00318-5

24. Solms Von, Rossouw, and Johan Van Niekerk. "From information security to cyber security." computers & security 38: 97-102, 2013. https://doi.org/10.1016/j.cose.2013.04.004

25. Vijay Anant, Athavale, and Ankit Bansal. "Problems with the implementation of blockchain technology for decentralized IoT authentication: A literature review." Blockchain for Industry 4.0: 91-119, 2022.

26. Bhardwaj, Ritu Tyagi, Neha Sharma, Akhilendra Khare, Manbir Singh Punia, and Vikash Kumar Garg. "Network intrusion detection in software defined networking with self-organized constraint-based intelligent learning framework." Measurement: Sensors 24: 100580, 2022.https://doi.org/10.1016/j.measen.2022.100580

27. Muqbil, ChatGPT is transformational with wide ranging ramifications:tech leaders, ETCIO, (2023)