Review Article

ACCENTS Transactions on Information Security, Vol 7(25)
ISSN (Online): 2455-7196
http://dx.doi.org/10.19101/TIS.2021.621013

Cybersecurity data science and threats: an overview from machine learning perspective

Shivam Priyadarshi* **and M. Adil Hashmi**
Madhyanchal Professional University, Bhopal, Madhya Pradesh, India

Received: 15-December-2021; Revised: 20-January-2022; Accepted: 22-January-2022

Abstract
Cybersecurity has become a significant threat to all operations in the modern world. Due to the continuous development of information and communication (ICT) technologies, the efficiency of machine operation has been improved. Therefore, extracting the pattern of a security incident from the cybersecurity and corresponding data-driven model is the primary element to make an automated security system. To analyse and understand the actual phenomena, different machine learning methods, systems and processes are used. This work also sheds light on how the security system and measures can be improved and maintained by bringing innovation in technology and upgrading the power systems. An example of cybersecurity risks in power systems is the two simultaneous malicious attacks that occurred in 2015 and 2016. Besides, in the IT and healthcare industry, the number of cyberattacks is increasing daily, increasing the cost of data breaches. The distribution of cyberattacks across different countries is discussed in this research. Additionally, issues of cyber physical system (CPS) and its impacts on human society have also been inspected in the work following.

Keywords
Cybersecurity, Cyber physical systems, Machine learning, Information and communication.

1.Introduction
Due to the growing dependency on internet of things (IoT) and digitalisation, different security incidents such as zero-day attacks, malware attacks, data breaches and unauthorised access, have grown significantly in recent years [1]. Cyberattacks and crime may cause destructive financial losses as well as affect individuals and organisations. As per the view of Zong et al. (2019), [2] software vulnerabilities can be defined as the flaws that foster the chances of occurring cyberattacks in computer systems. Vulnerabilities remain unknown for users when new software is published. This is because users do not have adequate knowledge regarding the root problems and the gap in the software. It is noticed that cybersecurity threats in the power systems, healthcare sector, IT industry and government organisations have become a serious issue. As stated by Bagale et al. (2021) [3], small and medium-sized enterprises usually face cyberattacks and data breach issues due to inadequate knowledge, lack of funding and technical support.

According to Sadiq et al. (2021) [4], there are four types of attacks that are phishing attacks, malware attacks, ransomware attacks and SQL injection attacks, which are mainly responsible for data hacking, misplacement and corruption in recent times. As depicted by Neto et al. (2021), [5] in 2019, 15.1 billion private data have been exposed through unauthorised access. As a result, organisational performance is affected, which tends to hinder brand reputation. This is also a reason for the cyber insurance has been taken into consideration nowadays to manage cybersecurity risks. Soe et al. (2020) [6] proposed a new selection framework and an algorithm which is known as the correlated-set thresholding on gain-ratio (CST-GR) algorithm. In the case of the selection algorithm, the selection result totally depends on the merit function, which has become a major problem in recent times. The author has also focused on calculating each value of the gain feature.

The security teams in different organisations have faced unprecedented security challenges over time [1]. As per the view of Saxena et al. (2020) [7], information security has also witnessed a critical challenge that is required to be mitigated by organisations to keep the customer's and

*Author for correspondence

organisations' records confidential. A recent report showcases that around 71% of global organisations have experienced ransomware attacks which were 68.5% in 2020 [8]. In contrast to Kurniati, and Sahide (2022) [9], in 2021, the rate of malware attacks has been valued at 5.4 billion. As the rate of security attacks is continuously increasing, maintaining cybersecurity has become a major challenge for the security team of the industry. As opined by Alahmari and Duncan (2020) [10], inadequate knowledge among employees of the organisation increases the chances of cybersecurity threats. Proper training can help to solve this problem in the future.

The major goal of cybersecurity in the field of data science is intelligent decision-making from relevant data for cybersecurity solutions [1]. The integration of operation technology and information technology enables people to form a cyber physical system (CPS) that focuses on the communication between computation, physical and networking processes [11]. CPS permits people to create, imagine, permit, develop and refine smart systems in different fields for the betterment of companies and industries. According to Yaacoub et al. (2020) [12], CPS contributes to making people's life better by enabling and developing a wider range of applications and services including smart homes, e-commerce and e-health. Zhang et al. (2021) [13], suggested that the CPS is prone to various physical and cyber security attacks, challenges and threats. This happened due to its heterogeneous and grounded nature meaning that it is more reliant on sensitive and private data and its large range of deployment in smart applications. That is why the researcher has chosen this topic to address the gap in CPS and recommend an effective reliable security solution. The primary motivation of this work is to identify the main cybersecurity and CPS threats, attacks and vulnerabilities and discuss the limitations and advantages of existing solutions.

The primary objective of this paper is to analyse the impacts of cybersecurity threats on human society and organisational performance. Additionally, this research study will highlight the challenges, threats and limitations of cyber-physical systems that are being faced by people, while handling any task. This research will also emphasis analysing the role of data science in the field of cybersecurity.

This study has done a significant job of reviewing the more complex aspects of cybersecurity threats and the existing security solution. This research work has discussed numerous factors extensively, which have contributed to cyberattacks and their impacts on human society. The major contribution of this paper is described as follows,

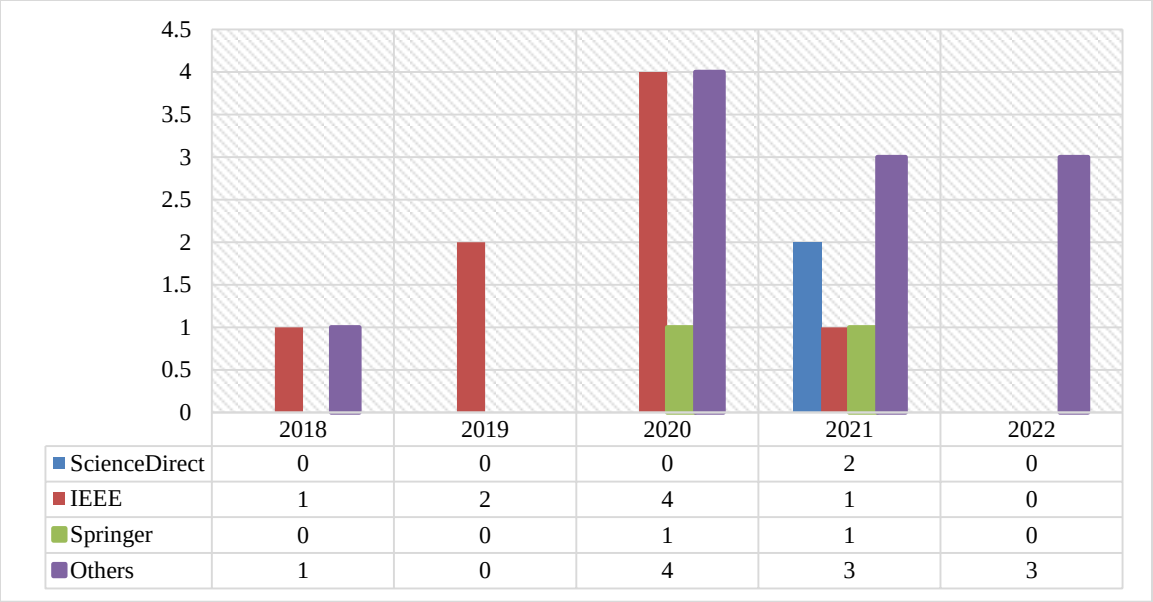
- The exploration of several factors and variables associated with cybersecurity threats and CPS
- The proper review of the methodological results, indicating the issues related to threats and CPS and the limitations of the existing security solutions
- The review and analysis of the machine learning algorithms for identifying and classifying cybersecurity threats

2.Related works

This section has focused on previous works that are conducted based on cybersecurity threats, cyberattacks and CPS. The discussion of this section covers the advantages, limitations and advantages of existing security solutions such as Firewall, Encryption tools and antivirus software. A total of 23 relevant research articles and journals have been reviewed in this part to critically evaluate the impacts of cyberattacks and the way of maintaining security in real-life. Different machine learning methods are being used by the developers to detect the chances of security threats at the early stage. ScienceDirect, IEEE, MDPI, Springer and other publishers have been considered by the researcher to critically evaluate the impacts of cyber threats on society. At the starting time, the researcher has chosen more than 50 articles and journals for reviewing cybersecurity strategies and their limitations. After removing Non-English and Non-method samples, 23 research papers have been finally selected for the purpose of analysis and review. The distribution of research samples considered from 2018 to 2022 is properly shown in the figure depicted in *Figure 1*.

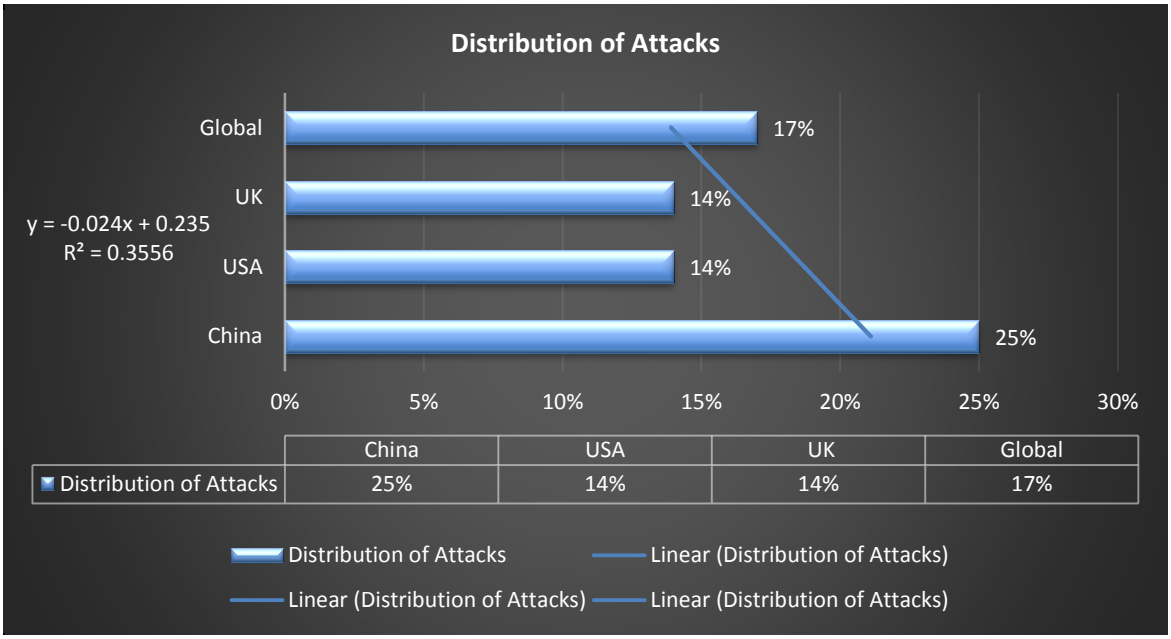
Concept of Cybersecurity: The term cybersecurity is used in several contexts from mobile computing to businesses and is segmented into some common categories including network security, information security, operational security and application security [14]. Network security is mainly concerned with securing the existing system network from intruders and hackers. Sarker et al. (2020) [1] stated that application security focuses on keeping systems and software free from potential cyber threats whereas operational security includes fruitful processes that enable developers of protecting and handling data assets. As illustrated by Seemma, Nandhini, and Sowmiya (2018) [15], information security emphasises keeping confidential data secure and protecting information from hacking and corruption. In general, cybersecurity systems are considered

computer security systems and network security system that contains antivirus software, IDS (Intrusion Detection System) and a Firewall [16] (*Figure 2*).



	2018	2019	2020	2021	2022
ScienceDirect	0	0	0	2	0
IEEE	1	2	4	1	0
Springer	0	0	1	1	0
Others	1	0	4	3	3

Figure 1 Distribution of the total number of papers



	China	USA	UK	Global
Distribution of Attacks	25%	14%	14%	17%

Figure 2 Distribution of attacks in different countries

Prevalence of cyberattacks and their impacts: Covid-19 has brought significant changes in human life as a result traditional systems have converted to digital systems [17]. It is noticed that the number of cyberattacks has increased during the period of Covid-19. According to Lallie et al. (2021) [18], in the last quadrant of 2020, the global rate of cyberattacks in terms of the number of cyberattacks and their impacts, the cyberattacks rate in the UK has increased by 14%. Similarly, there is a 14% increase seen in the number of cyberattacks in the USA. Li and Liu (2021) [19] claimed that cyberattacks are reviewed and considered within the context of the global occurrence of cyberattacks. World Health

Organization (WHO) has published this report regarding the distribution of cyberattacks in both developing and developed countries. Moreover, the average number of cyberattacks has risen by 17% across the world due to the lack of technical support, and inadequate knowledge among employees and others [19]. As stated by Ahmad et al. (2020) [20], the primary reasons behind increasing the rate of attacks are ineffective security policies and measures. It is estimated that the total data breach cost will be $10.5 trillion by the end of 2025 [21]. Hence, it is needed to develop an effective cybersecurity policy and strategies including establishing a firewall, using updated antivirus and utilising a strong user ID and password. Small and medium-sized enterprises have the maximum chances of facing cyberattacks as compared to large enterprises [10].

As opined by Bubukayr and Almaiah (2021) [22], smartphones become the lucrative target of attackers because most people use mobile phones in managing their daily-based tasks. In contrast to Bongomin et al. (2020), [23] the use of smartphones has become essential in every field including the retail industry, government agencies, the education sector, entertainment and many other industries. Alahmari and Duncan, (2020) [10] stated that smartphone security threats are on the rise, and account for around 60% of fraud, from stolen passwords to phishing attacks. Two main cyber threats are noticed which are data theft and data losses [24]. Updated antivirus and strong passwords will help people to protect smartphones or mobile devices from being hacked. CPS are designated as necessary parts of IoT and they are mainly supported by Industry 4.0 technologies. CPS helps people to operate real-time smart applications accurately [12]. As depicted by Reich et al. (2020) [25], although CPS has different usability in smart applications, it poses a cyber security challenge for people. The main reason for generating cyber threats is its overreliance on sensitive and private data. It might lead to the unaccepted overhead of the network system, especially in the context of latency. As per the view of Tantawy (2022) [26], zero-day vulnerability could be generated due to the increasing use of CPS systems in real-life applications. On the other hand, there are different kinds of cybersecurity events which can result in a security risk to an individual, organisation's network and systems are as follows:
Malware: Malware refers to malicious software that is intentionally developed and designed to cause and affect or damage a system, computer network and client-server [27]. Different types of malwares such as Trojan, Ransomware, Denial of Service, Phishing and Zero-day-attack aim to steal confidential data and block the access of authorised users until the data is stolen [1].

Unauthorised access: Unauthorised access signifies the action of accessing private data from the computer system without having any kind of authorisation [28]. It leads to the violation of existing security policies.

Cybersecurity strategies: Effective strategies are required to protect the private records of an organisation and individual. As per the cybersecurity defence policy, an intrusion detection system has started to be established by the companies to protect endpoint and entry point network systems [29]. IDS are of different types based on scope and usage. As stated by Othman et al. (2018) [30], host-based intrusion detection system (HIDS) and network-based intrusion detection (NIDS) systems are two common types of IDS depending on the scope of one machine to large networks. As per the opinion of Einy et al. 2021 [31], two types of IDS are in use, that is anomaly-based IDS and Signature based IDS. All types of mentioned IDS are used to protect existing network systems from cyberattacks as well as a detect intrusion at the early stage. As suggested by Abdullah et al. (2019) [32], strong user ID and passwords needs to be used to store private data in a secure way. In this instance, updated antivirus will also help to notify users about the potential security threat and provide a chance for users to take immediate actions in reducing the chances of cyberattacks. Although there are many existing solutions, the skills gap among employees is also increasing the tendency of cyberattacks, resulting in violating cybersecurity policies [33].

The major problem found by the researchers are the variable nature of security threats and the time of detection.

3.Analysis based on results

The result-based analysis is shown in *Table 1*.

The major findings from the review and analysis of the above-discussed research papers are described in the below part.

- Deep learning and machine learning methods are efficient in the detection of cybersecurity threats. These approaches can be used considering the detection from disease data also [39-43].

- Both the DT and SVM provide better accuracy in the case of detecting cyber security threats at the early stage.
- It is also found that the logistic regression model is more efficient in discovering security vulnerabilities than other regression models.
- An effective IDS system needs to be established by the organisation or individual to secure the existing network system.
- Strong passwords, encrypted code and updated antivirus need to be used by people to protect the computer system and mobile applications from cyberattacks [44, 45].

Table 1 Result based analysis

S. No.	Source	Method	Results	Gap
1	[34]	Entity-based crowdsourcing model	Crowds, processing units, external impartial resources and processing units are the key components of this proposed model. This Entity based crowd-sourcing model is proposed by the researcher to mitigate cybersecurity threats with the help of crowdsourcing.	IoT: Limitations in the computation and storage
2	[1]	Deep learning, multilayer perceptron (MLP) and artificial neural network (ANN)	Machine learning methods play a vital role to inspect the behavioural pattern of security data. In this instance, multiple data processing frameworks are useful to identify security information from the existing raw data that helps in bruising a smart cybersecurity machine.	A lack of conventional solutions has been encountered because the number of cybersecurity incidents is significantly increasing
3	[35]	Support vector machine (SVM), decision tree (DT), random forest (RF), naïve Bayes (NB), ANN and deep belief networks (DBN)	The result indicates that the DT, SVM and Random Forest have provided the maximum accuracy in identifying the cybersecurity solution. However, the ANN and DBN method has given the best recall value in the case of intrusion detection.	Handling new variations of systems and a brief discussion about the advantages of each classification model
4	[36]	Cognitive cybersecurity model, custom ransomware design and concept network architecture	The result exhibits that the proposed developed cognitive dashboard is capable in reporting the event of cybersecurity. This system is capableable to give proper security solutions by testing the ransomware attacks	Implementing an effective new system to add new cybersecurity threats
5	[37]	Constrained application protocol, advanced message queuing protocol (AMQP), and data distribution service	The common technology that is mainly used in detecting cybersecurity threats is edge computing, blockchain, fog computing and machine learning methods. It is found that the security team and developers more rely on blockchain technology to detect cybersecurity threats as compared to other technologies.	Limited computation capability and new cybersecurity threats
6	[38]	Attack System Configuration, KNN, Linear SVC, SVM, DT, RF and SVM	It is found that the cross-validation score of the DT (0.895) is better as compared to other methods. Therefore, the researcher has recommended using DT for predicting the number of cyberattacks more accurately at the early stage. The proposed model derived from DT and logistic regression gives 92% accuracy in maintaining the security of password authentication.	New security vulnerabilities and threats
7	[4]	Data mining, deep learning and machine learning	Machine learning models help people to detect cybersecurity threats. In this paper, the researcher has recommended different security strategies to protect against the threat of cyberattacks such as establishing a firewall on the network, updating antivirus and using strong passwords.	No practical implementation
8	[12]	Cryptographic authentication and encrypted data	CPS must be secure to reduce the chances of cyberattacks. Encrypted code can help people to reduce potential cybersecurity threats.	Differential privacy and limited application
9	[13]	CPS scenario analysis	The relevant paper survey the way of detecting	Requiring larger sample

S. No.	Source	Method	Results	Gap
		method	cyberattacks by using machine learning and deep learning. It is evident that these method enables people to detect cybersecurity threat by analysing raw data.	data

4.Discussion

Figure 3 shows the light on the analysis of the role of machine learning and deep learning methods in detecting cybersecurity threats.

- This paper effectively reflected the impacts of the research topic and introduces the primary region of cybersecurity.
- It is found from this research that machine learning models such as SVM, logistic regression, DT, RF and ANN provide the best way to detect the potential threat of cyberattacks at the early stage.
- This study has also discussed how the machine learning models works in detecting cybersecurity threats and recommended the existing strategy that is available in the cybersecurity solution.
- SVM and DT have given high accuracy in the early detection of cybersecurity threats.
- It is also known that Firewall needs to be established on the endpoint and entry point network system to secure private records from hacking, data misplacement and corruption.

This paper provided an in-depth analysis of cybersecurity threats and their impacts on an individual and organisations. The advantages and restrictions of the ML methods are diverse. The research is confined to emphasising all the benefits and drawbacks of the existing cybersecurity solutions in order to broaden the topic.

A complete list of abbreviations is shown in *Appendix I.*

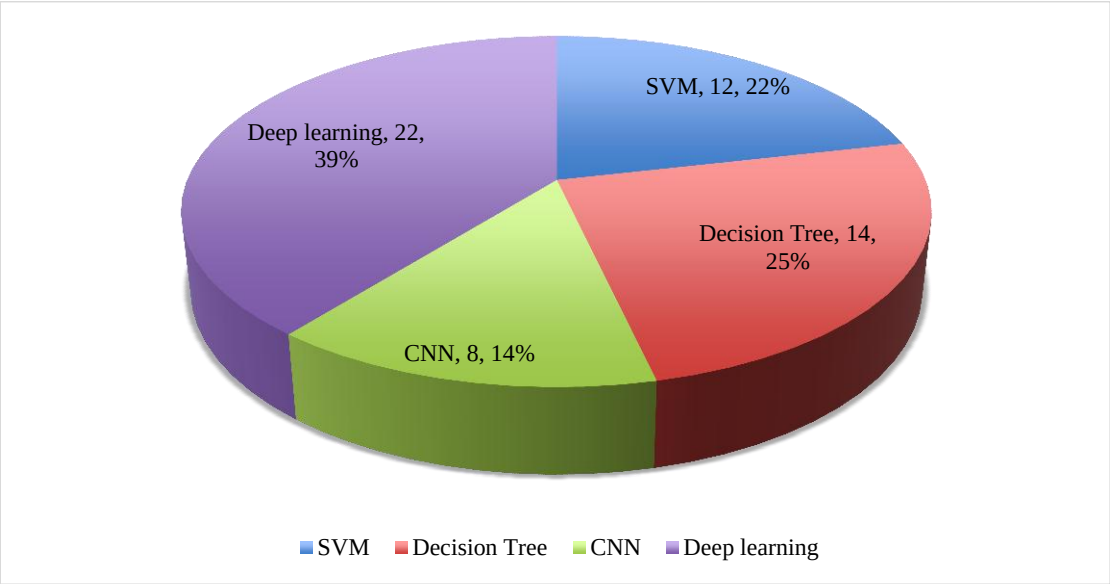


Figure 3 Methodology used in cybersecurity threat detection

5.Conclusion and future work

As per the above discussion, over time, the security teams in various organisations have encountered never-before-seen security difficulties. Organizations must address a serious challenge in information security in order to protect the privacy of their customers and their own data. Maintaining cybersecurity has become a significant problem for the industry's security team as the frequency of security attacks keeps rising. Proper security management can be provided considering the aspects of detection, prevention and updates. These three aspects are important as there’re is the need of applicability of proper prevention mechanism along with the detection strategies which should be updated time to time.

Acknowledgment
None.

Conflicts of interest
The authors have no conflicts of interest to declare.

References
[1] Sarker IH, Kayes AS, Badsha S, Alqahtani H, Watters P, Ng A. Cybersecurity data science: an overview from machine learning perspective. Journal of Big Data. 2020; 7:1-29.
[2] Zong S, Ritter A, Mueller G, Wright E. Analyzing the perceived severity of cybersecurity threats reported on social media. arXiv preprint arXiv:1902.10680. 2019:1-11.
[3] Bagale GS, Vandadi VR, Singh D, Sharma DK, Garlapati DV, Bommisetti RK, et al. Small and medium-sized enterprises' contribution in digital technology. Annals of Operations Research. 2021:1-24.
[4] Sadiq A, Anwar M, Butt RA, Masud F, Shahzad MK, Naseem S, Younas M. A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0. Human Behavior and Emerging Technologies. 2021; 3(5):854-64.
[5] Neto NN, Madnick S, Paula AM, Borges NM. Developing a global data breach database and the challenges encountered. Journal of Data and Information Quality. 2021; 13(1):1-33.
[6] Soe YN, Feng Y, Santosa PI, Hartanto R, Sakurai K. Towards a lightweight detection system for cyber attacks in the IoT environment using corresponding features. Electronics. 2020; 9(1):1-19.
[7] Saxena N, Hayes E, Bertino E, Ojo P, Choo KK, Burnap P. Impact and key challenges of insider threats on organizations and critical businesses. Electronics. 2020; 9(9):1-29.
[8] https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/. Accessed 10 November 2022.
[9] Kurniati E, Sahide A. Paris call as french diplomacy instrument. International Journal of Multicultural and Multireligious Understanding. 2022; 9(8):442-54.
[10] Alahmari A, Duncan B. Cybersecurity risk management in small and medium-sized enterprises: a systematic review of recent evidence. In international conference on cyber situational awareness, data analytics and assessment 2020(pp. 1-5). IEEE.
[11] Kavallieratos G, Katsikas S. Managing cyber security risks of the cyber-enabled ship. Journal of Marine Science and Engineering. 2020; 8(10):1-19.
[12] Yaacoub JP, Salman O, Noura HN, Kaaniche N, Chehab A, Malli M. Cyber-physical systems security: limitations, issues and future trends. Microprocessors and Microsystems. 2020; 77:1-33.
[13] Zhang J, Pan L, Han QL, Chen C, Wen S, Xiang Y. Deep learning based attack detection for cyber-physical system cybersecurity: a survey. IEEE/CAA Journal of Automatica Sinica. 2021; 9(3):377-91.
[14] Ma C. Smart city and cyber-security; technologies used, leading challenges and future recommendations. Energy Reports. 2021; 7:7999-8012.
[15] Seemma PS, Nandhini S, Sowmiya M. Overview of cyber security. International Journal of Advanced Research in Computer and Communication Engineering. 2018; 7(11):125-8.
[16] Alqahtani H, Sarker IH, Kalim A, Minhaz Hossain SM, Ikhlaq S, et al. Cyber intrusion detection using machine learning classification techniques. In computing science, communication and security: first international conference 2020 (pp. 121-31). Springer Singapore.
[17] Soto-Acosta P. COVID-19 pandemic: Shifting digital transformation to a high-speed gear. Information Systems Management. 2020; 37(4):260-6.
[18] Lallie HS, Shepherd LA, Nurse JR, Erola A, Epiphaniou G, Maple C, et al. Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security. 2021; 105:1-20.
[19] Li Y, Liu Q. A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments. Energy Reports. 2021; 7:8176-86.
[20] Ahmad A, Desouza KC, Maynard SB, Naseer H, Baskerville RL. How integration of cyber security management and incident response enables organizational learning. Journal of the Association for Information Science and Technology. 2020; 71(8):939-53.
[21] Sharif MH, Mohammed MA. A literature review of financial losses statistics for cyber security and future trend. World Journal of Advanced Research and Reviews. 2022; 15(1):138-56.
[22] Bubukayr MA, Almaiah MA. Cybersecurity concerns in smart-phones and applications: a survey. In international conference on information technology 2021 (pp. 725-31). IEEE.
[23] Bongomin O, Gilibrays Ocen G, Oyondi Nganyi E, Musinguzi A, Omara T. Exponential disruptive technologies and the required skills of industry 4.0. Journal of Engineering. 2020; 2020:1-7.
[24] Kettani H, Wainwright P. On the top threats to cyber systems. In 2nd international conference on information and computer technologies 2019 (pp. 175-9). IEEE.
[25] Reich J, Schneider D, Sorokos I, Papadopoulos Y, Kelly T, Wei R, et al. Engineering of runtime safety monitors for cyber-physical systems with digital dependability identities. In computer safety, reliability, and security: 39th international conference, 2020 (pp. 3-17). Springer International Publishing.
[26] Tantawy A. On the elements of datasets for cyber physical systems security. arXiv preprint arXiv:2208.08255. 2022.
[27] Aslan ÖA, Samet R. A comprehensive review on malware detection approaches. IEEE Access. 2020; 8:6249-71.
[28] Sarker IH, Furhad MH, Nowrozy R. Ai-driven cybersecurity: an overview, security intelligence

modeling and research directions. SN Computer Science. 2021; 2:1-8.
[29] Ghelani D, Hua TK, Koduru SK. Cyber security threats, vulnerabilities, and security solutions models in banking. Authorea Preprints. 2022.
[30] Othman SM, Alsohybe NT, Ba-Alwi FM, Zahary AT. Survey on intrusion detection system types. International Journal of Cyber-Security and Digital Forensics. 2018; 7(4):444-63.
[31] Einy S, Oz C, Navaei YD. The anomaly-and signature-based IDS for network security using hybrid inference systems. Mathematical Problems in Engineering. 2021; 2021:1-10.
[32] Abdullah TA, Ali W, Malebary S, Ahmed AA. A review of cyber security challenges attacks and solutions for Internet of Things based smart home. IJCSNS International Journal of Computer Science and Network Security. 2019; 19(9):139-46.
[33] Al-Alawi AI, Al-Bassam MS. The significance of cybersecurity system in helping managing risk in banking and financial sector. Journal of Xidian University. 2020; 14(7):1523-36.
[34] Nieto A, Acien A, Fernandez G. Crowdsourcing analysis in 5G IoT: cybersecurity threats and mitigation. Mobile Networks and Applications. 2019; 24:881-9.
[35] Shaukat K, Luo S, Varadharajan V, Hameed IA, Chen S, Liu D, et al. Performance comparison and current challenges of using machine learning techniques in cybersecurity. Energies. 2020; 13(10):1-27.
[36] Narayanan SN, Ganesan A, Joshi K, Oates T, Joshi A, Finin T. Early detection of cybersecurity threats using collaborative cognition. In 4th international conference on collaboration and internet computing 2018 (pp. 354-63). IEEE.
[37] Altulaihan E, Almaiah MA, Aljughaiman A. Cybersecurity threats, countermeasures and mitigation techniques on the IoT: future research directions. Electronics. 2022; 11(20):1-41.
[38] Lee K, Yim K. Cybersecurity threats based on machine learning-based offensive technique for password authentication. Applied Sciences. 2020; 10(4):1-16.
[39] Dubey AK, Dubey AK, Namdev M, Shrivastava SS. Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment. In CSI sixth international conference on software engineering 2012 (pp. 1-8). IEEE.
[40] Dubey AK, Gupta U, Jain S. Computational measure of cancer using data mining and optimization. In sustainable communication networks and application 2020 (pp. 626-32). Springer International Publishing.
[41] Dubey A, Gupta U, Jain S. Medical data clustering and classification using TLBO and machine learning algorithms. Computers, Materials and Continua. 2021; 70(3):4523-43.
[42] Nemade V, Pathak S, Dubey AK, Barhate D. A review and computational analysis of breast cancer using different machine learning techniques. International Journal of Emerging Technology and Advanced Engineering. 2022; 12(3):111-8.
[43] Chahar R, Dubey AK, Narang SK. A review and meta-analysis of machine intelligence approaches for mental health issues and depression detection. International Journal of Advanced Technology and Engineering Exploration. 2021; 8(83):1279-314.
[44] Patil SS, Patidar K, Saxena G, Sharma N. An improve image security algorithm using hybrid cryptography approach. ACCENTS Transactions on Information Security. 2021; 6 (23):13-9.
[45] Shrivastava A, Dubey AK. An efficient hybrid encryption approach with bit shuffling for image data security. ACCENTS Transactions on Information Security. 2021; 6(24):20-25.

Md Adil Hashmi is working as Assistant proffesor with the department of Computer Science and Engineering at Madhyanchal Proffessional University , Bhopal , India. He has completed his Bachelor of Engineering and Master of Technology in Computer Science Engineering from Rajeev Gandhi Technical University Bhopal (M.P). He has more than Five Publication in reputed general and conferences His reserch area in network and web security, etc.
Email:adilhashmi17@gmail.com

Appendix I

S. No.	Abbreviation	Description
1	AMQP	Advanced Message Queuing Protocol
2	ANN	Artificial Neural Network
3	CPS	Cyber Physical System
4	CST-GR	Correlated-Set Thresholding on Gain-Ratio
5	DBN	Deep Belief Networks
6	DT	Decision Tree
7	HIDS	Host-Based Intrusion Detection System
8	ICT	Information and Communication
9	IoT	Internet of Things
10	MLP	Deep Learning, Multilayer Perceptron
11	NB	Naïve Bayes
12	RF	Random Forest
13	SVM	Support Vector Machine
14	WHO	World Health Organization