Cyber Security Attacks Detecting Thread in the Virtual World of Corporate Sectors

Manasa R. [1], & A. Jayanthila Devi [2]

[1] Research Scholar, Institute of Computer Science and Information Science, Srinivas University, Mangalore, India,
ORCID: 0000-0003-0392-2388; E-mail: manasa.ccis@srinivasuniversity.edu.in

[2] Professor, Institute of Computer Science & Information Science, Srinivas University, Mangalore – 575001, India,
ORCID: 0000-0002-6023-3899; Email: drjayanthila@gmail.com

Area of the Paper: Computer Science.
Type of the Paper: Literature Review.
Type of Review: Peer Reviewed as per |C|O|P|E| guidance.
Indexed In: OpenAIRE.
DOI: https://doi.org/10.5281/zenodo.7818522
Google Scholar Citation: IJCSBE

How to Cite this Paper:
R., Manasa, & A., Jayanthila Devi, (2023). Cyber Security Attacks Detecting Thread in the Virtual World of Corporate Sectors. *International Journal of Case Studies in Business, IT, and Education (IJCSBE), 7*(2), 90-105. DOI: https://doi.org/10.5281/zenodo.7818522

International Journal of Case Studies in Business, IT and Education (IJCSBE)
A Refereed International Journal of Srinivas University, India.

Crossref DOI: https://doi.org/10.47992/IJCSBE.2581.6942.0261

Paper Submission: 08/07/2022
Paper Publication: 12/04/2023

International Journal of Case Studies in Business, IT, and Education (IJCSBE), ISSN: 2581-6942, Vol. 7, No. 2, April 2023

SRINIVAS PUBLICATION

Cyber Security Attacks Detecting Thread in the Virtual World of Corporate Sectors

Manasa R. [1], & A. Jayanthila Devi [2]

[1] Research Scholar, Institute of Computer Science and Information Science, Srinivas University, Mangalore, India,
ORCID: 0000-0003-0392-2388; E-mail: manasa.ccis@srinivasuniversity.edu.in

[2] Professor, Institute of Computer Science & Information Science, Srinivas University, Mangalore – 575001, India,
ORCID: 0000-0002-6023-3899; Email: drjayanthila@gmail.com

ABSTRACT

Purpose: *Attempting to get access to a computer, computer network, or computing system without authorization is known as a cyber-attack. To modify, impede, erase, manipulate or steal data from computer systems is the purpose of a cyber-attack. These attacks may be carried out in a number of ways. This placeholder information is used to identify a single instance of the use of a prgramme that may support numerous users at once. A thread is information that a programme requires to serve a single user or a single service request. Cybercriminals make use of technology to do malicious actions on digital systems or networks in order to make a profit. These crimes include hacking computer systems and stealing confidential information from businesses and individuals. A thorough study on the algorithms to detect threats in the virtual world of corporate sectors.*

Finding/Result: *Researchers are using a wide array of deep learning algorithms to achieve this goal, and the results have been rather impressive. A system like this may provide substandard results because to its limited ability to describe the problem area and the complexity of its modeling of hazardous behaviours. Supervised learning systems often deliver a high level of accuracy because of the large amount of data made available by manually labelled samples.*

Originality/Value: *Antivirus software is an absolute need for any and all computers. The vast majority of antivirus software is able to identify malicious software such as malware, spyware, ransomware, and harmful email attachments.*

Paper Type: *Literature Review.*

Keywords: Cyber-attacks, Cyber-security, Fifth Generation, Machine Learning Algorithm, Security Threats, SWOC analysis.

1. INTRODUCTION :

Within an effective cyber security policy, there are several layers of defense that secure networks, computers, programmers, and other types of sensitive information [1]. For a society to have a successful defense against cyber-attacks, it is necessary for people, processes, and technology to all operate together. It is possible to automate the modifications that need to be made to certain Cisco Security products, which may speed up crucial security procedures such as discovery, inspection, and remediation. There has been a noticeable increase in the breadth as well as the quantity of cyber-attacks [2-3]. As a direct consequence of this, they have become the most significant threats to the online world [4]. In 2015, almost 98% of the online applications that were tested by Trust wave were found to be open to some kind of cyber-attack [5]. The Department of Business, Innovation, and Skills performed a survey on security in 2015 and found that 90 percent of big organizations and 74 percent of small organizations have suffered security breaches [6]. As a direct consequence of this, research into internet safety has exceeded all other fields [7]. Information stored in cyberspace has to be kept confidential while still being maintained safe and easily accessible. To guarantee the success of such a broad idea

as cyber security, coordination is required across a wide variety of different fields [8-9]. This connection between two separate domains is shown in Figure 1.

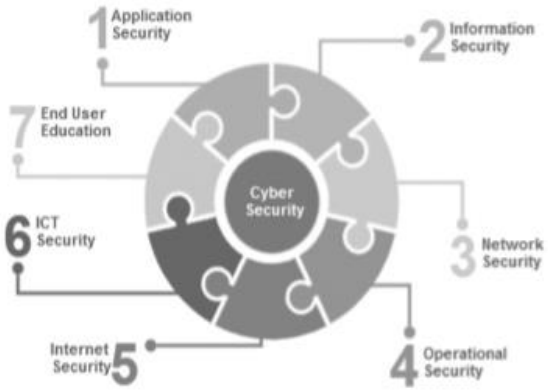

Fig. 1: Cyber security and verious Domains (Aleesa et.al) [10].

2. OBJECTIVES :

From digital assaults, digital protection guarantees the mystery of PC connected structures, programming, equipment, and information. An attacker can easily gain access to your device and misuse your personal information, client information, business intelligence, and other data if a security policy is not in place. The purpose of this analysis is to acquire a deeper comprehension of the term's "cybercrime" and "cyber security," as well as to propose efficient and appropriate strategies for dealing with these issues in the modern internet world. In order to achieve the desired outcome, the following items are necessary:

(1) To examine the most recent system for cyber-attacks and to clearly define the problem statement for the same aspect.

(2) To introduce a brand-new method for detecting cyber-attacks, with an emphasis on suspicious behavior from DDoS and ransomware attacks.

(3) To demonstrate a machine learning-based method for detecting an attack in the network;

(4) To compare the proposed system's performance metrics to those of other cutting-edge frameworks to determine its viability.

(5) To analyse the study using SWOT Analysis,

3. METHODOLGY :

The data and information used in the analysis come from a wide range of sources. The resources include cyber security-related standard reference textbooks, numerous articles, websites, and literature reviews on virtual world, cyber security, and machine learning algorithms.

3.1 Database searches: The following are a few examples of online and World Wide Web sources that are repositories of various conference publications and peer-reviewed journals.

- Google Scholar search engine
- IEEE Explorer
- Research Gate

4. RELATED RESEARCH WORK :

Identifying and avoiding Cyber-attacks in virtual world of corporate sectors. Available literature is collected using Google Scholar on the articles published between years 2018 to 2022. Keywords 'Cyber security,' cyber attacks', 'virtual world', are used to perform searches. Articles are further filtered by considering discussions about the virtual world of corporate sectors. Details of the related work are listed in Table 1.

Table 1: Review of articles related to Cyber Security Attacks Detecting Thread in Virtual world.

S. No.	Focus	Contribution	References
1	Cyber Security	In order to ensure cyber security, one must have a thorough understanding of the assaults and the capacity to identify potential dangers.	Shone, et.al. (2018). [11]
2	Deep learning and Cyber Security	The first step is to outline the basic issues of network safety and attack detection, and then we present a number of successful related applications employing deep learning structures.	Aleesa, et.al., (2020). [12]
3	Virtualization of Network infrastructures	Network infrastructures may be adapted to the individual demands of different network applications. Virtualization is widely used, however, the common usage of routing devices and communication channels raises security risks.	Sultana, et.al., (2019). [13]
4	Machine learning and Cyber Security	Based on system calls, a vector space model for the development of suggested dataset is used to examine the behavioral features. Data comparison and evaluation using Machine Learning (ML) techniques are two of the goals of this work.	Meneghello, et, al., (2019). [14]
5	Cyber Security	Modern IT companies have a significant challenge in maintaining data privacy, integrity, and accessibility. This comprehensive strategy incorporates a number of different components. This comprises activities related to cyber-security, in which a group of personnel is tasked with monitoring and safeguarding the organization from any and all types of cyber-attack.	Pearce, et.al., (2013). [15]
6	Cyber Security & policy	Every year, as attacker's efficiency and sophistication rise, cybercrime climbs dramatically. A cyber assault occurs for a variety of causes and in a variety of methods. Nevertheless, the common thread is that cybercriminals seek to exploit weaknesses in the security policies, procedures, or technology of an organization.	McKeown, et.al., (2008). [16]

7	Network Intrusion	If a business's systems or the whole organization are compromised by a security threat, it is considered a malevolent act. A data breach or network intrusion that may have occurred at a firm is referred to as a security incident. When a breach of data or a network happens, the occurrence is referred to as a "security incident."	Pan et.al., (2011). [17]
8	Network infrastructures	Additionally, virtual networks are not constrained by the real network's protocol stack, allowing for a wide range of topological options. Consequently, it is feasible to create virtual network infrastructures adapted to the individual demands of diverse network applications.	Pignolet, et al., (2015). [18]
9	Cyber Security	These preventative steps are referred to by Stallings as "security services,"	Fukushima et.al., (2013). [19]
10	Network Security	The goal of this project is to create network architectures that can withstand the failure of individual routers. Through the usage of backups, this goal is met (i.e., redundant routers and links). The physical substrate is being underutilized because of the unused resources.	Chowdhury & Boutaba, (2010). [20]
11	Deep Learning	In this study, we build a framework for deep learning by making use of BRNN-LSTM.	Wang, & Lim., (2008). [21]
12	Deep Learning	This research estimates the short-term passenger demand of an on-demand transportation service platform by evaluating the spatio-temporal correlations between trip requests and available vehicles.	Salcedo et al., (2012). [22]
13	Cyber Security	In this article, we provide the first statistical approach for carefully assessing honeypot data that was recorded during a cyber-assault.	Khali et al., (2014). [23]
14	Digital Signatures	The majority of the present detection and prevention systems depend on approaches that are based on signatures.	Goumidi et al., (2020). [24]
15	Cyber Security	We follow up on our previous work and provide a comprehensive introduction to the Cyber security Dynamics	Bhoi, & Khilar, (2014). [25]
16	Network Traffic	We introduce a unique domain-specific concurrency model in this work that tackles this problem by introducing the concept of detection scope. The detection scope is a unit for splitting network traffic such that the traffic in each resultant "slice" is independent for detection purposes.	Viriyasitavat et al., (2015). [26]

17	Cyber Threats	In this research, we provide a model for trend analysis of cyber threats that is based on the hidden Markov model (HMM). The approach incorporates extra environmental information into the trend analysis.	Jameel et.al., (2018). [27]
18	Deep learning	In this study, an original approach to the NSSA model is proposed. A multi-perspective analysis is included in the model for the assessment of the scenario.	Liu & Masouros, (2020). [28]
19	Network Security	The use of gray-box models shown by the data, is recommended by this technique.	Rappaport et al., (2021). [29]
20	Cyber Attack	In this article, we study one specific angle of the issue, namely the extreme value phenomena that is demonstrated by cyber-attack rates. This is a phenomenon that has been exhibited by cyber assault rates	Drucker, et al., (1999). [30]
21	Cyber Defence	In this essay, we look at how to evaluate and predict the effectiveness of the cyber defence technique known as early-warning. This mechanism is known to detect potential threats before they become actual threats.	Arivudainambi & Visu, (2020). [31]
22	Cyber Security	The purpose of this study is to offer an overview of the several approaches of prediction and forecasting that are employed in the field of cyber security.	Wang Liu & Feng, (2022). [32]
23	Security Breaches	The model is predicated on the concept that security breaches may be identified. This theory forms the foundation of the model.	Tang, et al., (2021). [33]
24	Network Security Detection	We present an overview of the state of the art in the field of novelty detection using statistical methods.	Staudemeyer, (2015). [34]
25	Deep learning	This is one of the first DL studies to look at spatio-temporal correlations to estimate the short-term passenger demand of an on-demand transportation service platform, and this study is one of the first DL studies to do so.	Krishnan & Raajan., (2016). [35]
26	Digital Forensics	Examines the various forensics and anti-forensics challenges, tools, methods, and types. As a new safeguard for forensics, anti-forensics would be helpful.	Yaacoub et al., (2021). [36]
27	Digital Forensics and Cyber Crime	The purpose of the proposed system is to determine the motivation, pattern, and types of cyberattacks that occurred over a given time period. System administrators are able to reduce the system's vulnerability thanks to the proposed framework.	Ikuesan, & Venter, H. S. (2019). [37]

27	Internet of Things security and forensics	IoT nodes are becoming a data mine for malicious actors as they collect and process private information. introduces major IoT security and forensics issues currently in existence.	Conti et al., (2018). [38]
28	Cyber-Attack & Digital Forensics	Made an effort to determine who was responsible and what they were planning. One of the most challenging aspects of digital forensics is determining the motivations behind cyberattacks. A model for analysing cyberattacks' intentions will be proposed.	Al-Mousa, (2021). [39]
29	Machine learning & Cyber Forensics	Investigate the potential uses of machine learning (ML) in cyber forensics. Talk about the various research problems whose solutions will help make better predictions for cyber forensics.	Rajendiran, et al., (2021).[40]
30	Artificial Intelligence and Digital Forensics	Propose an AI-based framework that performs the majority of routine tasks with trained intelligence and requires little user input	Parag, et al., (2016). [41]

5. PRESENT STATUS OF VIRTUAL WORLD OF CORPERATE SECTOR :

- A new online space that is both functional and interactive has emerged by combining artificial intelligence with virtual and augmented reality (VR/AR), supported by its own distinct economy. Avatars are created and powered by devices and headsets to enable human participation.
- The possibility of complete online immersion has never been closer, despite the fact that the majority of these devices require additional fine-tuning by their manufacturers. We might all see our avatars roaming virtual worlds and gaining access to entertainment and information in a novel way in just a few years.

6. DESIRED STATUS AND IMPROVEMENTS REQUIRED :

- In today's market, applications that go beyond tourism, marketing, or leisure and are less expensive for users are in high demand. Additionally, virtual interfaces must be improved to avoid clipping, which gives the impression that some solid objects can pass through them. or to lessen the negative effects that virtual reality has on people, such as motion sickness, which is a feeling of fainting brought on by a mismatch between how our bodies move and what we see in the virtual world [42].
- Major technology companies are developing headsets that can view high-definition images without the use of cables at the moment. They are developing virtual reality headsets with significantly increased power and resolution of 8K. Even the incorporation of AI into the future is under consideration [42].
- The most recent 5G standard might also provide VR with some extremely intriguing scenarios. More devices and large user communities will be able to connect with this standard. Customers will also be able to receive images in real-time, almost like they were seeing them in person, due to its almost imperceptible latency [43].

7. IDEA BEHIND IMPLEMENTATION OF A CYBER ATTACK DETECTION IN VIRTUAL WORLD :

As there are more digital operations and a more complicated threat landscape, it is becoming harder to prioritize threats and respond to them [43]. Through digital transformation, an event's effects extend to third parties and the cloud. Consequently, integrated hazard control must be incorporated into the mitigation strategy for threat identification and integration [43]. Machine learning algorithms establish baseline norms and learn about their environment before taking unusual actions that may suggest a compromise. In any case, if the cyber-attack is continually rethinking itself to meet business deftness

needs and the unique climate misses the mark on the predictable pattern, the arrangement of rules will not be able to lay out what is ordinary and will raise warnings for apparently guiltless ways of behaving [44-45]. The "unthinkable" number of signs that ml-location programming generates daily is the most common study of it [46-47]. Examiners reject administration assault as a result. A genuine alert will fill a security analyst's queue, but a black box will only leave a ticket that says "alert" when it arrives. The class and sample weighted C-support vector machine (CSWC-SVM) algorithm was first proposed to safeguard industrial safety, enhance the operational stability of the industrial control system, implement response measures in the event that the network environment is attacked from the outside, and simulate in a virtual reality environment [49-52]. After that, an analyst will have to sort through logs and activities to determine what caused the change [48]. The interruption recognition model for the contemporary control network is then constructed using the CSWC-SVM calculation [53].

The disruption of essential services caused by distributed denial of service (DDoS) attacks is one of the most dangerous threats to the modern Internet [54]. The combination of assault strategies and the amount of live traffic to be examined is the test for DDoS discovery [55-57]. Lucid is a compact deep learning DDoS detection system that employs Convolutional Neural Network features [58-59].

(1) A novel approach to detecting DDoS traffic made use of a CNN with low processing overhead [60].
(2) A pre-processing technique for online attack detection that generates traffic observations without regard to the dataset [61].
(3) An activation analysis to provide an explanation for Lucid's DDoS classification [62].
(4) The solution's empirical validation on a hardware platform with limited resources [63].

Manufacturing businesses have been confronted with a number of obstacles over the past few years, including fluctuating demand and shifting requirements from suppliers and customers, necessitating new technological roadmaps and manufacturing system interventions [64-66]. Information processes aimed at workers are supported by cutting-edge technologies [67]. As a result, augmented and virtual reality (A/V) can be utilized for workforce training; they ought to communicate effectively with a human workforce [68-70]. In 2016, one of the largest known distributed denials of service (DDoS) attacks took place [71]. Non-authorized remote access to Internet of Things (IoT) devices was made possible by security flaws [72]. As a result, a botnet, or Mirai, has been installed on a lot of IoT devices by unknown attackers. These devices were located in distinct network domains separated by distance. The compromised IoT devices then simultaneously generated a significant amount of traffic through the botnet toward particular Internet Servers at a particular point in time, utilizing their resources [73-75]. Because of this, it was challenging to eliminate each attack source, resulting in the services that those servers typically provided being unavailable for several hours [76].

8. RESEARCH GAP :

Researchers in this field have been using a variety of approaches to help them better protect the nation's vital infrastructure by spotting and fixing flaws. As a result of ongoing research, we have discovered an effective way for finding vulnerabilities and implementing evaluation procedures to protect SCADA systems [77-79]. In order to assist vendors, utilities, and others in assessing and improving security measures on their own SCADA systems, this evaluation methodology was developed based on lessons acquired from evaluating vendor systems. Additional equipment is required to ensure that the examination is completed without interruption [80-83].

Research Gap 1: It is essential that an assault machine with all the necessary instruments be accessible for this task. Having access to the Internet for research in the testing area also helps to speed up the process. Using the Metasploit Framework, you may create, test, and use exploit code. For penetration testing, exploit creation, and vulnerability research it is a powerful tool.

Research Gap 2: Any fully discriminating statistical method must accurately describe the baseline network behaviour due to the dynamic nature of today's networks. Person behaviour modelling techniques are a problem in almost every job. Data mining on internet server logs to imitate real-world surfing habits takes a long time and is easy to make mistakes.

Research gap 3: The public of the available responses has no educational value because they are aware of how to detect DDOS attacks with a high detection rate or a low false alarm rate. Only a few of these have been put into action in real time.

9. RESEARCH AGENDA :

- What is the importance of virtual world in corporate sectors?
- What is the role and importance cyber security in virtual world?
- Implementing different machine learning algorithms to protect virtual world from cyber threats.

10. ANALYSIS OF RESEARCH AGENDA :

- Analyzing the importance of virtual world in corporate sectors. With the availability of low-cost, user-friendly headsets, virtual reality has recently entered the mainstream.
- Cyber security importance in virtual world. Research by McAfee discovered that 81% of global organisations experienced increased cyber threats during the Covid-19 pandemic
- Given the possibilities it opens up for liberating our minds from the physical constraints of our bodies and enabling us to "see" into places that are only accessible online, this is not surprising.

11. RESEARCH PROPOSAL :

For the categorization of attacks, use RNNs in a saw y self-enlightenment-based Intrusion Detection System. Although they were able to filter out attacks, their suggested intrusion detection system was unable to identify false positives throughout the tests [85-87]. When compared to the baseline approaches, their suggested method is more accurate and efficient in terms of metrics such as classification accuracy and time. RNN for intrusion detection, a method they call RNN-IDS. To put it another way, the hidden units in an RNN model may be seen as storage units to store end-to-end and valuable information for classification, with information flowing in just one direction from the visible units to their respective hidden counterparts. Using the NSL-KDD dataset, they evaluated whether characteristics such as the number of neurons had an influence on the RNN-IDS. RNN-IDS outperforms prior approaches like ANN, random forest, and SVM in terms of classification accuracy [88-90].

12. SWOC ANALYSIS :

SWOC means Strength, Weakness, Opportunities, and Challenges. It is commonly used to assess the internal capacities of organizations. SWOC analysis is used in scientific papers to comprehend internal organizational analysis, ABCD analysis as a Conceptual framework, and PESTLE analysis as outside institutionalism [91-93]. The SWOC analysis of AWS is discussed below.

Strengths:

- A tool for security investment planning: It can be used as a planning tool to make sure that the security budget goes to the most important thing [94].
- Performance administration: The incorporation of performance management to evaluate and enhance the standard impact [95].
- Enhances security: enhanced security in comparison to the less stringent baseline security [96].

Weakness:

- An inadequate information security system for employees who work from home [97]
- Creating marketing and product development strategies with a focus on customers in mind [97]
- The strengths and threats box or the opportunities and weaknesses box should be the sole focus of cyber security [98].

Opportunities:

- The growing significance of digital files, as well as modernization and organizational growth [99].
- Projection of interfaces that are more user-friendly and efficient.
- Constructing security protocols that are better and more efficient [100].

Challenges

- To ensure Enterprise – IT Architecture have security embedded.
- Fraudulent intrusion (hackers, computer criminals, fired employees [100].

- Cyber security technology changing too fast [101].

13. EXPECTED OUTCOME OF THE PROPOSED STUDY :

We talk about a few different ways to communicate information about an observed network in a Virtual World (VW). These are intended to demonstrate the breadth and capabilities of VWs, avatars of VWs, and objects for communicating with humans. MATLAB will be used to test and simulate the proposed model, which is based on cyberattacks and uses machine learning techniques. The proposed model would be compared to other cutting-edge models in terms of accuracy, recall, precision, false alarm rate, and F1 score measure, which weights precision and recall equally as the variant most often used when learning from imbalanced data among other metrics.

14. SUGGESTION :

- **Use strong passwords**: hackers can easily get into your account without your permission. By using a strong and unique password for each account, you should make your system and other accounts more secure. To safeguard your passwords, you can also make use of password management applications.
- **Never share your passwords** Share your password with no one, no matter how close you are to them or how urgent your task is. Cybercriminals can gain access to all of your sensitive information if you share your password with them.
- **Change your passwords frequently** It's understandable if it's hard to remember the most recent passwords, but it's better to change them on a regular basis than to be the target of cyberattacks.
- **Update software** Your anti-virus software should be kept up to date on a regular basis to ensure that it is ready to defend your system against the most recent cyberattacks. It is highly recommended that you never snooze or miss these updates.
- **Check emails thoroughly** One of the most serious cyberattacks, email spoofing is difficult to spot. In order to give the impression that an email is coming from a reputable source, cybercriminals alter the header of the message they send.

15. CONCLUSION :

Our strategy's capacity to convey a large amount of information is its primary advantage over other methods. The amount of data that can fit in a particular flat diagram or spreadsheet layout in a virtual world is not a constraint. With Immersively, multiple, simultaneous, and more natural channels can be used to convey information. The fact that data in a virtual world is presented in a format with which humans are more familiar and able to interpret is a secondary benefit. We aim to adapt the tool to the analyst's language rather than adapting to the tool's language. In the future, the study may include a few more advanced neural networks and a focus on particular kinds of rational attacks.

REFERENCES :

[1] Casey, P., Baggili, I., & Yarramreddy, A. (2019). Immersive virtual reality attacks and the human joystick. *IEEE Transactions on Dependable and Secure Computing*, *18*(2), 550-562. Google Scholar↗ Cross Ref/DOI↗

[2] Imperatori, C., Dakanalis, A., Farina, B., Pallavicini, F., Colmegna, F., Mantovani, F., & Clerici, M. (2020).Global storm of stress-related psychopathological symptoms: a brief overview on the usefulness of virtual reality in facing the mental health impact of COVID-19. *Cyberpsychology, Behavior, and Social Networking*, *23*(11), 782-788. Google Scholar↗ Cross Ref/DOI↗

[3] Alzahrani, S., & Hong, L. (2018). Generation of DDoS attack dataset for effective IDS development and evalation. *Journal of Information Security*, *9*(4), 225-241. Google Scholar↗ Cross Ref/DOI↗

[4] Rawashdeh, A., Alkasassbeh, M., & Al-Hawawreh, M. (2018). An anomaly-based approach for DDoS attack detection in cloud environment. *International Journal of Computer Applications in Technology*, *57*(4), 312-324. Google Scholar↗ Cross Ref/DOI↗

[5] Liu11, X., Sohn, Y. H., & Park, D. W. (2018). Application development with augmented reality technique using Unity 3D and Vuforia. *International Journal of Applied Engineering Research*, *13*(21), 15068-15071. . Google Scholar↗ Cross Ref/DOI↗

[6] Roopak, M., Tian, G. Y., & Chambers, J. (2020). Multi-objective-based feature selection for DDoS attack detection in IoT networks. *IET Networks*, *9*(3), 120-127. . Google Scholar↗ Cross Ref/DOI↗

[7] Mayne, R., & Green, H. (2020). Virtual reality for teaching and learning in crime scene investigation. *Science & Justice*, *60*(5), 466-472. . Google Scholar↗ Cross Ref/DOI↗

[8] Ahir, K., Govani, K., Gajera, R., & Shah, M. (2020). Application on virtual reality for enhanced education learning, military training and sports. *Augmented Human Research*, *5*(1), 1-9. Google Scholar↗ Cross Ref/DOI↗

[9] Ahmed, M. E., Ullah, S., & Kim, H. (2018). Statistical application fingerprinting for DDoS attack mitigation. *IEEE Transactions on Information Forensics and Security*, *14*(6), 1471-1484. Google Scholar↗ Cross Ref/DOI↗

[10] Rosin, F., Forget, P., Lamouri, S., & Pellerin, R. (2020). Impacts of Industry 4.0 technologies on Lean Principles. *International Journal of Production Research*, *58*(6), 1644-1661. Google Scholar↗ Cross Ref/DOI↗

[11] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion Detection. *IEEE transactions on emerging topics in computational intelligence*, *2*(1), 41-50Google Scholar↗ Cross Ref/DOI↗

[12] Aleesa, A. M., Zaidan, B. B., Zaidan, A. A., & Sahar, N. M. (2020). Review of intrusion detection systems based on deep learning techniques: coherent taxonomy, challenges, motivations, recommendations, substantial analysis and future directions. *Neural Computing and Applications*, *32*(14), 9827-9858. Google Scholar↗ Cross Ref/DOI↗

[13] Sultana, N., Chilamkurti, N., Peng, W., & Alhadad, R. (2019). Survey on SDN based network intrusion detection system using machine learning approaches. *Peer-to-Peer Networking and Applications*, *12*(2), 493-501. Google Scholar↗ Cross Ref/DOI↗

[14] Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019). IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet of Things Journal*, *6*(5), 8182-8201. Google Scholar↗ Cross Ref/DOI↗

[15] Pearce, M., Zeadally, S., & Hunt, R. (2013). Virtualization: Issues, security threats, and solutions. *ACM Computing Surveys (CSUR)*, *45*(2), 1-39. Google Scholar↗ Cross Ref/DOI↗

[16] McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., & Turner, J. (2008). OpenFlow: enabling innovation in campus networks. *ACM SIGCOMM computer communication review*, *38*(2), 69-74. Google Scholar↗ Cross Ref/DOI↗

[17] Pan, J., Paul, S., & Jain, R. (2011). A survey of the research on future internet architectures. *IEEE Communications Magazine*, *49*(7), 26-36. Google Scholar↗ Cross Ref/DOI↗

[18] Pignolet, Y. A., Schmid, S., & Tredan, G. (2015). Adversarial topology discovery in network Virtualization environments: a threat for ISPs? *Distributed Computing*, *28*(2), 91-109. Google Scholar↗ Cross Ref/DOI↗

[19] Fukushima, M., Sugiyama, K., Hasegawa, T., Hasegawa, T., & Nakao, A. (2013). Minimum Disclosure routing for network virtualization and its experimental evaluation. *IEEE/ACM Transactions on Networking*, *21*(6), 1839-1851. Google Scholar↗ Cross Ref/DOI↗

[20] Chowdhury, N. M. K., & Boutaba, R. (2010). A survey of network virtualization. *Computer Networks*, *54*(5), 862-876. Google Scholar↗ Cross Ref/DOI↗

[21] Wang, X., & Lim, A. O. (2008). IEEE 802.11 s wireless mesh networks: Framework and challenges. *Ad Hoc Networks*, *6*(6), 970-984. Google Scholar↗ Cross Ref/DOI↗

[22] Salcedo, O., Pedraza, L. F., & Espinosa, M. (2012). Evaluación de redes MPLS/VPN/BGP con rutas reflejadas. *Tecnura*, *16*(32), 108-117. Google Scholar↗ Cross Ref/DOI↗

[23] Khalil, I. M., Khreishah, A., & Azeem, M. (2014). Cloud computing security: A survey. *Computers*, *3*(1), 1-35. Google Scholar↗ Cross Ref/DOI↗

[24] Goumidi, H., Aliouat, Z., & Harous, S. (2020). Vehicular cloud computing security: A survey. *Arabian Journal for Science and Engineering*, *45*(4), 2473-2499. Google Scholar↗ Cross Ref/DOI↗

[25] Bhoi, S. K., & Khilar, P. M. (2014). Vehicular communication: a survey. *IET networks*, *3*(3), 204-217. Google Scholar↗ Cross Ref/DOI↗

[26] Viriyasitavat, W., Boban, M., Tsai, H. M., & Vasilakos, A. (2015). Vehicular communications: Survey and challenges of channel and propagation models. *IEEE Vehicular Technology Magazine*, *10*(2), 55-66. Google Scholar↗ Cross Ref/DOI↗

[27] Jameel, F., Wyne, S., Nawaz, S. J., & Chang, Z. (2018). Propagation channels for mmWave vehicular communications: State-of-the-art and future research directions. *IEEE Wireless Communications*, *26*(1), 144-150. Google Scholar↗ CrossRef/DOI↗

[28] Liu, F., & Masouros, C. (2020). A tutorial on joint radar and communication transmission for vehicular networks—Part II: State of the art and challenges ahead. *IEEE Communications Letters*, *25*(2), 327-331. Google Scholar↗ Cross Ref/DOI↗

[29] Rappaport, T. S., Murdock, J. N., & Gutierrez, F. (2011). State of the art in 60-GHz integrated circuits and systems for wireless communications. *Proceedings of the IEEE*, *99*(8), 1390-1436. Google Scholar↗ CrossRef/DOI↗

[30] Drucker, H., Wu, D., & Vapnik, V. N. (1999). Support vector machines for spam categorization. *IEEE Transactions on Neural networks*, *10*(5), 1048-1054. Google Scholar↗ Cross Ref/DOI↗

[31] Arivudainambi, D., KA, V. K., & Visu, P. (2020). Ransomware Traffic Classification Using Deep Learning Models: Ransomware Traffic Classification. *International Journal of Web Portals (IJWP)*, *12*(1), 1-11.Google Scholar↗ Cross Ref/DOI↗

[32] Wang, J., Liu, Y., & Feng, H. (2022). IFACNN: efficient DDoS attack detection based on improved firefly alg orithm to optimize convolutional neural networks. *Mathematical Biosciences and Engineering*, *19*(2), 1280-1303. Google Scholar↗ Cross Ref/DOI↗

[33] Tang, D., Tang, L., Shi, W., Zhan, S., & Yang, Q. (2021). MF-CNN: a new approach for LDoS attack detection based on multi-feature fusion and CNN. *Mobile Networks and Applications*, *26*(4), 1705-1722. Google Scholar↗ Cross Ref/DOI↗

[34] Staudemeyer, R. C. (2015). Applying long short-term memory recurrent neural networks to intrusion detection. *South African Computer Journal*, *56*(1), 136-154. Google Scholar↗ Cross Ref/DOI↗

[35] Krishnan, R. B., & Raajan, N. R. (2016). An intellectual intrusion detection system model for attacks classification using RNN. *Int. J. Pharm. Technol*, *8*(4), 23157-23164. Google Scholar↗

[36] Tymoshenko, Y. P., Kozachenko, O. I., Kyslenko, D. P., Horodetska, M. S., Chubata, M. V., & Barhan, S. S. (2022). Latest technologies in criminal investigation (testing of foreign practices in Ukraine). *Amazonia Investiga*, *11*(51), 149-160. Google Scholar↗ Cross Ref/DOI↗

[37] Ikuesan, A. R., & Venter, H. S. (2019). Digital behavioral-fingerprint for user attribution in digital forensics: Are we there yet?. *Digital Investigation*, *30(1)*, 73-89. Google Scholar↗ Cross Ref/DOI↗

[38] Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, *22*(2), 1191-1221. Google Scholar↗ Cross Ref/DOI↗

[39] Frantzeskou, G., Stamatatos, E., Gritzalis, S., Chaski, C. E., & Howald, B. S. (2007). Identifying authorship by byte-level n-grams: The source code author profile (scap) method. *International Journal of Digital Evidence*, *6*(1), 1-18. Google Scholar↗ Cross Ref/DOI↗

[40] Rosenberg, I., Shabtai, A., Elovici, Y., & Rokach, L. (2021). Adversarial machine learning attacks and defense methods in the cyber security domain. *ACM Computing Surveys (CSUR)*, *54*(5), 1-36. Google Scholar↗ Cross Ref/DOI↗

[41] Chhabra, G. S., Singh, V. P., & Singh, M. (2020). Cyber forensics framework for big data analytics in IoT environment using machine learning. *Multimedia Tools and Applications*, *79*(23), 15881-15900. Google Scholar↗ Cross Ref/DOI↗

[42] Morovati, K., & Kadam, S. S. (2019). Detection of Phishing Emails with Email Forensic Analysis and Machine Learning Techniques. *International Journal of Cyber-Security and Digital Forensics*, *8*(2), 98-108. Google Scholar↗ Cross Ref/DOI↗

[43] Rigby, M., & Winter, S., (2015). Enhancing launch pads for decision-making in intelligent mobility on-de ma *Journal of Location Based Services*, *9*(2), 77-92. Google Scholar↗ Cross Ref/DOI↗

[44] Dandl, F., Hyland, M., Bogenberger, K., & Mahmassani, H. S. (2019). Evaluating the impact of spatio-temporal demand forecast aggregation on the operational performance of shared autonomous mobility fleets. *Transportation*, *46*(6), 1975-1996. Google Scholar ↗ Cross Ref/DOI↗

[45] Selvapandian, D., & Santhosh, R. (2021). Deep learning approach for intrusion detection in IoT-multi cloud environment. *Automated Software Engineering*, *28*(2), 1-17.Google Scholar↗ Cross Ref/DOI↗

[46] Rao, R. S., & Pais, A. R. (2019). Detection of phishing websites using an efficient feature-based machine learning framework. *Neural Computing and Applications*, *31*(8), 3851-3873.Google Scholar↗ Cross Ref/DOI↗

[47] Jain, A. K., & Gupta, B. B. (2018). Towards detection of phishing websites on client-side using machine learning based approach. *Telecommunication Systems*, *68*(4), 687-700.Google Scholar↗ Cross Ref/DOI↗

[48] Albadra, M. A. A., & Tiuna, S. (2017). Extreme learning machine: a review. *International Journal of Applied Engineering Research*, *12*(14), 4610-4623.Google Scholar↗ Cross Ref/DOI↗

[49] Xu, X., Zhang, X., Gao, H., Xue, Y., Qi, L., & Dou, W. (2019). BeCome: Blockchain-enabled computation offloading for IoT in mobile edge computing. *IEEE Transactions on Industrial Informatics*, *16*(6), 4187-4195. Google Scholar↗ Cross Ref/DOI↗

[50] Xu, X., Mo, R., Dai, F., Lin, W., Wan, S., & Dou, W. (2019). Dynamic resource provisioning with fault tolerance for data-intensive meteorological workflows in cloud. *IEEE Transactions on Industrial Informatics*, *16*(9), 6172-6181.Google Scholar↗ Cross Ref/DOI↗

[51] Zhan, Z., Xu, M., & Xu, S. (2013). Characterizing honeypot-captured cyber-attacks: Statistical framework and case study. *IEEE Transactions on Information Forensics and Security*, *8*(11), 1775-1789. Google Scholar ↗ Cross Ref/DOI↗

[52] Baheti, R., & Gill, H. (2011). Cyber-physical systems. *The impact of control technology*, *12*(1), 161-166. Google Scholar↗

[53] Herley, C., & Van Oorschot, P. C. (2018). Science of security: Combining theory and measurement to reflect the observable. *IEEE Security & Privacy*, *16*(1), 12-22.Google Scholar↗ Cross Ref/DOI ↗

[54] Xu, S., Yung, M., & Wang, J. (2021). Seeking foundations for the science of cyber security. *Information Systems Frontiers*, *23*(2), 263-267.Google Scholar↗ Cross Ref/DOI↗

[55] Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & security*, *31*(4), 597-611.Google Scholar↗ Cross Ref/DOI↗

[56] Gulliver, T. A., & Li, K. F. (2009). Guest editorial: Special issue on the 2009 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing. *Canadian Journal of Electrical and Computer Engineering*, *34*(4), 134-135. Google Scholar↗ Cross Ref/DOI↗

[57] Zhan, Z., Xu, M., & Xu, S. (2015). Predicting cyber-attack rates with extreme values. *IEEE Transactions on Information Forensics and Security*, *10*(8), 1666-1677. Google Scholar↗ Cross Ref/DOI↗

[58] Zhao, Y., Liang, X., Fan, X., Wang, Y., Yang, M., & Zhou, F. (2014). MVSec: multi-perspective and deductive visual analytics on heterogeneous network security data. *Journal of Visualization*, *17*(3), 181-196. Google Scholar↗ Cross Ref/DOI↗

[59] Xu, M., Schweitzer, K. M., Bateman, R. M., & Xu, S. (2018). Modeling and predicting cyber hacking breaches. *IEEE Transactions on Information Forensics and Security*, *13*(11), 2856-2871. Google Scholar↗ Cross Ref/DOI↗

[60] Peng, C., Xu, M., Xu, S., & Hu, T. (2017). Modeling and predicting extreme cyber attack rates via marked point processes. *Journal of Applied Statistics*, *44*(14), 2534-2563.Google Scholar↗ Cross Ref/DOI↗

[61] Xu, M., Hua, L., & Xu, S. (2017). A vine copula model for predicting the effectiveness of cyber defense early-warning. *Technometrics*, *59*(4), 508-520. Google Scholar↗ Cross Ref/DOI↗

[62] Peng, C., Xu, M., Xu, S., & Hu, T. (2018). Modeling multivariate cybersecurity risks. *Journal of Applied Statistics*, *45*(15), 2718-2740.Google Scholar↗ Cross Ref/DOI↗

[63] Husák, M., Komárková, J., Bou-Harb, E., & Čeleda, P. (2018). Survey of attack projection, prediction, and forecasting in cyber security. *IEEE Communications Surveys & Tutorials*, *21*(1), 640-660. Google Scholar ↗ Cross Ref/DOI↗

[64] Leevy, J. L., & Khoshgoftaar, T. M. (2020). A survey and analysis of intrusion detection models based on cse-cic-ids2018 big data. *Journal of Big Data*, *7*(1), 1-19.Google Scholar↗ CrossRef/DOI↗

[65] Markou, M., & Singh, S. (2003). Novelty detection: a review—part 1: statistical approaches. *Signal processing*, *83*(12), 2481-2497.Google Scholar ↗ Cross Ref/DOI↗

[66] He, S., & Shin, K. G. (2019). Spatio-temporal adaptive pricing for balancing mobility-on-demand networks. *ACM Transactions on Intelligent Systems and Technology (TIST)*, *10*(4), 1-28. Google Scholar ↗ Cross Ref/DOI↗

[67] Walraven, S., Truyen, E., & Joosen, W. (2014). Comparing PaaS offerings in light of SaaS development. *Computing*, *96*(8), 669-724. Google Scholar ↗ Cross Ref/DOI↗

[68] Han, Y. (2011). Cloud computing: case studies and total cost of ownership. *Information technology and libraries*, *30*(4), 198-206. Google Scholar ↗ Cross Ref/DOI↗

[69] Holla, R. (2017). A Study on SWOC Analysis of Reliance Jio. *International Journal of Engineering Research and Modern Education (IJERME)*, *2*(1), 42-47. Google Scholar ↗ Cross Ref/DOI↗

[70] Beno, M. M., I. R, V., S. M, S., & Rajakumar, B. R. (2014). Threshold prediction for segmenting tumors from brain MRI scans. *International Journal of Imaging Systems and Technology*, *24*(2), 129-137. Google Scholar ↗ Cross Ref/DOI↗

[71] Karie, N. M., Kebande, V. R., & Venter, H. S. (2019). Diverging deep learning cognitive computing techniques into cyber forensics. *Forensic Science International: Synergy*, *1*(1), 61-67. Google Scholar↗ Cross Ref/DOI↗

[72] Wu, Z., Chen, S., Rincon, D., & Christofides, P. D. (2020). Post-cyber-attack state reconstruction for nonlinear processes using machine learning. *Chemical Engineering Research and Design*, *159*(1), 248-261. Google Scholar ↗ Cross Ref/DOI↗

[73] Wang, H., Ruan, J., Wang, G., Zhou, B., Liu, Y., Fu, X., & Peng, J. (2018). Deep learning-based interval state estimation of AC smart grids against sparse cyber-attacks. *IEEE Transactions on Industrial Informatics*, *14*(11), 4766-4778. Google Scholar ↗ Cross Ref/DOI↗

[74] Wang, D., Wang, X., Zhang, Y., & Jin, L. (2019). Detection of power grid disturbances and cyber-attacks based on machine learning. *Journal of information security and applications*, *46*(1), 42-52. Google Scholar ↗ Cross Ref/DOI↗

[75] Perez-Diaz, J. A., Valdovinos, I. A., Choo, K. K. R., & Zhu, D. (2020). Flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning. *IEEE Access*, *8*(2), 155859-155872. Google Scholar ↗ Cross Ref/DOI↗

[76] Wei, F., Wen, Z., & He, H. (2019). Cyber-attack recovery strategy for smart grid based on deep reinforcement learning. *IEEE Transactions on Smart Grid*, *11*(3), 2476-2486. Google Scholar ↗ Cross Ref/DOI↗

[77] Ismail, M., Shaaban, M. F., Naidu, M., & Serpedin, E. (2020). Deep learning detection of electricity theft cyber-attacks in renewable distributed generation. *IEEE Transactions on Smart Grid*, *11*(4), 3428-3437. Google Scholar ↗ Cross Ref/DOI↗

[78] Behal, S., Kumar, K., & Sachdeva, M. (2017). Characterizing DDoS attacks and flash events: Review, research gaps, and future directions. *Computer Science Review*, *25*(1), 101-114. Google Scholar ↗ Cross Ref/DOI↗

[79] Singh, R., Kumar, H., Singla, R. K., & Ketti, R. R. (2017). Internet attacks and intrusion detection system: A review of the literature. *Online Information Review*, *41*(2), 171-184. Google Scholar ↗ Cross Ref/DOI↗

[80] Jiang, K., Wang, W., Wang, A., & Wu, H. (2020). Network intrusion detection combined hybrid sampling with the deep hierarchical network. *IEEE Access*, *8*(1), 32464-32476. Google Scholar ↗ Cross Ref/DOI↗

[81] Samy, A., Yu, H., & Zhang, H. (2020). Fog-based attack detection framework for the internet of things using deep learning. *IEEE Access*, *8*(1), 74571-74585. Google Scholar ↗ Cross Ref/DOI↗

[82] Subroto, A., & Apriyana, A. (2019). Cyber risk prediction through social media big data analytics and statistical machine learning. *Journal of Big Data*, *6*(1), 1-19. Google Scholar ↗ CrosRef/DOI↗

[83] Ramotsoela, D. T., Hancke, G. P., & Abu-Mahfouz, A. M. (2019). Attack detection in water distribution systems using machine learning. Human-centric *Computing and Information Sciences*, *9*(1), 1-22. Google Scholar ↗ Cross Ref/DOI↗

[84] Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H. & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. *IEEE Access*, *6*(1), 35365-35381.Google Scholar ↗ Cross Ref/DOI↗

[85] Kanimozhi, V., & Jacob, T. P. (2021). Artificial Intelligence outflanks all other machine learning classifiers in Network Intrusion Detection System on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. *ICT Express*, *7*(3), 366-370. Google Scholar ↗ Cross Ref/DOI↗

[86] Hussain, B., Du, Q., Sun, B., & Han, Z. (2020). Deep learning-based DDoS-attack detection for the cyber-physical system over 5G network. *IEEE Transactions on Industrial Informatics*, *17*(2), 860-870. Google Scholar ↗ Cross Ref/DOI↗

[87] Aamir, M., & Zaidi, S. M. A. (2021). Clustering-based semi-supervised machine learning for DDoS attack classification. *Journal of King Saud University-Computer and Information Sciences*, *33*(4), 436-446. Google Scholar ↗ Cross Ref/DOI↗

[88] Al-Abassi, A., Karimipour, H., Dehghantanha, A., & Parizi, R. M. (2020). An ensemble deep learning-based cyber-attack detection in the industrial control system. *IEEE Access*, *8*(1), 83965-83973. Google Scholar ↗ Cross Ref/DOI↗

[89] Saharkhizan, M., Azmoodeh, A., Dehghantanha, A., Choo, K. K. R., & Parizi, R. M. (2020). An ensemble of deep recurrent neural networks for detecting IoT cyberattacks using network traffic. *IEEE Internet of Things Journal*, *7*(9), 8852-8859. Google Scholar ↗ Cross Ref/DOI↗

[90] Pan, Y., Sun, F., Teng, Z., White, J., Schmidt, D. C., Staples, J., & Krause, L. (2019). Detecting web attacks with end-to-end deep learning. *Journal of Internet Services and Applications*, *10*(1), 1-22. Google Scholar ↗ Cross Ref/DOI↗

[91] Benzaghta, M. A., Elwalda, A., Mousa, M. M., Erkan, I., & Rahman, M. (2021). SWOT analysis applications: An integrative literature review. *Journal of Global Business Insights*, *6*(1), 55-73. Google Scholar ↗ Cross Ref/DOI↗

[92] David, F. R., Creek, S. A., & David, F. R. (2019). What is the key to effective SWOT analysis, including AQCD factors. *SAM Advanced Management Journal*, *84*(1), 25-35. Google Scholar ↗ CrosRef/DOI↗

[93] Aithal, P. S. (2017). An effective method of developing business case studies based on company analysis. *International Journal of Engineering Research and Modern Education* (IJERME), *2*(1), 16- 27. Google Scholar ↗ Cross Ref/DOI↗

[94] Vlados, C., & Chatzinikolaou, D. (2019). Towards a restructuration of the conventional SWOT analysis. *Business and Management Studies*, *5*(2), 76-84. Google Scholar ↗ Cross Ref/DOI↗

[95] Ibor, A. E., Oladeji, F. A., Okunoye, O. B., & Ekabua, O. O. (2020). The conceptualization of Cyberattack prediction with deep learning. *Cybersecurity*, *3*(1), 1-14. Google Scholar ↗ Cross Ref/DOI↗

[96] Ibor, A. E., Oladeji, F. A., Okunoye, O. B., & Uwadia, C. O. (2022). Novel adaptive cyberattack pre-diction model using an enhanced genetic algorithm and deep learning (AdacDeep). *Information Security Journal: AGlobal Perspective*, *31*(1), 105-124.Google Scholar ↗ Cross Ref/DOI↗

[97] Zhang, J., Pan, L., Han, Q. L., Chen, C., Wen, S., & Xiang, Y. (2021). Deep learning-based attack detection for cyber-physical system cybersecurity: A survey. *IEEE/CAA Journal ofAutomatica Sinica*, *9*(3), 377-391. Google Scholar ↗ Cross Ref/DOI↗

[98] Karie, N. M., Kebande, V. R., & Venter, H. S. (2019). Diverging deep learning cognitive computing techniques into cyber forensics. Forensic Science International: *Synergy*, *1*(1), 61-67. Google Scholar ↗ Cross Ref/DOI↗

[99] Wu, Z., Chen,S., Rincon, D., & Christofides, P. D. (2020). Post-cyber-attack state reconstruction for nonlinear processes using machine learning. *Chemical Engineering Research and Design*, *159*(1), 248-261. Google Scholar ↗ Cross Ref/DOI↗

[100] Padmajothi, V., & Iqbal, J. L. (2022). Review of machine learning and deep learning mechanism in cyber- physical system. *International Journal of Nonlinear Analysis and Applications*, *13*(1), 583-590. Google Scholar ↗ Cross Ref/DOI↗

[101] Yan, W., Mestha, L. K., & Abbaszadeh, M. (2019). Attack detection for securing cyber physical systems. *IEEE Internet of Things Journal*, *6*(5), 8471-8481. Google Scholar ↗ Cross Ref/DOI↗

******