Sindh Journal of Headways in Software Volume 2, Issue 1
Published Online 07-10-2023.

Cyber Security Approaches and Trends in Internet of Things: Systematic Literature Review and Unwrapped Issues

Ali Aizaz, Aurangzaib Ali
Sukkur Institute of Business Administration/Computer system, Sukkur, 65200, Pakistan
Email:aliaizazshaikh94@gmail.com, aurangzeb5707@gmail.com

Received: 22 May, 2023; Accepted: 14th Aug, 2023; Published: 07th October 2023

Abstract*:* Currently, the revolution in Internet of Things (IoT) has immensely been witnessed since the last decade. Internet of things is based on diverse devices that consist on sensors, actuators, devices, and other technologies. The goal is to use the internet to connect and share data with other devices and systems. Internet of Things and Cyber Security are the fastest growing buzzwords that have a deeprelation to each other. The revolution in IoT enhances cybercrimes which maliciously affect critical and confidential information.Therefore, there is a dire need for essential cybersecurity approaches and algorithms to secure the exchange of data between IoT devices over the internet. In this paper, we have conducted a systematic literature review of current trends and approaches that are essential for securing IoT. Furthermore, we have founded widely popular cybercrimes that distort the performance of IoT such as; Denial of service attacks, routing attacks, viruses, malicious open-source software, external interruption, malicious code injection, and email fraud. In addition to this, we have presented existing effective solutions and recommendations for effective Cybersecurity in IoT including; Ghost European framework, Block chain technology, layers-based security, societal model, secure authentication, and various machine learning algorithms. Finally, we have also addressed some unwrapped issues for future scholars and this SLR will play an essential role for the researchers who engage in the research of IoT and Cybersecurity

Index Terms: Internet of Things, Cyber Security, Cyber-attacks, Cyber Policies, diversities, frameworks, authentication, algorithms, and unwrapped**.**

1. INTRODUCTION

Internet of Things (IoT) has been evolving almost in every professional field. In the IoT concept, various devices such as sensors and actuators possess computing capability and network connectivity. As a result, these devices are accessible for monitoring, control and in formation collection, via the literally ubiquitous Internet [1]. The IoT concept is bringing in an entirely new gamut of services and applications. According to European Research Centre, by 2020, there will be around 50 billion linked devices in use, with total IoT revenue anticipated to exceed one trillion euros [3]. As an emerging technology, IoT is vulnerable to cyber security assaults, and the need for remedies to secure such ecosystems is expanding all the time. While the Internet of Things (IoT) paradigm will bring a variety of appealing services and economic impact; yet, security and privacy concerns have been a primary emphasis area for IoT. With the evolution of IoT many cyber-crimes have been also surging along with it. Hence, there is essential need of effective cyber security for chocking those terrible cyber-crimes.

This study has identified many terrible cyber-crimes in an Internet of Things. We have classified different cyber-attacks according to their severity in three categories. Firstly, High severe attacks are those attacks that create large damage intensity in the IoT technology. It includes Denial Severe Attack (DoS) which is most vicious attack in IoT as it largely harms its functionality attackers or by temporarily or indefinitely disrupting services of a host linked to the Internet, attackers attempt to make a system or network resources unavailable to its intended users [4]. Second, Bot IoT attack is also severe attack Bots are automated devices which means they run according to their instruction given by user, typically routers, which are infected from malware leads to Bot attacks in IoT environment [10]. The third high severe attack in

IoT, IP Spoofing is a sort of cyber-attack in which an attacker uses a computer, device, or network to deceive other computer networks by impersonating a genuine entity and taking advantage of the IoT environment. [6]. Secondly, medium severe attacks category the cyber-attacks are less intense then the high severe attacks but it also terribly affects the IoT environment terribly. First and foremost, Routing attacks is a network layer attack, in this attack routing information floods through unknown traffic. Second, Malicious code injection, in malicious code injection an attacker uses a node to inject a malicious code into the system which gives the attacker a full control of the network, it causes a complete shutdown [2]. Third medium severe attack is DNS Server attack, in which the attacker exploits vulnerabilities in the Domain Name System [2], [5-6]. Thirdly, Low severe attacks category the cyber-attacks are least intense than above two categories. First, Man-in-the-Middle attack is widely contributing to alter the exchange of data between two IoT devices. Second, the use of Pirated Software. Basically, Pirated Software is a severe threat to internet security, through this software attacker get accessibility in the victim system and exploit it [7]. Third, least severe attack is Data Transit Attack in which attackers target the moving data from one location to another in an IoT environment and tries to alter that data and then misuse it for various purposes [2], [10]. Our study mainly investigates the proper existing strategies for ensuring effective cyber security in an IoT environment. Firstly, Ghost European framework is multilayered architecture and it emphasizes on integration aspects of IoT devices through dynamic and re-configurable solutions. Secondly, The Block chain technology has become a popular issue in a variety of fields. Block-chain technology is a decentralized open ledger that is shared publicly by all network participants. One of the most important elements of block chain is the use of cryptography to guarantee authentication and integrity for the information in the network. Decentralization and scalability, identification, autonomy, reliability, security, and market of services are some of the benefits of integrating Block chain into IoT. Thirdly, Societal Model is guardian which provides complete framework for an IoT environment, it provides endpoint security, group security and alert mechanism by utilizing the basic security requirements, namely, confidentiality, integrity, availability, accountability, authenticity, and non-repudiation. Along with it, Intrusion Detection is a best technique in an IoT technology, it provides solutions for a variety of security concerns by continuously monitoring the system and issuing an alarm in the event of any suspicious behavior. It also retains a log of the attacker's activities, which may aid in tracing the attacker [2-6]. Moreover, the major goals of the GPRS security architecture are to secure the network from illegal access and to preserve the privacy of users in an IoT context [6]. Lastly, the use of effective Machine learning algorithms can drift the security of IoT such as; Naïve Bayes, Bayes Net, Decision Tree C4.5, and Random Tree. Therefore, utilizing above approaches can ensure secure and risk free IoT environment.

This Systematic Literature Review is based on complete review methodology from well-known and reputable studies to ensure the authenticity of extracted literature. It has four sections; section1 is introduction which provides complete overview of research in summarize form. Section2 furnishes entire research methodology and complete process of research. Section 3 is based on the review of selected studies with comprehensive analysis of literature, and section 4 consists on future directions for interested researchers and conclusion along with a few unwrapped issues of our SLR.

2. RESEARCH METHODOLOGY

The Research Methodology magnifies the Systematic Literature Review (SLR) guidelines which lead towards proper research in any discipline. Basically, SLR is based on three phases named; Planning, Conducting and Reporting. All phases consist on meaningful steps which play essential role to conduct proper research. Firstly, in planning phase we particularly plan our entire research and its strategies that answer how we will execute our plan in a proper way in order to conduct a suitable research which can contribute in body of knowledge (will be discussed in section 2.1). Secondly, in Conducting phase we practically conduct our research in order to collect broad literature related to our field which ultimately helps us to move towards writing our research (will be discussed in section 2.2) . Finally, in Reporting phase we write our research and summarizing and validating through our reviewed literature (will be discussed in section 2.3).

2.1 Planning:

The purpose of this SLR is to summarize and clarify the IoT based AI technique used in precision agriculture. The following four research questions (RQs) were raised to achieve this aim as shown in table 1.

2.1.1 Identification of Research Questions:

In this step of planning phase, we basically identify various research questions even its sub-questions for our research problem. We have also identified the various questions regarding our research topic "*Cyber Security Approaches and Diversities in IOT: Systematic Literature Review and unwrapped problems*" and these questions are given in Table 1.

Table 1 Research Questions

RQ1	What are existing Cyber Security approaches and trends in to counter Cyber Crimes for IOT?
RQ2	What is importance of IOT in current era of technology?
RQ3	What are current available security modules for IOT?
RQ4	What are Cyber Security essentials for IOT to counter current terrible cyber-crimes?
RQ5	What type of security risks are there in IoT devices?
RQ6	Why is security essential for IoT?
RQ7	What types of existing security solutions are currently available for IoT?

2.1.2 Identification of Data Sources:

For conducting proper research and extracting good literature related to our topic from reputable data sources, we haveto select good and recognized data sources in order to pursue better research and to contribute effective way in body ofknowledge. We have identified various data sources which are mentioned below:

i. Scopus
ii. Web of Science
iii. IEEEXplore
iv. Science Direct

2.1.3 Study Selection Criteria (Inclusion and Exclusion)

Study selection criteria reflects the scope and limitation of our research which is given in Table 2.

Table 2 List of Inclusion and Exclusion Criteria

Sr.No	**Inclusion Criteria**
1	The paper must have Cyber Security approaches related to Internet of Things (IoT).
2	The paper must have identified open security issues related to IoT.
3	The paper must have contained various diversities, methods or algorithms of Cyber Security for securing IoT.
4	The paper should be written entirely English.
5	The Article should be published in between 2015 and 2020.
6	The Article should be either conference proceeding our Journal article.
Sr.No	**Exclusion Criteria**
1	The paper has contained information about other research topics other than Cyber Security and Internet of things (IoT).
2	The paper has contained information about either Cyber Security or IoT.
3	The paper has been published before 2015 and after 2020.
4	The paper has been published in language other than English.

2.1.4 Quality Assessment Criteria (QAC):

The quality assessment criteria of paper are based on various points which are mentioned below:

2.1.4.1 The paper should have clear objective.
2.1.4.2 The methodology of paper should be clear.
2.1.4.3 A comprehensive literature review should be given in the paper.
2.1.4.4 The results should be clearly mentioned in the paper.
2.1.4.5 The strategies along with proper analysis should be accurately discussed in the paper.

2.1.5 Data Extraction Strategy:

Data extraction strategy is completely mentioned in Table 3.

Table 3 Data Extraction

Sr.No	Data Extraction Strategy
1	Title of Paper and its authors
2	Main objective of paper
3	Methodology and algorithms that are mentioned in paper
4	Results of Paper
5	Limitation and Future work

2.2 Conducting:

2.2.1 Search Process:

Search process of various research papers from aforementioned data sources is based on keywords that are formulatedon the basis of research topic and research question that we have identified and selected.

2.2.2 Identify Keywords and formulate search query:

We have classified the search keyword in various group and then formulated the query based on those keywords.As shown in Table 4.

Table 4 Keywords and Search Query

Groups	Keywords
Group 1 Related to Cyber Security, Cyber laws,Security in broader context	cyber policies, safe computing, authentication protocols, authorization protocols, privacy breach, cyber-crimes, cyber threats, vulnerabilities, hackingtechniques, hacking tools, security exploitation, Computer viruses.
Group 2 Related to Internet of Things inbroader context	Internet of things (IOT), sensor devices, networking nodes, end user devices,distribution networking devices, IT assets.
Group 3 Additional key words for combination and connection	Diversities, approaches, trends, tools and techniques, models, methods, frameworks, policies, projects, algorithms.
Group 4 Publication years	January 2015 to December 2020
Group 5 Research Paper Medium	English language only
Final Search Query	(Group1) And (Group2) And (Group3) And (Group4) And (Group5) And (Group6)

2.2.3 Selection of Primary Studies:

Selection of primary studies is based on six filters and four academic databases which is given in Table 5.

Table 5 Searching of Primary Studies

Databases	Initial Search	After Duplication Removal	After Screening of Abstract	After Full Text Reading	After Evaluation of Query
Scopus	72	56	32	12	8
Web of Science	44	41	24	9	8
Science Direct	13	8	6	5	3
IEEE Xplore	36	31	14	12	9
Total	165				28

2.2.4 Assess Study Quality:

We have assessed the quality of study based on aforementioned Quality Assessment Criteria (QAC) and study selection criteria as shown in Table 1. The main purpose of QAC is to evaluate the study in order to address our review objectives.Furthermore, we both authors of this paper collectively made a checklist in order to assess our primary studies as shownin Table 4. In addition to this, result of each selected study has evaluated and examined on the basis of our objective andresearch topic. We have also made threshold from 1 to 10, in order to rate our selected studies and then review our literature on the basis of that threshold. We have selected those studies which rated 7 or more unanimously. Thus, we have selected 28 articles for our review from various databases on the basis of our rating and QAC.

2.2.4 Data Extraction:

Data has been extracted in tabular form from our 28 selected articles as mentioned in data extraction strategy in Table 2 and it is comprised on the following five aspects: (1) Title of the paper, (2) main objective of the paper, (3) algorithms, approaches or methods for the security of IoT from cyber-crimes, (4) results and performance metrics, and (5) limitation and future work mentioned in the papers.

2.2.5 Data Synthesis:

For data synthesis, we have extracted data in Endnote and also made one excel file in order to manage data in proper form. Furthermore, we have also made different folders for various studies that we have selected from different data sources and placed extracted data in those folders. Hence, last 28 studies we have placed in one folder after its quality assessment in order to review those studies on the basis of our quality assessment criteria and defined threshold.

2.3 Reporting:

This phase of Systematic literature review is very essential. This phase will begin after complete planning and conductingphase. In this phase we have to do summarization, critical analysis and also mention future directions of selected literaturethat we have reviewed. There are two main aspects of this phase. 1) Writing a review, in this aspect we write a review on the basis of SLR guidelines and following those guidelines we have to logically analyze it and then put it together in text form coherently and logically. 2) Validating the review, in this aspect we validate our research by giving references of reviewed paper and their contribution regarding our topic in proper manner in order to present effective research and contributing in body of knowledge. Lastly, in the reporting phase of SLR we have to write our entire research paper which should be systematically meet the requirements that were defined previously. Hence, we have also followed all guidelines of SLR in order to write our review paper in proper way which are mentioned in sections 1, 2,3 and 4.

3. REVIEW AND DISCUSSION

In this section we have presented our studies and literature that we have reviewed in an organized and coherent form. Wewill discuss the cyber-attacks that choke the performance of Internet of Things (IoT) and their solutions in given below sections.

3.1 Different Types of Cyber Attacks Identified in IOT:

Cyber-attacks are very terrible for entire Internet of Things (IoT) environment; it is not only distorting its performance but also affect the functionality of the end devices. In this paper, we have classified different cyber-attacks according to their severity in three categories. Firstly, High severe attacks are those attacks which create large damage intensity in the IoT technology. In high severe attacks category, Denial of Service (DoS) attack is the first cybercrime thatdamages the security of IoT, it is widely considered as a lethal tool that degrades the performance of IoT devices. A DoSattack can be done by sending thousands of requests to a target within a short time, which will cause the server to overflowcapacity. This attack simply makes an online service unavailable with the help of enormous traffic from multiple sources [4]. Second, Bot IoT attack, is also considered as the most severe attack in an IoT. Basically, Bots are automated deviceswhich means they run according to their instruction given by user, typically routers, which are infected from malware leads to Bot attacks in IoT environment [10]. The third most severe attack, IP Spoofing is a sort of cyber-attack in whichan attacker uses a computer, device, or network to deceive other computer networks by impersonating a genuine entity and taking advantage of the IoT environment. [6].

In medium severe attacks category, the cyber-attacks are less intense then the high severe attacks though it affectsthe IoT environment terribly. First and foremost, Routing attacks is a network layer attack, in this attack routing information floods through unknown traffic, alteration or replay in order to make resources unavailable to intended users and attacker tries to get the control of the desired network [2]. Second, Malicious code injection is medium severe attack.Malicious code injection is when an attacker uses a node to inject malicious code into a system, giving the attacker complete control of the network and causing it to shut down completely [2]. Third medium severe attack is DNS Server attack, in which the attacker exploits vulnerabilities in the Domain Name System and poisoning the cache of the victim device in order to get the control of the system [2],[5-6].

In low severe attacks category, the cyber-attacks are least intense than above two categories. Firstly, Man-in-theMiddle attack is widely contributing to alter the exchange of data between two IoT devices. Further, it aims to eavesdrop to the communication channel to monitor or control all the private communications between the two parties and then utilizes for the desired purpose [2]. Secondly, pirated software is a clone of the original program created by reverse engineering processes and then designing the same logic in a different form of source code creation of software by unlawfully reusing source codes and passing it off as the original version. Basically, Pirated Software is a severe threat to internet security, through this software attacker get accessibility in the victim system and exploit it [7]. Third least severeattack is Data Transit Attack in which attackers target the moving data from one location to another in an IoT environment and tries to alter that data and then misuse it for various purposes [2], [10]. Therefore, above attacks have been playing very vicious role to choke the performance of IoT at every level (Figure 1).

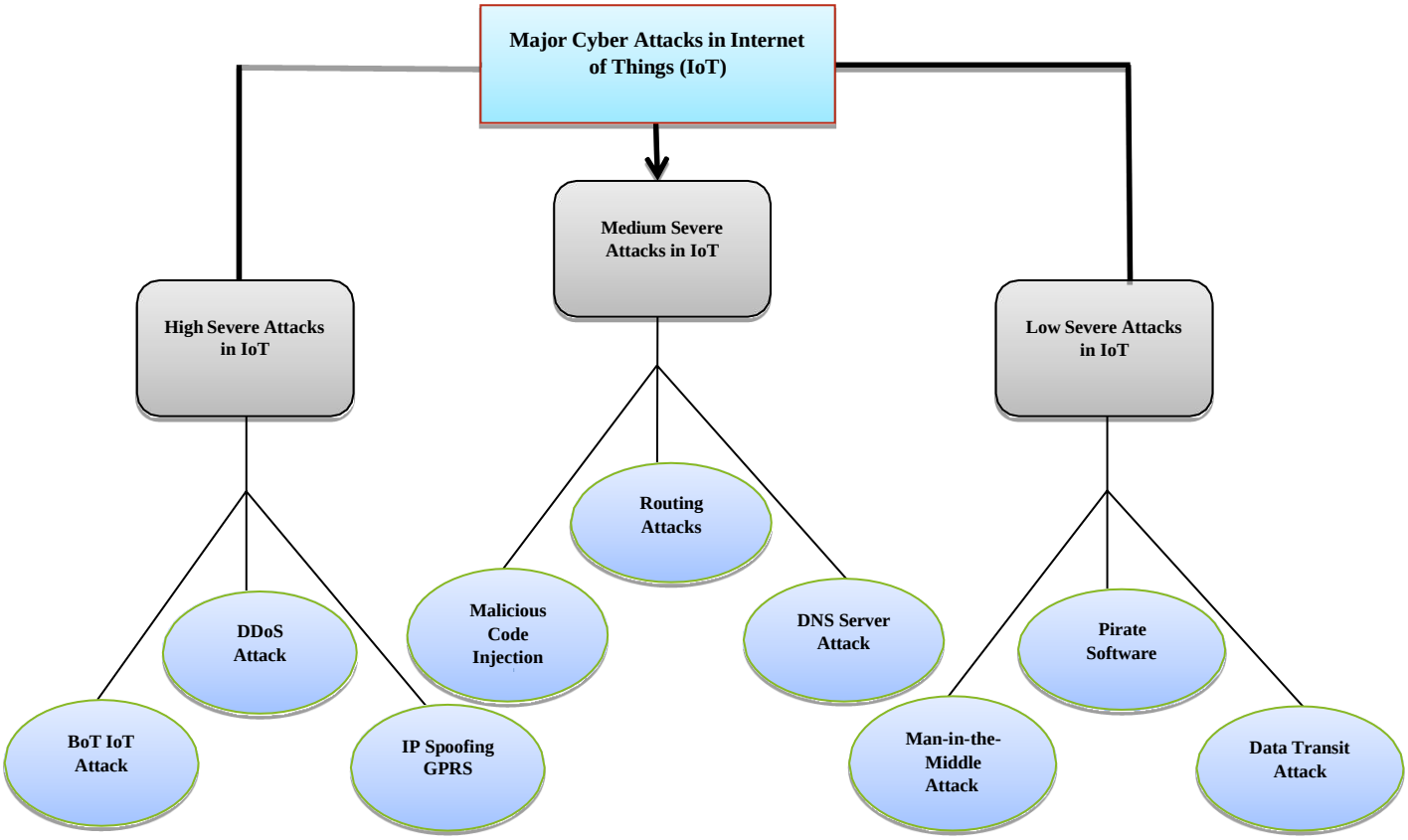

Figure 1: Types of Cyber Attacks

3.2 Review Of Existing Cyber Security Strategies And Methods For Securing Iot Environment:

In our studies, we have identified many strategies and approaches for security of IoT Environment. Those techniques are very effective for securing home automation, end nodes, network devices, data storage devices, etc. There are number of studies presented for the detection and prevention of cyber-attacks such as; Societal Model, The H2020 Ghost framework, Block Chain technology, Intrusion detection, GPRS security architecture, Machine learning techniques, etc. (Graph 2). In each study the different cybersecurity technique has been defined to tackle different types of cyber-attack (Graph 1). Basically, The H2020 European research project Ghost Safe-Guarding Home IoT Environments with Personalized Real-time Risk Control and aims to deploy a highly effective security framework for IoT smart home residents through novel reference architecture for user-centric cyber security in smart homes providing an unobtrusive and user-comprehensible solution [1].

Moreover, for mitigation of Distributed Denial of Service attack (DDoS) in IoT, the two best solutions have been presented in paper. One, Prevent Key based Infrastructure (PKI) solution, in this secret key can be used which mustbe declared as public key and it can be securely stored in secure tamper-proof chip and only legitimate IoT device can access the secret data [4]. Second, Peer-to-Peer (P2P) and Blockchian technology has proposed to use for mitigation of DDoS, a new network group can be created which will generate P2P network using Blockchian programming to quarantine all the peers which send unusual requests then the request will be sent to the system to check whether the request is valid or not [4]. Along with it, Intrusion Detection is a best technique in an IoT technology, it provides solutions for a variety of security concerns by continuously monitoring the system and issuingan alarm in the event of any suspicious behavior. It also retains a log of the attacker's activities, which may aid in tracing the attacker. [2,6]. Moreover, the GPRS security architecture uses a series of security methods that make up the GPRS security architecture. The majority of these methods were created for GSM, but they've been tweaked to operate with packet-oriented traffic and GPRS network components. The GPRS security architecture primarily pursues two objectives: a) to prevent unwanted access to the network, and b) to preserve users' privacy. [6]. Furthermore, Trusted Cloud Platform is used to provide the reliable security to cloud in a network specifically in anIoT environment. The foundation of trusted computing is the establishment of a trust mechanism based oncryptography and a trusted computing base. [10]. In addition to this, there are many Machine Learning (ML) techniques are presented in different articles to secure IoT technology from terrible cybercrimes. Most effective machine learning techniques that we extracted from our literature are given below (Figure 2).

i **Naïve Bayes and Bayes Net:** These both are machine learning classifiers based on Bayes theorem and used to calculate pre and post risks through total probability. These techniques collectively known as Bayesian Network. This network is very efficient to identify malicious traffic in IoT environment [11].

ii **Random Forest Tree and Decision Tree:** These two machine learning classifiers can also be used as trees and very efficient for classification and regression. These are supervised machine learning algorithms and very effective against Denial of Service (DoS) attack and identification of malicious traffic of each node in an IoT technology [11].

iii **Malware and Software Piracy Detection Techniques:** Preprocessing and Deep Convolutional Neural Network (DCNN) ML techniques are used to malware detection. Basically, color image is generated by using binary file through preprocessing and then malware detect through image classification problem after it, DCNN uses two layers including; Convolution layer and pooling layer to reduce data overhead while keeping valuable data for detection of malware in network traffic [7]. Secondly, for software piracy detection preprocessing feature extraction ML techniques were used for this many essential ML algorithms used to include; Parse tree, K-nearest neighbor algorithm, Latent Semantic Analysis, and Multiple Linear Regression [7].

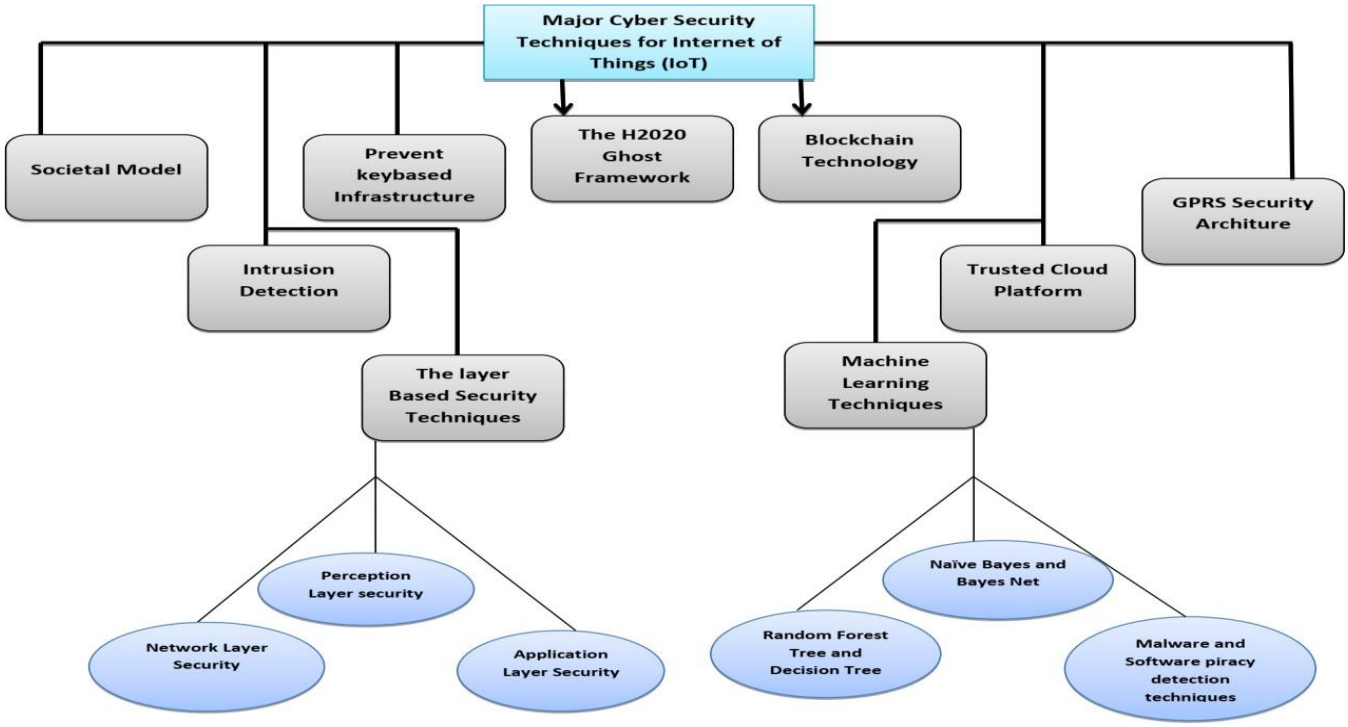

Figure 2: Major Cyber Security Techniques

3.3 Review of Existing Strategies Against Cyber Attacks:

Its effectiveness basis on its results and challenges in an Internet of Things (IoT) environment. The main purpose of Table 6 is to clearly and coherently address each strategy according to the perspective of IoT. Finally, it will surely help for future implementations in an IoT, its rating based on quantitative analysis that we have given in Table 6 after reviewing its effectiveness basis on its results and challenges in an Internet of Things (IoT) environment. coherently address each strategy according to the perspective of IoT. Finally, it will surely help for future implementations in an IoT, its rating based on quantitative analysis that we have given in Table 6 after reviewing its effectiveness basis on its results and challenges in an Internet of Things (IoT) environment. environment. The main purpose of Internet of Things (IoT) environment. reviewing its effectiveness basis on its results and challenges in an Internet of Things (IoT) environment. Table 6 is to clearly and performance, its rating based on quantitative analysis that we have given in Table 6 after reviewing its effectiveness basis on its results and challenges in an Internet of Things (IoT).

Table 6 Strategies for Cyber Attack

Sr.No	Framework/ Methods/ Approaches	Cyber Security Metrics	Tackling Types Cyber Attack	Process and Results	Effectiveness for Internet of Things(Ratingon your own Analysis
1	TheH2020 European Project Ghost	NetworkandData FlowAnalysis (NDFA), Context Reasoning Time Series Approach (CR-ISA), Context Reasoning Communication Event(CR-CE)	Malicious traffic, Data transit attack. Denial of Service attack.	Effective Monitoring, Ensure privacy, and Identify communication between two channels	Highly Effective for Smart homes and IoT Environment
2	The Layer Based Security (Application, Network, Perception Layer)	Authentication, Encryption, Reliable, Transmission and Secrecy	Denial of Service attacks, Routing attacks, Malicious code injection and Data transit attack	Collect information from physical equipment, apply cyber security metrics, and filterthe collected information.	Very Effective from IoT devices and their communication
3	The Societal Model	Data definition, Data syntax and data semantics.	Distributed Denial of Service attack (DDoS).	The Guardian device I- Guardian is used for filtering the traffic according to syntax and its semantics.	Effective for IoT
4	The Block Chain Technology	Processed transaction, Processing time, authentication, Digital signature , hit/miss Requests and identify of traffic.	Denial of Service attack and Malicious traffic.	Stores record in the form of blocks, connected various data as various chain and authorize it according to mentioned metrics.	Very Effective in an IoT Environment.
5	The Prevent Key based Infrastructure (PKI) Solution	Authentication, Cryptography and secrecy.	Denial of Service attacks.	Cryptography and authentication of IoT devise allow secure communication between them.	Effective for IoT.
6	The Intrusion Detection	Monitoring, traffic classification, anomaly detection.	Malicious traffic, Malicious code injection.	Monitoring the system, detect the suspicious activity and generate alert message.	Effective for IoT.
7	Trusted Cloud Platform	Cryptography and Authentication.	Malicious traffic.	Strengthen the cloud platform, traffic passes through trusted root, trusted hardware platform, trusted operating system and trusted application by applying metrics.	Very Effective in an IoT Environment.

8	GPRS Security Architecture	Authentication, Confidentiality and security	Malicious code injection.	Protect network against unauthorized access, Protect privacy of used	Effective for IoT.
9	Machine Learning Techniques	Naïve Bayes, Bayes Net, Random Forest Tree, Decision Tree, Preprocessing and Neural Network.	Malicious traffic, Denial of Service attack, malware detection and software privacy.	Applying machine learning techniques such as: Naïve Bayes, Decision Tree, Preprocessing and Convolutional neural network to detect malicious activity.	Highly Effective in an IoT Environment.

4. Conclusion and Future Directions

This study presented a review of 28 selected primary studies from various reputable sources with critical analysis and comprehensive presentation. The focused of entire review paper was last 5 years' research papers which were filtered on the basis of relevancy along with systematic approach. In this paper, we have presented different challenges and issues occurred in Internet of Things (IoT) along with existing strategies to counter those challenges.The different solutions and strategies we have presented in our review paper with their methodology though they were not perfect enough to provide sustainable security to IoT environment. However, those cyber security techniques were beneficial against terrible cyber-attacks in an IoT. We have also identified future directions and some unwrapped issues. First of all, The Ghost European framework is user centric in which authentication is complex. Furthermore, it is effective for smart homes only, which opens space to implement it in more real world environment with better security and authentication. Secondly, Block chain technology has not properly implemented yet it really opens a door for researchers to work on it in order to contribute in security for Internet of Things (IoT) with proper methodology. Furthermore, no proper defense system has introduced yet against Denial ofService attack researchers can work on it as well. Moreover, IoT devices need inbuilt cyber security in order to ensure proper connectivity and privacy of data. Along with it, utilization of different machine learning techniques including; regression, classification, correlation, precision, K-nearest neighbor (KNN) algorithm, latent semantic analysis and other machine earning algorithms can be proved very beneficial to strengthen the security of IoT. While concluding the entire discussion, we believe this comprehensive review will provide a depth understanding of the various cyber-attacks in an IoT along with present approaches and trends to choke those attacks with some future direction that can open doors for future researchers to contribute in this evolving technology.

References

[1]. Augusto-Gonzalez, J., et al. From internet of threats to internet of things: A cyber security architecture for smart homes, IEEE.2019

[2]. Faisal, M., et al. (2020). "Cyber Security and Key Management Issues for Internet of Things: Techniques, Requirements, and Challenges." Complexity 2020.

[3]. Tsunoda, H. and G. M. Keeni Feasibility of societal model for securing Internet of Things, IEEE.2017.

[4]. Rohit, M. H., et al. Mitigating and Detecting DDoS attack on IoT Environment, IEEE.2019..

[5]. Hossain, M., et al. Securing the internet of things: A meta-study of challenges, approaches, and open problems, IEEE.2017.

[6]. Tonge, A. M., et al. (2013). "Cyber security: challenges for society-literature review." IOSR Journal of computer Engineering 12(2): 67-75.

[7]. Taheri, S., et al. Multi-Source Cyber-Attacks Detection using Machine Learning, IEEE.2019.

[8]. Ullah, F., et al. (2019). "Cyber security threats detection in internet of things using deep learning approach." IEEE Access 7: 124379-124389.

[9]. Kang, C.-q., et al. Cyber Security Risk Analysis and Protection Structure Design for Power Distribution IoT, IEEE.2020

[10]. Shafiq, M., et al. (2020). "Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city." Future Generation Computer Systems 107: 433-442.

[11]. Shi, Y., et al. Energy audition based cyber-physical attack detection system in IoT.2019.

[12]. Faraj, O., et al. Taxonomy and challenges in machine learning-based approaches to detect attacks in the internet of things.2020.

[13]. Securing ZigBee IoT Network Against HULK Distributed Denial of Service Attack, IEEE.2020

[14]. Nirmal, K., et al. (2020). "Analyzing and eliminating phishing threats in IoT, network and other Web applications using iterative intersection." Peer-to-Peer Networking and Applications: 1-13.

[15]. Gupta, S., et al. (2019). "Cyber Security Threat Intelligence Using Data Mining Techniques and Artificial Intelligence." Int. J. Recent Technol. Eng 8: 6133-6140.

[16]. Zainab, A., et al. (2020). "Ensemble-Based Spam Detection in Smart Home IoT Devices Time Series Data Using Machine Learning Techniques." Information 11(7): 344.

[17]. Laszka, A., et al. (2020). "Integrating redundancy, diversity, and hardening to improve security of industrial internet of things." Cyber-Physical Systems 6(1): 1-32.

[18]. Carreras Guzman, N. H., et al. (2020). "Conceptualizing the key features of cyber-physical systems in a multi- layered representation for safety and security analysis." Systems Engineering 23(2): 189-210.

[19]. Oravec, J. A. Emerging “cyber hygiene” practices for the Internet of Things (IoT): professional issues in consulting clients and educating users on IoT privacy and security, IEEE.2017.

[20]. Wolf, M. and D. Serpanos (2017). "Safety and security in cyber-physical systems and internet-of-things systems." Proceedings of the IEEE 106(1): 9-20

[21]. Ionescu, O., et al. On the development of a robust cyber security system for Internet of Things devices, IEEE.2019.

[22]. Tawalbeh, L. a., et al. (2020). "IoT Privacy and security: Challenges and solutions." Applied Sciences 10(12): 4102.

[23]. Faisal, M., et al. (2020). "Cyber Security and Key Management Issues for Internet of Things: Techniques, Requirements, and Challenges." Complexity 2020.

[24]. Zhang, R. and Q. Zhu (2019). "$\mathtt {FlipIn} $: A Game-Theoretic Cyber Insurance Framework for Incentive- Compatible Cyber Risk Management of Internet of Things." IEEE Transactions on Information Forensics and Security 15: 2026-2041.

[25]. Zahra, S. R. and M. A. Chishti Ransomware and internet of things: A new security nightmare, IEEE.

[26]. Lange, T. and H. Kettani On security threats of botnets to cyber systems, IEEE.2019.

[27]. Dua, A., et al. Iisr: A secure router for iot networks, IEEE.2019

[28]. Ammirato, S., et al. (2019). "The potential of IoT in redesigning the bank branch protection system." Business Process Management Journal.

Acknowledgment:

We are deeply grateful to all those who played a role in the success of this research paper. We would like to thank specifically Dr.Ghulam Mujtaba Shaikh, Dr. Javed Ahmed Shahani, Dr.Qammar Uddin Khand and Dr. Raheel Ahmed Memon for their invaluable input and support throughout the research process. Their insights and expertise were instrumental in shaping the direction of this research. Moreover, we also want to thank SHJSE foraccepting our research paper and we are optimistic enough that this research will definitely prove as beneficial tool for future researchers.

Authors' Profiles

Ali Aizaz has completed Graduation in Information Technology from Quaid-e-Awam University of Engineering Science and Technology, Nawabshah with various distinction, declared as "Best Graduate", "Faculty Top", and "1st Position Holder". During his graduation degree, he has been involved inmany hardware and software projects. Along with it, my final year project with thesis was "E-TrackingSystem for Municipal Solid Waste Management System Using RFID Technology" which was hybrid project and amalgamation of hardware and software with the aim of maintaining and managing solid waste by using centralized technology. Currently, Ali enrolled in Sukkur IBA University for the Master's Program in Computer Scienceand also involved in many research projects with the affiliation of various foreign universities.

Aurangzaib Ali has completed his Graduation in Computer System Engineering from Quaid-e-Awam University of Engineering Science and Technology, Nawabshah with flying colors. Furthermore, his final year project in graduation was "Edhi Online Tracking System". Currently, I am enrolled in Sukkur IBA University for the Master's Program in Computer Science and also involved in many research projects with the affiliation of various foreign universities.