ISSN (ONLINE) : 2045-8711
ISSN (PRINT) : 2045-869X

INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY & CREATIVE ENGINEERING

April 2023
Vol - 13 No - 4
@IJITCE Publication

Design by Hemharsith

UK: Managing Editor
International Journal of Innovative Technology and Creative Engineering
1a park lane,
Cranford
London
TW59WA
UK

USA: Editor
International Journal of Innovative Technology and Creative Engineering
Dr. Arumugam
Department of Chemistry
University of Georgia
GA-30602, USA.

India: Editor
International Journal of Innovative Technology & Creative Engineering
36/4 12th Avenue,
1st cross St,
Vaigai Colony
Ashok Nagar
Chennai, India 600083

Email: editor@ijitce.co.uk

www.ijitce.co.uk

IJITCE PUBLICATION

International Journal of Innovative Technology & Creative Engineering

Vol.13 No.04

April 2023

IJITCE

INNOVATE TO CREATE

www.ijitce.co.uk

Dear Researcher,

Greetings!

Articles in this issue discusses about study on data mining concepts in computer science.

We look forward many more new technologies in the next month.

Thanks,
Editorial Team
IJITCE

Editorial Members

Review Board Members

Contents

AN ANALYSIS AND OVERVIEW ON CYBER-SECURITY IN IOT NETWORKS USING MACHINE LEARNING

Mrs. Kalpana Chittor S [1]
Research Scholar, School of Science Studies, CMR University, Bangalore,India.
Dr Chitra Ravi2
Director & Professor, SOSS, OMBR Layout, CMR University, Bangalore,India.

Abstract – The network models evolved over a long period; the next generation network is the IoT (Internet of Things). IoT is nothing but intelligent connectivity between plenty of devices. IoT derives huge gains in many of the ubiquitous applications like smart health, smart transport, smart city, and smart home. Its vision is to support every walk of life including agriculture, and factory automation as a part of the industrial revolution and in diverse fields. Thus, the IoT network will be a lifeline for the future digital system. However, every system has vulnerabilities due to its architectural design and characteristics. These vulnerabilities assist and attract attackers to plan their strategies. The threats and risks due to attacks on the IoT application and network can cause a serious effect on both users as well as service providers, not only financially but sometimes fatal too. Therefore, it is an essential research issue to put focus on the security features of IoT.

The emerging trend of intelligent technologies like SDN (Software Defined Networking), DL (Deep Learning), AI (Artificial Intelligence), and ML (Machine Learning) is attracting widespread attention in the research community for addressing various security issues in the wireless network system. Machine learning and deep learning techniques are robust technologies that have the capability of data exploration and learning. The solution developed based on machine learning collects data from the sensor nodes and based on their capability, it classifies the normal and abnormal pattern of the traffic flow in the network as well as the behavior of networking and information sensing devices according to how devices interact with each other within the IoT ecosystem.

Keywords: Internet of Things (IoT), IoT Platforms, IoT Attacks, Authentication, Datasets, Technological Providers.

1. INTRODUCTION

Over the past decades, the IoT platform was used in every aspect of Human Life. IoT is considered a Misnomer as devices need not be connected to the public internet, but can be connected to Network and can be addressed individually. IoT Paradigm integrates the Internet and various physical objects of several domains. In IoT, the various electrical devices are interlinked with the Server, and information is exchanged, without the intervention of Humans. It integrates a variety of networks of devices to provide intelligent and advanced services. A network is a group of peripherals, network devices, servers, computers, or other devices connected to allow Data Sharing. Providing Network Security for IoT devices has become a challenging task. [1]

IoT network has become a lifeline for the future digital communication system. IoT is facing more security challenges because of the demand for smart devices usages and its tremendous easy accessibility. The existing security measures and traditional techniques are not sufficient to enhance the up-to-date security system for the next generation of IoT. However, every system has associated vulnerabilities due to its architecture, design, and characteristics. These vulnerabilities assist the attackers to plan their strategies. The threats and risks due to attacks on the IoT application and network can cause a serious effect on both users as well as service providers. Therefore, it is an essential research issue to put focus on the security aspects of IoT. To detect intruders/attacks and overcome network security problems, Machine Learning (ML) is considered a powerful technology. [2]

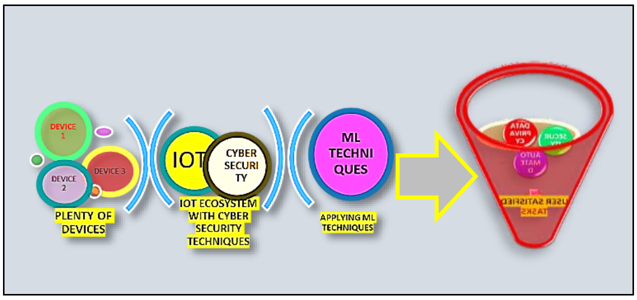


Fig.1: Process of Detecting Intruders in Cyber Security of Iot Using Ml Achieving Data Security and End-User Automated Tasks

Fig.1 depicts the usage of ML techniques in attaining End-User tasks.ML and DL approaches are robust technologies. Furthermore, ML can be also very useful for predicting new kinds of attacks and unknown attacks, which may be modified versions of traditional attacks. It is being observed that there are 11,906 journals in the domain of IoT and out of which 3,137 journals are on security, which is approximately 26.4% that shows there is active research on the security domain in IoT.

2. IOT

The concept of Smart devices are discussed in early 1982, with a Coca-Cola vending machine, the first ARPANET-connected appliance at Carnegie Mellon University. It can inventory report whether newly loaded drinks are cold or not. Later the word " Internet of Things" was invented by Kevin Ashton in 1999. As years passed, the usage of Internet Of Things(IoT) applications drastically increased in various fields like Military Applications, Infrastructure Applications, Industrial Applications, Organizational Applications, and Consumer applications.

The IoT consists of Physical Objects, interconnected with Software, Sensors, Processing ability and other Technologies. It is an everything-to-everything communication. They communicate and exchange data among themselves either by the Internet or by any other communication network where each device is addressed individually. Figure 2 describes IOT 3-Tier Architecture which has three layers. They are a) The Perception/Hardware Layer b) The Network/Communication Layer and c) The Application Layer.

Perception Layer: This layer comprises PHY (Physical) and MAC (Medium Access Control) and deals with hardware like Sensors and Actuators, while the MAC layer creates a link between Physical devices & Networks to provide communication. A collection of internet-connected devices is connected to detect objects, gather data, and communicate with other devices through Internet communication networks. Examples: GPS (Global Positioning Systems), Cameras, RFID, Sensors, etc.

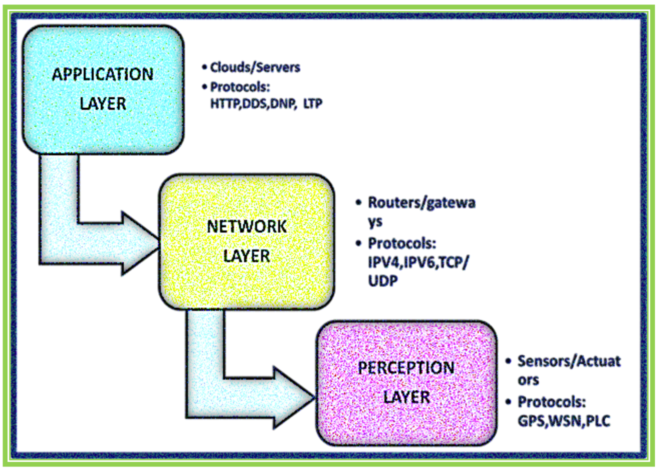
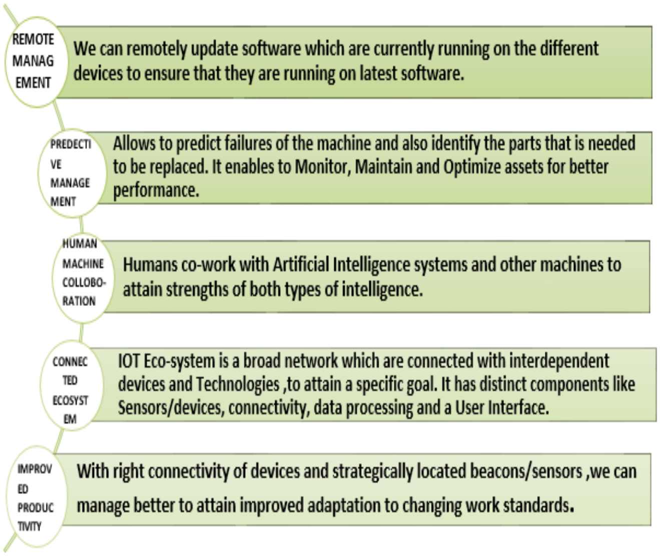


Fig 2: Three-Tier Architecture Of Iot

The PHY layer deals with hardware like Actuators and Sensors. Network Layer: It forwards data from the perception layer to the application layer. This layer includes communication and messaging protocols. The main communication technology in IoT is Wireless Sensor Network(WSN). It supports dynamic communication based on 802.15.4 standards. They contain short-range communication protocols PLC, WiFi, Zigbee, 4G, 5G, Bluetooth, etc. Application Layer: It is the upper layer that processes the incoming information which helps in designing better power distribution and management strategies. The aggregator is an important component that acts as a gateway for IoT architecture. In the IoT ecosystem, another core element is the cloud. It provides services like storage, analytics, and Data processing. It provides Data Processing, Privacy Protection, and Authentication. Examples: power system monitoring, smart cities, energy management, and integration of renewable energy generators. [3] The below given Fig.3 clearly explains the benefits of IOT.



We can remotely update software which are currently running on the different devices to ensure that they are running on latest software.

Allows to predict failures of the machine and also identify the parts that is needed to be replaced. It enables to Monitor, Maintain and Optimize assets for better performance.

Humans co-work with Artificial Intelligence systems and other machines to attain strengths of both types of intelligence.

IOT Eco-system is a broad network which are connected with interdependent devices and Technologies ,to attain a specific goal. It has distinct components like Sensors/devices, connectivity, data processing and a User Interface.

With right connectivity of devices and strategically located beacons/sensors ,we can manage better to attain improved adaptation to changing work standards.

Fig. 3: Benefits Of IOT

2.1 Applications of IOT

Fig.4 shows various usages of IOT in different fields like Industries, Organisations, Home Automations, Medical field and in Military.

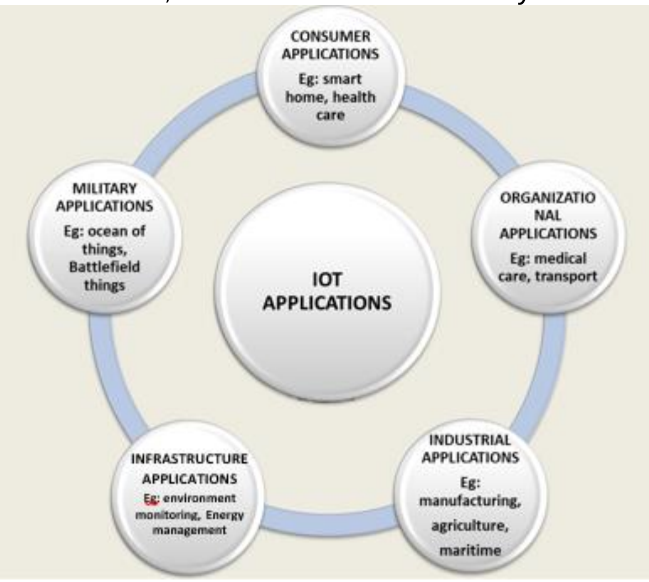

IOT APPLICATIONS
CONSUMER APPLICATIONS
Eg: smart home, health care
ORGANIZATIO NAL APPLICATIONS
Eg: medical care, transport
INDUSTRIAL APPLICATIONS
Eg: manufacturing, agriculture, maritime
INFRASTRUCTURE APPLICATIONS
Eg: environment monitoring, Energy management
MILITARY APPLICATIONS
Eg: ocean of things, Battlefield things

Fig. 4: Different Usages Of Iot In Various Fields

a) Consumer Applications: IoT Applications are created for consumer use like Wearables technology, connected vehicles, Home Automation, Appliances with Remote Monitoring, and Connected Health.

b) Transport: IOT can be used for assisting various communication, and control to process information over the transportation system. It can be enabled in Electronic Toll Collection systems, Smart Parking, Vehicle control, Road assistance, Safety, and Fleet management.

c) Home Automation: It is applied to Electrical, Mechanical, and electronic systems in various types of buildings.

d) Industrial Applications: IOT helps in regulating and monitoring Industrial systems. They can be used to analyze data from locations, people, operational technology, etc.

e) Military applications: IoT technologies are applied in a military domain for surveillance, reconnaissance, and other objectives. It can be used for prospects of warfare, human-wearable biometrics, robots, vehicles, and also for other smart technologies related to the battlefield. [4]

2.2 Importance of Security in IoT

The real-life examples of IoT security Failures that caused major distractions are:

- In 2010, an IoT attack was Stuxnet, which targeted the smart industry controller which utilizes nuclear facilities. The malware destroyed one-quarter of centrifuges, bringing down nuclear program halt for the next days.
- In 2015, Russian IOT malware attacked the electrical grids of Ukraine, leaving 2,30,000 people without power.
- The famous IOT hacks in Mirai, Botnet attacked Liberia's Infrastructure, used brute force authentication against ID cameras, as these cameras used, most commonly used Usernames and passwords, and attacked nearly 3,60,000 servers. Hackers also attacked websites like Netflix, Reddit, Twitter, GitHub, etc.
- In 2017, a Hacker got access to 2,00,000 open printers and printed over the internet, thereby affecting almost 1,50,000 printers.

Therefore, providing security to IoT devices has become a burning and problematic task as IoT devices use minimal capacity things, objects, sensors, and actuators. Moreover, in the IoT ecosystem, Millions of devices are connected. But still, sensitive information needs to be secured thoroughly without leaking to intruders to avoid major losses.

2.3 IoT security methods using ML

The defining characteristic of IoT is interconnectivity among different devices. To collect data from the surrounding sensor devices and transfer it to the Internet is the responsibility of a Gateway device. In plenty of cases, the use of Machine Learning (ML) algorithms for securing IoT devices and Networks has proved to be extremely beneficial and also given promising results. We can use ML as a practical tool in many programming scenarios, especially in Cyber security. IoT Security is a major challenging area in Cyber security. There is constant development of new techniques to secure IoT devices to better protect against cyber-attacks on IoT devices and networks, which are evolving and ever-changing. In complex networks, IoT devices need to select and Identify Key attributes and Protective strategies. However, developing security measures for IoT devices, have its own set of challenges. [5]

Different Kinds of Attacks: IOT Attacks are broadly classified as Physical and Cyber Attacks as shown in Figure 5. Further Cyber-attacks can be divided into Active & Passive Attacks. In Cyber-attack, the attacker/intruder targets different IoT devices, by hacking the system to alter, delete, steal, or destroy the User's information. In a Physical attack, the attacker directly causes physical damage to IoT devices. Eg: Mobiles, cameras, routers, sensors, etc. Active Attacks: When an attacker access the network to interrupt certain user services, such attacks are called Active Attacks. Examples of active attacks are spoofing, hole attacks, DOS, Man-in-Middle, Sybil attacks, Jamming, and Data Tampering. [6]

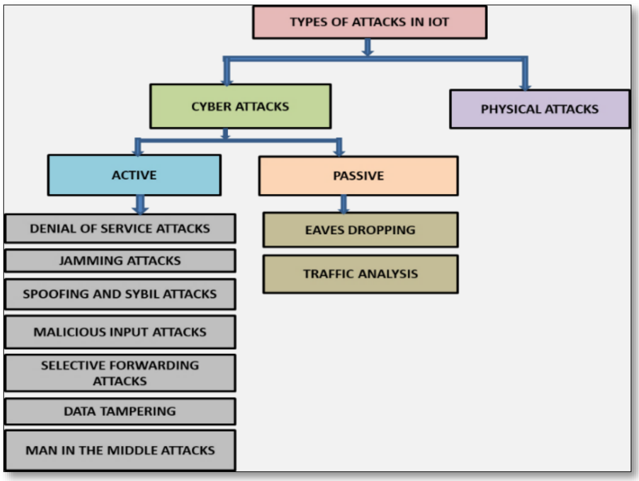


Fig. 5: Different Types of Attacks in IOT

3. Review of Literature

To arrive at and understand the research trend in the security aspects of the IoT using machine learning models, an initial survey is being conducted. The research focus is to explore the use of ML in the security domain so the further search is narrowed down to the use of ML for solving security problems in IoT, which is about 306 Journals within the timeline of 2010 till 2021. For research proposal writing selected papers including survey papers and other related work to the chosen problem domain is considered from 2016 to date. However, a closer look reveals the fact that the papers on security using machine learning are only from 2016 onwards.

Concerns regarding the risks to data security have exploded as a result of the growth of the IoT. Factors like vulnerabilities, denial-of-service attacks, viruses, and intrusion attempts affect IoT devices. The work carried out by [7] underlined the significance of high-quality training data for enhancing detection performance. The authors suggested a powerful IDS ("Intrusion Detection System") built on improved SVM ("Support Vector Machines") characteristics. The study's empirical findings, which focused on getting new and higher-quality SVM detection, demonstrated useful values including strong performance, a high detection rate, and few false positive alarms.

The authors in [7] discussed the IoT security architecture based on SDN (Software-Defined Networking). This work defines the operation of the security architecture and summarizes the opportunities for using SDN to implement network security more effectively and flexibly. In this article, self-organizing networks' network access control, as well as global traffic monitoring, are taken into consideration, various architectural design decisions of SDN utilizing OpenFlow are highlighted and their effects on performance are examined.

A recent survey discusses security issues, particularly about the IoT, and the integration of physical devices with the network as the integration of real-world devices into cyber security threats is brought about in most daily activities [8]. Attacks against vital infrastructure, like power plants and public transportation, may have disastrous effects on whole towns and nations.

The researcher explored a study regarding IDS methodologies for IoT and they also developed a taxonomy to categorize the papers utilized in the present research based on characteristics, detection technique, IDS deployment approach, security threat, and validation approach. It was also mentioned that the study of IDS approaches for IoT is still in its early stages and that the suggested solutions do not cover a broad variety of threats and IoT technologies. They also showed a classification method to categorize the papers utilized in the present study, which is based on detection approaches, attributes, IDS placement strategies, verification strategies, and security threats.

The author in [9] used three original-sized data sets called ISCX, KDDCUP99, and NSL-KDD for experimental purposes related to computer network intrusion detection. The study introduced an IoT/Fog network threat detection system based on distributed DL. Experiments show that artificial intelligence has been successfully applied for network security purposes. A system for attack detection in a distributed architecture with IoT uses (like smart cities) was also created and built by the author. Detection rate, false alarm rate, and accuracy are all performance measures used in the assessment process to compare the efficacy of the deep and shallow models.

Table 1

Citations	Year	Problem Context	Solution Approach	Dataset
[10]	2017	Attack Detection performance	SVM & logarithm marginal density ratio transformation	NSL_KDD
[11]	2015	Security Issue	Survey	---
[12]	2017	Security Issue, cyber threats	Survey	---
[13]	2018	Intrusion detection	Distributed deep learning	KDDCUP99, ISCX, and NSL-KDD
[14]	2018	Compromised Node Identification	decision trees	Customized Dataset

Another research work by [15]suggested an IDS based on the protocol model method and ML. The system contains 2 detection steps. In the 1st step, local identity, and network behavior data are gathered by devoted explorers to form a collection of properly classified examples using a supervised learning method based on decision trees. In the 2nd step, the global identities, the samples are aggregated by the super nodes to form time-based profiles, known as cumulative measures of volatility, for individual malicious & normal nodes.

In the [16] the authors introduce a deep autoencoder-based model for network attack detection. The investigators assessed their proposed work with KDD-CUP 99 dataset, and 94.71 percent of attack detection accuracy was attained. Their experimental findings demonstrated that their model outperformed deep belief networks in terms of performance.

In the work of [17], researchers presented a hybrid genetic algorithm and SVM as well as a DoS attack detection scheme based on particle swarm optimization. The investigators implemented their suggested scheme with KDD 99 data set and attained an accuracy of 96.38%. Another work towards the application of ML in IoT security successfully identified and categorized IoT attacks with Bayesian and SVM [18].

The KDD Cup99 dataset was used by the authors to develop their model, and they attained an accuracy rate of 91.50 percent. In [19], the author proposed a model based on a deep neural network and wavelet transform to identify false data Injection attacks. The investigators implemented their scheme by using IEEE 118 data set. The attack detection accuracy is 91.80%. In [20], an extreme learning approach for IoT intrusion detection based on linear discriminant analysis is suggested. The investigators employed the NSL_KDD data set to assess the accuracy of the suggested scheme. The accuracy they achieved is 92.35%. However, none of these approaches focused on improving computational efficiency and they have not shown either their method provides similar performance when the attacking scenario is changed.

There is no doubt that there has been a lot of research in the field of IoT security, but there are still many important issues that need to be solved.

- ➢ There is a lack of information in existing literature regarding the selection of suitable data sets for attack detection in the IoT environment. Most research uses the KDD_CUP and NSL_KDD data sets, which are outdated and are associated with simulation artifacts.

- There are few studies on the exploration of effective data sets in the preprocessing step.
- Most publicly available data sets lack the required functionality, lack proper labeling, incomplete network functionality, lack of original pcap files, and incomprehensible and/or incomplete CSV files.
- There is currently no standard research direction and guidance on the feature set that accurately distinguishes network traffic.
- Also, the existing research works lack providing information on what basis they selected particular machine learning techniques. It is unclear which datasets and intelligent techniques are most appropriate for designing an efficient and stable IDS for the IoT ecosystem. This requires an effective exploratory study.

Table 2

Citations	Year	Problem Context	Solution Approach	Dataset
[21]	2018	Attack detection	Deep-autoencoder	KDD-CUP 99
[22]	2018	Denial of Service Attack	The joint approach of Genetic algorithm & SVM, and Particle swarm optimization	KDD 99
[23]	2019	Attack detection and mitigation	SVM and Bayesian	KDD Cup99
[24]	2018	False data injection attacks	deep neural network and Wavelet transform	IEEE 118
[25]	2020	Intrusion detection	Extreme learning technique and linear discriminant analysis	NSL_KDD

4. Objectives of research work

- To conduct exploratory analysis on the available datasets.
- To design a preprocessing algorithm and carry out a feature engineering process to extract the final version of inputs to the security model.
- To design and develop a learning model for the identification of both known and unknown attacks.
- To conduct effective benchmarking over a suitable dataset and evaluate performance over the other similar existing methods

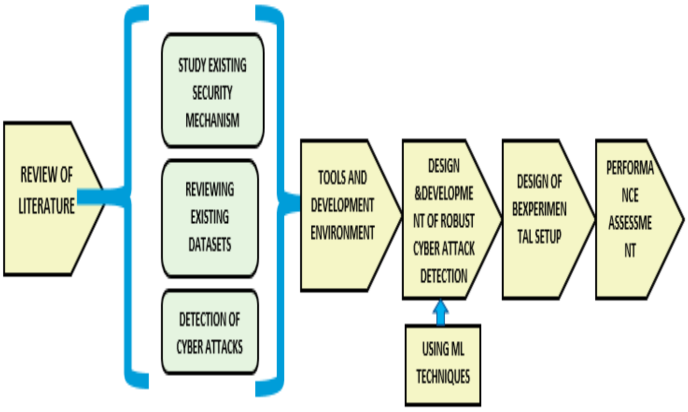

REVIEW OF LITERATURE
STUDY EXISTING SECURITY MECHANISM
REVIEWING EXISTING DATASETS
DETECTION OF CYBER ATTACKS
TOOLS AND DEVELOPMENT ENVIRONMENT
DESIGN &DEVELOPMENT OF ROBUST CYBER ATTACK DETECTION
USING ML TECHNIQUES
DESIGN OF BEXPERIMENTAL SETUP
PERFORMANCE ASSESSMENT

Fig 6: Flow of Methodology Adopted

Figure 6 shows the Overall Planning of Implementation of Proposed Study that we need to adopt. The work will be carried out in the following steps.

- In-depth Analysis of the existing literature to explore research trends and open issues.
- Comparative analysis of different security mechanisms and cyber-attack detection systems in the modern networking scenario like IoT.
- Study of the different datasets used in the proposed literature in the context of network security.
- Study different tools and development environments to select the suitable platform for research execution.
- Design and development of robust cyber-attack detection system using Machine Learning technique
- Design of experimental setup and performance assessment based on the simulation and other tools.

4.1 Methods

We utilize Python Scapy, an open-source Python library to gather the wireless network data and then extract features with the help of the suggested library depending on Scapy's built-in library support. The cyber security toolkit, CyberSecTK, is a simple Python package for preprocessing & feature extraction from data linked to cyber-security. Network packets are processed using Python Scapy functions.

4.2 Expected outcome

- Detection of known and unknown attacks in the wireless network.
- Higher accuracy and less false alarm rate in the detection process.
- Computationally efficient
- Comparative analysis with the existing security systems.
- To get a promising outcome against the attack on modern networking systems, thereby providing dynamic protection against various lethal attacks without much utilization of resources and improving network performances.

5. Conclusion

There is no doubt that there has been a lot of research in the field of IoT security, but still, there are so many important issues that need to be solved. There is a lack of information in existing literature regarding the selection of suitable data sets for attack detection. Furthermore, understanding which approaches are most appropriate for securing the IoT ecosystem is a challenging task owing to the involvement of a variety of devices and applications. The existing security schemes require modification and optimization in their design, development, and implementation process. Also, the existing research work lacks providing information on what basis they selected particular machine learning techniques. So, conducting exploratory analysis on the available datasets can be carried out further.

Need to design a preprocessing algorithm and carry out a feature engineering process to extract the final version of inputs to prepare advanced security models. To enhance security, designing and developing a learning model for the identification of both known and unknown attacks is still an open research challenge.

References

[1] C. V. S. V. J. D. P. a. S. B. Hassija V, A Survey on IOT security: application area ,security Threats and solutions architecture, vol. 7, IEEE Access, 2019, pp. 82721-82743.

[2] R. R. ,. S. T. Somayya Madakkam, “Internet Of Things,” Journal of Computer and Communications, vol. 03 No.05, 2015.

[3] A. A. K. a. R. M.Saharkhizan, “IEEE Internet Of Things Journal,” IEEE, vol. 7, no. 9, pp. 8852-8859, September 2020.

[4] M. H. D. H. Amine Khatib, “Intrusion Detection for Cyber Security In IOT Networks,” E3S Web of Conferences, vol. 297, 2021.

[5] H. K. S. Syeda Manjia Tahsien, "Machine learning based solutions for security of Internet of Things (IoT):A Survey," Journal of Network and Computer Applications, 2020.

[6] S. D. M. Francesco Redtuccia, "Securing the Internet of Things in the Age of Machine Learning and Software-defined Networking," IEEE Internet Of Things Journal, vol. 1, Jan 2018.

[7] G. C. N. F. panel Flauzac Olivier, "New Security Architecture for IoT Network," Procedia Computer Science, vol. 52, pp. 1028-1033, 2015.

[8] R. S. C. T. S. C. A. Bruno Bogaz Zarpelão, "A survey of intrusion detection in Internet of Things," Journal of Network and Computer Applications, vol. 84, pp. 25-37, 15 April 2017.

[9] N. C. Abebe Abeshu Diro, "Distributed attack detection scheme using deep learning approach for Internet of Things," Future Generation Computer Systems, vol. 82, pp. 761-768, May 2018.

[10] "An effective intrusion detection framework based on SVM with feature augmentation," Knowledge-Based Systems.

[11] G. C. N. F. Flauzac Olivier, "New Security Architecture for IoT Network," Procedia Computer Science, vol. 52, pp. 1028-1033, 2015.

[12] o. S. M. C. T. K. S. C. A. Bruno Bogaz Zarpel, "A survey of intrusion detection in Internet of Things," Journal of Network and Computer Applications, vol. 84, pp. 25-37, 15 April 2017.

[13] N. C. Abebe Abeshu Diro, "Distributed attack detection scheme using deep learning approach for Internet of Things," Future Generation Computer Systems, vol. 82, pp. 761-768, May 2018.

[14] A. Amouri, V. T. Alaparthy and S. D. Morgera, "Cross layer-based intrusion detection based on network behavior for IoT," 2018.

[15] A. Amouri and V. T. Alaparthy, "Cross layer-based intrusion detection based on network behavior for IoT," IEEE, April 2018.

[16] F. Farahnakian and J. Heikkonen, "A deep auto-encoder based approach for intrusion detection system," 20th International

Conference on Advanced Communication Technology (ICACT), pp. 178-183, 2018.

[17] K. E. Y. a. a. S. B. Mehdi Moukhafi, "A novel hybrid GA and SVM with PSO feature selection for intrusion detection system," International Journal of Advances in Scientific Research and Engineering (ijasre), vol. 4, no. 5, May 2018.

[18] M. K. ,. N. R. L. khalvati, "Intrusion Detection based on a Novel Hybrid Learning Approach," Journal of Artificial Intelligence & Data Mining (JAIDM), vol. 6, no. 1, pp. 157-162, March 2018.

[19] Y. H. a. V. O. K. L. J. J. Q. Yu, "Online False Data Injection Attack Detection With Wavelet Transform and Deep Neural Networks," IEEE Transactions on Industrial Informatics, vol. 14, no. 7, pp. 3271-3280, July 2018.

[20] Z. H. ,. O. N. W. a. P. C. Dehua Zheng, "An Improved LDA-Based ELM Classification for Intrusion Detection Algorithm in IoT Application," Sensors, vol. 20, no. 6, 19 March 2020.

[21] F. Farahnakian and J. Heikkonen, "A deep auto-encoder based approach for intrusion detection system," in 20th International Conference on Advanced Communication Technology (ICACT), 2018, 2018.

[22] K. E. Y. a. S. B. Mehdi Moukhafi, "A novel hybrid GA and SVM with PSO feature selection for intrusion detection system," International Journal of Advances in Scientific Research and Engineering (ijasre), vol. 4, May 2018.

[23] M. K. ,. N. R. L. khalvati, "Intrusion Detection based on a Novel Hybrid Learning Approach," The Journal of Artificial Intelligence & Data Mining (JAIDM), March 2018.

[24] Y. H. a. V. O. K. L. J. J. Q. Yu, "Online False Data Injection Attack Detection With Wavelet Transform and Deep Neural Networks," IEEE Transactions on Industrial Informatics, pp. 3271-3280, July 2018.

[25] Z. H. ,. O. N. W. a. P. C. Dehua Zheng, "An Improved LDA-Based ELM Classification for Intrusion Detection Algorithm in IoT Application," Sensors, vol. 20, no. 6, p. 1706, 19 March 2020.

[26] S. M. et.al, " Internet Of Things (IOT)," Journal of Computer and Communications, pp.164-173.

[27] A. a. X. H.Fang, “Fast Authentication and Progressive Authorization in Large scale IOT,” IEEE Network, vol. 34, no. 3, pp. 24-29, May/June 2020.

[28] M. B. M. A. O. M. H. E. F. Idriss Idrissi, “Intrusion Detection System For IOT,” IAES International Journal Of Atrificial Intelligence, vol. 10, no. 1, pp. 110-120, March 2021.

[29] N. Abebe Abeshu Diro, Ed.Future Generation Computer Systems, vol. 82, pp. 761-768, May 2018.

[30] F. F. a. J. Heikkonen, "A deep auto-encoder based approach for intrusion detection system," 2018 20th International Conference on Advanced Communication Technology (ICACT), pp. 178-183, Feb 2018.

[31] A. M. G. ,. S. Y. Y. O. a. O. E. Anahita Golrang, “A Novel Hybrid IDS,” Electronics 2020, vol. 9, no. 4, p. 577, 29 march 2020.

[32] S. Z. a. M. İskefiyeli, “Anomaly-Based Intrusion Detection From Network Flow,” IEEE Access, vol. 8, pp. 108346-108358, 2020.

[33] M. M. M. a. A. A. A.-R. M. Alsaeedi, “OpenFlow-SDN Flow Control,” IEEE Access, vol. 7, pp. 107346-107379, 2020.

[34] S. S.-H. M. B. A. W. a. N. R. L. Fawcett, “A Distributed SDN Framework for Scalable Network Security,” IEEE Journal on Selected Areas in Communications, vol. 36, no. 12, pp. 2805-2818, December 2018.

[35] J. ,. S. H.Wang, An effective Intrusion detection framework based on SVM with feature augmentation, vol. 136, Knowledge based system, pp. 130-139.

[36] J. H.Wang, "An effective Intrusion detection framework based on SVM with feature Augmentation," Knowledge Based Systems, vol. 136, pp. 130-139, 15 November 2017.

April 2023

Vol - 13 No - 4

@IJITCE Publication