JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A REVIEW ON CNN BASED ATTACK DETECTION IN IOT HEALTHCARE SYSTEM

Aditya Chauhan, Er. Harpreet Kaur
Research Scholar, Asst. Professor
Department of Computer Science & Engg.
Galaxy Global Group of Institutions, Dinarpur

Abstract- Cyberattacks in the Internet of Things (IoT) are growing exponentially, especially zero-day attacks mostly driven by security weaknesses on IoT networks. Traditional intrusion detection systems (IDSs) adopted machine learning (ML), especially deep Learning (DL), to improve the detection of cyberattacks. DL-based IDSs require balanced datasets with large amounts of labelled data; however, there is a lack of such large collections in IoT networks. This paper proposes an efficient intrusion detection framework based on transfer learning (TL), knowledge transfer, and model refinement, for the effective detection of zero-day attacks. The framework is tailored to 5G IoT scenarios with unbalanced and scarce labelled datasets.

Keywords: *Attack Detection, IoT, Healthcare system, CNN etc.*

I. INTRODUCTION

The Internet of Things (IoT) today uses IP-based communications to connect a wide range of devices, including sensors, to the Internet. IoT in the healthcare sector offers alternatives for remote monitoring, early detection, and medical care for institutionalized disabled people. For the Internet of Things, individuals or things can be outfitted with sensors, actuators, RFID tags, etc. Career access is made easier by such tools and tags. For instance, IoT applications can read, recognize, find, and control RFID tags on patients' or patients' personal equipment (including medical devices). IoT makes it possible for a wide range of intelligent services and apps to address the difficulties that people or the healthcare industry confront. IoT can link dynamically with D2M (Device-to-Machine), O2O (Object-to-Object), P2D (Patient-to-Doctor), P2M (Patient-to-Machine), D2M (Doctor-to-Machine), S2M (Sensor-to-Mobile), M2H (Mobile-to-Human), and T2R (Tag-to-Reader), for instance. To ensure an efficient healthcare system, this intelligently integrates people, machines, smart devices, and dynamic systems. The age group over 60 is growing faster than any other age group as a result of an increase in life expectancy. This might be viewed as a triumph for socioeconomic growth, healthcare services, and public health policy. It also poses a challenge to society, which must deal with a large increase in the number of impaired persons. By 2050, there will be 2 billion people over the age of 65 in the world, predicts the World Health Organization (WHO). The elderly who are disabled must continue to live independently in their own homes in order to prevent overburdening health care. This not only raises their standard of living but also lowers the cost to them, their families, and society as a whole. New functionality must be created and new technology must be integrated into residential environments due to demographic changes. The development of home automation systems aimed at enhancing disabled people's quality of life began decades ago. They started with basic capabilities that involved automating routine operations, including employing motion detectors to control lighting. The introduction of increasingly complex, intelligent systems is a natural by-product of technological advancement. Ambient Assisted Living (AAL) environments provide care and assist the disabled by integrating smart features and ambient intelligence (AmI) in the home. In essence, the same technologies can potentially target a different population segment with a small tweak.

This paper is ordered as follows: section II provides brief about sustainable use of energy. Section III describes the brief introduction about load forecasting. Section IV provides the related work based on this work. At last, conclusion is described in Section V.

II. ARCHITECTURE OF IOT

As shown in Figure, the IoT architecture is composed of numerous layers, starting with the edge technology layer at the bottom and ending with the application layer at the top. The two lower levels help with data collection, whilst the two higher layers are in charge of using data in applications.

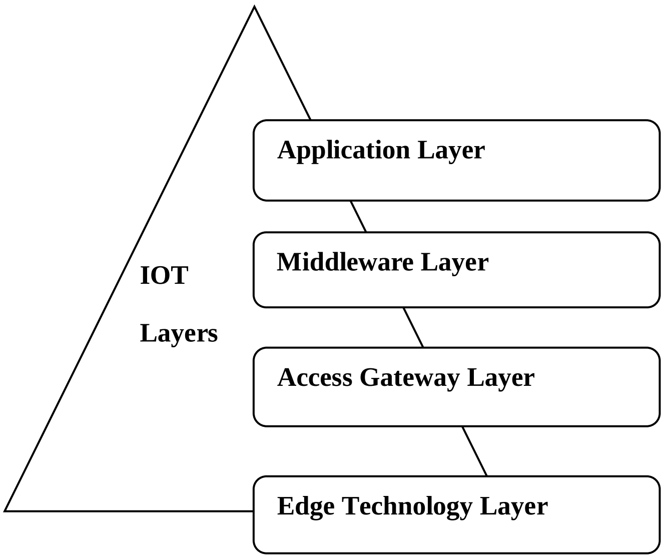

Fig 1: Layered Architecture of IoT [1]

The functions of the layers (from the bottom up) are as follows:

1) Edge Technology Layer

This is a layer of hardware that consists of devices for gathering data, such as wireless sensor networks (WSNs), RFID systems, cameras, intelligent terminals, electronic data interfaces (EDIs), and global positioning systems (GPS). These hardware parts enable identification and information storage (using RFID tags, for example), information collecting (using sensor networks), information processing (using embedded edge processors), communications, control, and actuation (using robots, for example), and more.

- **RFID systems**

They are the most crucial IoT elements. They make it possible for an RFID tag, a very portable device, to transmit data. The tag is read by an RFID reader, which then processes the data in accordance with the requirements of a particular application. Healthcare equipment can be tracked in real-time using RFID systems without having to be in direct line of sight. The tag may transmit data that includes location information, handicapped information (age, sex, blood pressure, glucose level, etc.), or device or disabled identity.

- **Wireless sensor networks (WSNs)**

A WSN may contain a large number of sensing nodes that transmit their findings to sinks, or specialized nodes.

2) Access Gateway Layer

This layer is in charge of handling data, which includes message publishing and subscribing, message routing, and data transport. Using communication methods like Wi-Fi, Li-Fi, Ethernet, GSM, WSN, and WiMAX, it transfers data received from the edge layer to the middleware layer.

3) Middleware Layer

It is a software platform that gives applications object abstraction. Additionally, it provides a wide range of services, including information discovery (using Electronic Product Code (EPC) or Object Naming Service (ONS)) and management, data filtering, data aggregation, and semantic data analysis.

4) Applications Layer

Various applications are delivered to various IoT consumers by this top layer. It has two below layers.

- **Data management sub-layer**

It offers machine-to-machine (M2M) services, directory services, Quality of Service (QoS), cloud computing technologies, data processing, etc.

- **Application service sub-layer**

It handles communication with end users and business apps that are running on top of the IoT applications layer.

III. IOT COMPONENTS

1. The Physical Objects IoT Component

They gather, recognize, and keep track of data on impaired people in their surroundings. This comprises equipment that tracks the vital indicators (blood pressure, heart rate, glucose, and daily activities) of impaired people. The physical gadgets are connected to the Internet, which transforms the information about the disabled that was gathered in the real world into information for the digital world.

2. The Communication Technologies IoT Component

Personal Area Networks (PANs), Local Area Networks (LANs), and Wide Area Networks (WANs) are the most prevalent network types for IoT healthcare applications for the disabled. Various wireless technologies are used in each type of network. The IoT healthcare applications most typically employ the following communication technologies:

- **ZigBee**

It is the Low-Rate Wireless Personal Area Network (LR-WPAN)-based IEEE 802.15.4 standard for low power and short range. It uses the 2.4 GHz ISM (Industrial, Scientific, and Medical radio) band and is less expensive than Bluetooth.

- **Bluetooth**

It is the IEEE 802.15.1 standard for low-power short-distance radio frequency, which is based on Wireless Personal Area Network (WPAN), which works in the 2.4 GHz ISM band and can support point-to-point and point-multipoint topologies. Bluetooth devices are inexpensive, and Bluetooth Low Energy (BTLE, BLE, OR LE) technology, also known as Bluetooth Smart or Version 4.0+, is aimed, among other things, at novel healthcare applications. It greatly reduces power consumption (running for "months or years" on a button cell).

- **Light Fidelity (Li-Fi)**

Similar to Wi-Fi, it is an optical Visible Light Communication (VLC) system that employs light rather than radio waves and the TCP/IP protocol. VLC transmits data using brief visible light pulses between 400 THz (780 nm) and 800 THz (375 nm). Li-Fi employs LED lamps with transceiver fittings to transmit and receive data while also lighting up the room. The LED transmits data (1 for on and

0 for off), which are picked up by photoreceptors and transformed to digital data there. Li-Fi has security problems with network coverage and dependability. In terms of reliability, the interaction from external light sources, such as sunshine or regular bulbs, will cause disturbance in the communication line. Li-Fi cannot send data in an area where there are walls or trees even when there is network coverage? Since the signal does not pass through walls, Li-Fi has no room for eavesdropping and many other benefits. Additionally, because there is no electromagnetic interference in VLC, Li-Fi does not have the issue of overlapping frequencies that arises when utilizing Wi-Fi for medical devices. As a result, radio waves can be used for an MRI scanner while Li-Fi can be used in a room to monitor patients.

- **Wi-Fi**

IEEE 802.11x (also known as Wireless LAN or WLAN) is one of numerous Wi-Fi variants. Wi-Fi uses the non-interoperable Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), and Infrared (IR) technologies. Both point-to-point and point-multipoint topologies are available. Using 2.4 GHz or 5 GHz RF bands, IEEE 802.11n offers good performance with a maximum data rate of 600 Mbps. Multiple Input Multiple Output (MIMO) technology can be used to make the most of the available bandwidth. In the healthcare industry, 802.11a, b, and g are also still in use. The following protocols can offer Wi-Fi security.

- **Long Term Evolution (LTE)**

The Third Generation Partnership Project (3GPP) created a 4G wireless broadband standard based on WWAN. LTE offers downlink (DL) and uplink (UL) data rates of up to 300 Mbps each. LTE provides a practical, affordable option for IoT M2M applications in the healthcare sector, such as monitoring and tracking of patients and medical equipment.

- **Long Term Evolution-Advanced (LTE-A)**

A substantial improvement over LTE, it is a "true" 4G mobile communication technology that offers up to three times the data throughput of LTE. Lower latency, 1.5 Gbs (DL), and 3 Gbs (DL). Upgraded M2M services should be able to utilize current LTE networks thanks to LTE-A's expected backward compatibility with LTE hardware.

IV. LITERATURE SURVEY

Anand A et al. [2021] [9] highlighted that the 5G-IoT has a significant role in e-health applications and has become indispensable in smart applications. For e-health applications to successfully combat security threats against patients' sensitive data, sophisticated architectures and schemes are required. Applications for e-healthcare keep data in the cloud, which makes it susceptible to security breaches. These threats can, however, be recognised using deep learning methods, which calls for hybrid models. In this paper, a new deep learning model (CNN-DMA) based on a CNN (Convolution Neural Network) classifier is suggested to detect malware threats. Three layers—Dense, Dropout, and Flatten—are used in the model. Twenty epochs, 25 classes, and 64 batch sizes are utilised to train the network. The first convolutional layer uses an input image. Results are obtained using the Malimg dataset, which contains input from 25 families of malware that our model has identified as malware. The suggested model CNN-DMA is validated using cutting-edge methods and is 99% accurate.

According to **Aljumah A. et al. [2021] [10],** linked items produce enormous amounts of data traffic in the information and communication technology age, allowing data analysis to reveal hidden trends and identify anomalous network-load. We list five fundamental design ideas that should be taken into account when creating an intrusion detection system (IDS) that uses deep learning. Based on these ideas, we suggested the Temporal Convolution Neural Network (TCNN), an intelligent model for IoT-IDS that combines generic convolution and convolution neural network (CNN). Synthetic minority oversampling is used to accumulate TCNN in order to manage unbalanced datasets with nominal continuity. Additionally, it is applied in combination with efficient feature engineering methods like attribute transformation and reduction. Using the Bot-IoT data repository, the given model is contrasted with two conventional machine learning methods, random forest (RF) and logistic regression (LR), as well as LSTM and CNN deep learning techniques. The results of the studies show that TCNN consistently strikes a good compromise between efficacy and performance. It is superior to other deep learning IDSs since it has a multi-class traffic detection feature.

According to **Young L. et al. [2021] [11],** network intrusion detection systems are crucial for safeguarding sophisticated communication networks. These systems were first hard-coded to recognise particular signatures, patterns, and rule breaches; however, artificial intelligence and machine learning algorithms increasingly provide viable substitutes. However, a variety of out-of-date datasets and a wide range of different evaluation measures are employed in the literature to demonstrate algorithm effectiveness. This work aggregates algorithms for various setups to provide a common denominator and suggests two new assessment measures. Together, both metrics—the detection score and the identification score—reliable present the functionality of a network intrusion detection system and enable broad-based practical comparison. We also provide a method for converting raw packet row data into machine learning input features. With the help of this framework, numerous algorithms can be swiftly implemented for various datasets, and their performance can be systematically compared. Our experimental results, which are on par with or better than the state-of-the-art, show the promise of our strategy. Raw traffic input features hold potential for use in real-time deep learning-based systems since they are significantly simpler and less expensive to extract than conventional features.

The Internet of Things (IoT) is experiencing an exponential increase in cyberattacks, particularly zero-day attacks, which are primarily motivated by security flaws in IoT networks, according to research by **Rodrguez E. et al. [2022] [12].** To enhance the detection of assaults, traditional intrusion detection systems (IDSs) adopted machine learning (ML), particularly deep learning (DL). IoT networks do not typically include balanced datasets with substantial amounts of labelled data, which is a need for DL-based IDSs. In order to effectively detect zero-day assaults, this research suggests an intrusion detection architecture based on transfer learning (TL), knowledge transfer, and model refining. The framework is designed to operate with 5G IoT scenarios that include sparse and unbalanced labelled datasets. On convolutional neural networks (CNNs), the TL model is built. The framework was tested for its ability to identify numerous zero-day attacks. Three specialized datasets were produced with this in mind. The suggested TL-based framework achieves good accuracy and a low false prediction rate (FPR), according to experimental data. These results show that TL is effective in the detection of cyberattacks in IoT environments with superior detection rates for the different families of known and zero-day threats than any previous DL-based IDS.

The application of deep learning in multiple models is a valuable tool in detecting Internet of Things (IoT) assaults and recognising new types of intrusion to access a better secure network, according to research by **Farhan B et al. [2022] [13].** The use of IoT and the type of data it produces, which leads to an increase in attacks, has increased the necessity for any intrusion detection system to be developed in order to identify and categorise attacks in an acceptable time and automated manner. Malicious assaults are constantly evolving and producing new ones. In this paper, we give a survey on the identification of anomalies and intrusion by separating legitimate and malicious behaviours while examining network data to find novel threats. This paper reviews prior work by assessing the performance of those studies using two categories of new real-traffic datasets (i.e., CSE-CIC-IDS2018 and Bot-IoT datasets). We demonstrate accuracy measurement for intrusion detection in several systems to assess performance.

The Internet of Things (IoT) has emerged as a popular paradigm to meet business demands for asset tracking, resource monitoring, and automation, according to **Kodys M et al.[14].** IoT devices are increasingly vulnerable to sophisticated intrusion assaults because security safeguards are frequently overlooked while they are being deployed. Over the past ten years, the cyber security community has deployed artificial intelligence (AI) to automatically detect these assaults. However, for Intrusion Detection Systems (IDS) specifically for IoT, deep learning techniques have not yet been thoroughly investigated. The majority of recent research relies on time sequential models like LSTM, and there is a dearth of work on CNNs because they are not well-suited to this issue. In this work, we suggest a unique countermeasure to CNN-based intrusion attacks on IoT devices. Convolutional procedures are used to encrypt the data in order to record sensor data patterns over time that can be used by CNNs to detect threats. The proposed approach is combined with two traditional CNNs, ResNet and Efficient Net, where the performance of detection is assessed. In comparison to the baseline utilizing LSTM, the experimental results demonstrate a considerable improvement in both true positive rate and false positive rate.

According to **Indira B. et al. [2022] [15],** Internet of Things (IoT) devices communicate with one another directly. Due to the network layer's design in their architecture and the fact that they are always linked to the internet, they are more vulnerable. Life-saving data is produced by IoT-based smart healthcare equipment like hospital patient monitoring cameras, which must be secured against attackers. Due to the enormous amount of data generated by the IoT, effective intrusion detection is necessary to protect sensitive private data before an attack occurs. In this study, a 5-layered architecture is suggested for detecting intrusion in sizable datasets. The learning rate and imperceptions during learning by the machine model are increased in this study by creating additional bespoke features. Recurrent Neural Networks with Long Short-Term Memory in both directions are utilized to identify the attack to optimize the prediction performance accuracy by using the IoTID20 dataset to defend IoT networks. The suggested ACAAS method acquires significant characteristics. The experiment's results showed an accuracy rate of 99.16%, an error rate of 0.008371%, a sensitivity ratio of 99.89%, and a specificity ratio of 98.203% for IoTID20 with unique features. The system's efficiency in preventing network intrusions is demonstrated by the high accuracy rate.

Denial of Service (DoS/DDoS) assaults are carried out to knock down a target by flooding it with worthless traffic, according to **Malliga S et al. [2022] [16].** The nature and traits of these attacks need to be carefully investigated because DoS/DDoS attackers frequently alter their attack tactics and patterns. The issue of creating methods to identify this threat is difficult. In recent years, the development of intrusion detection solutions has largely benefited from deep learning. Significant efforts have been made in recent years to build deep learning models to combat DoS/DDoS threats. In this paper, we present a taxonomy of DoS/DDoS assaults and techniques for DoS/DDoS detection based on deep learning. The article then addresses the major features of the most recent (as of 2016) defensive strategies against DoS/DDoS assaults that take advantage of deep learning techniques. Since datasets are essential for deep learning techniques, we also examine historical and modern datasets that have DoS/DDoS attack traces in them. The review article conclusions are also summarized, and they call for more work to be done to reinforce the current state-of-the-art approaches to dealing with the attackers' unpredictable behaviour. It also draws attention to the imbalances in the papers under study. We conclude by outlining a few crucial research areas that will require extra attention in the near future in order to guarantee strong protection against DoS/DDoS attacks utilising deep learning methods.

The IoT-cloud ecosystem is one of the most difficult and demanding tasks today, according to **Shitharth S et al. [2022] [17].** However, the IoT-cloud framework is more prone to vulnerabilities and assaults, which reduces the security level of the network by engaging in malicious activities. This is because it is built with a huge number of sensors that are used to generate a tremendous amount of data. Due to its best-in-class capacity to increase data security and dependability, artificial intelligence (AI) technology is the greatest choice for healthcare applications. This leads to the implementation of various AI-based security procedures in the traditional works for the IoT-cloud architecture. However, it has serious issues with increasing algorithm complexity, ineffective data handling, inability to interpret unstructured data, higher costs for IoT sensors, and greater time consumption. In order to increase the security of healthcare data stored in IoT-cloud, this study suggested Probabilistic Super Learning- (PSL-) Random Hashing (RH), an AI-based intelligent feature learning technique. Additionally, this study aims to lower the cost of IoT sensors by putting the suggested learning model into practise. In this case, the training model has been kept up to date with the reported attack's attributes in order to learn more about the characteristics of attacks. Additionally, the usual Elliptic Curve Cryptography (ECC) method for data security is combined with the random key generation process, which is based on the data matrix's hash value. Then, using the created random hash key, the upgraded ECC-RH mechanism executes the data encryption and decryption processes.

According to **Mohammadpour L et al. [2022] [18],** Internet applications have improved and have a large user base. The requirement for secure Internet networks has grown as a result. Network security must be ensured by intrusion detection systems (IDSs), which use artificial intelligence (AI) techniques. Deep learning (DL) algorithms as a subfield of AI are currently successfully used in IDSs. The convolutional neural network (CNN) is a well-known structure created for processing complicated data in deep learning neural networks. The CNN, which is mostly utilised in IDSs, overcomes the typical constraints of conventional machine learning algorithms. IDSs use a variety of CNN-based techniques to address privacy concerns and security vulnerabilities. To the best of our knowledge, there aren't any thorough studies of IDS methods that have used CNN. In order to better understand the numerous ways the CNN can be used to identify network intrusions, abnormalities, and other sorts of assaults, our study's main focus is on CNN-based IDSs. This research creatively categorises the investigated CNN-IDS techniques into various groups and outlines their main strengths and contributions. The primary characteristics of these methods are contrasted, including dataset, architecture, input shape, evaluated metrics, performance, feature extraction, and classifier technique. The experimental outcomes of CNN-IDS research are not comparable because different datasets are utilized. In order to assess various methodologies using common datasets, this study also conducted an empirical experiment, and the results are reported in detail.

Software-Defined Networking (SDN) is the next generation to transform the architecture of conventional networks, according to **Radhi M et al. [2022] [19].** One of the possible approaches to alter the design of internet networks is SDN. Because SDN design is centralised, attacks are more frequent. Security must be provided for the SDN. In this paper, we provide a strategy for SDN that uses a Network Intrusion Detection System-Deep Learning module (NIDS-DL). The approach we propose integrates a variety of deep learning methods with Network Intrusion Detection Systems (NIDS). Utilising a feature selection method, our methodology selects 12 features from a total of 41 features in the NSL-KDD dataset. Classifiers (CNN, DNN, RNN, LSTM, and GRU) were used. Our method obtained accuracy results of (98.63%, 98.53%, 98.13%, 98.04%, and 97.78%) when we compared classifier scores. Our unique method (NIDS-DL) uses five deep learning classifiers and pre-processes the dataset to yield the best outcomes. The fact that our suggested method for binary classification and attack detection worked well suggests that our method (NIDS-DL) could be applied with great effectiveness in the future.

The biggest problems with the Internet of Things, according to **Morteza R. et al. [2023] [20],** is security. The Internet of Things today plays a significant role in both information technology and everyday life. Security is one of the biggest problems with the Internet of Things. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are two typical ways to interfere with Internet of Things services. Therefore, the primary and most comprehensive components of a network monitoring system at the moment are intrusion detection systems, or IDSs. In order to detect distributed denial of service assaults and other cyberattacks, this study presents an intrusion detection model for software-driven Internet of Things networks based on deep neural networks using the CICIDS 2017 data set. In addition, we investigated CNN, DenseNet, CNN and LSTM hybrid models, as well as our own model, as efficient deep learning models to represent cyber security information in Internet of Things networks.

According to **Shaoul E et al. [2023] [21],** as internet of things (IoT) devices evolve quickly, cyberattacks are becoming more frequent and more intense. Recent reports indicate that distributed denial of service (DDoS) and denial of service (DoS) attacks are the most frequent ones against IoT networks. Because firewalls, intrusion detection systems, and other traditional security measures often filter both traffic and stop it in accordance with the principles specified first, they are unable to detect DoS and DDoS attacks. However, when used in conjunction with technologies based on artificial intelligence, these solutions can be successful and efficient. Deep learning models, particularly neural networks, have drawn a lot of interest recently because of how well they perform when processing images. This convolutional neural network (RNN) model can be used to detect sophisticated DDoS and DoS attacks, among other types of attacks. To analyse network data comprising negative data and train the RNN state model, a type of neural network data, we therefore suggest a method in this study. The plan achieves 99.99% accuracy in DoS and DDoS detection in the case of dual deployment. Additionally, the suggested strategy outperformed the most recent technology by 98% in accurately identifying different DoS and DDoS attack patterns.

V. PROBLEM FORMULATION

Over the previous decades, the developing technologies in IoT are continuously progressing which incorporating IT frameworks into physical components leads to security implications on water treatment plans, gas pipelines and smart grids. An IoT system usually focuses on availability rather than confidentiality and integrity. Normal and attack operation misclassification can restrict the network availability. Hence, the principle provides an opportunity for attacks and enables the system to be at risk. In recent years, the number of cyber-attacks has increased and securing the technologies and system is not an easy task, as can be demonstrated from the existing research. The existing research shows that ICS has been transformed into a hotspot for intrusion, attacks, vulnerabilities and threats. Promising solutions are expected from research into attack detection on IoT dataset.

VI. CONCLUSION

Traditional intrusion detection systems (IDSs) adopted machine learning (ML), especially deep Learning (DL), to improve the detection of cyberattacks. In this paper, we investigate the feasibility of deploying transfer-learning-based intrusion detection for zero-day attacks in IoT networks with scarce and unbalanced datasets. To this end, it developed an efficient intrusion detection framework that combines knowledge transfer and model refinement, with excellent detection accuracy for known and novel cyberattacks families. This work basically reviews the IoT healthcare dataset using CNN and will check the performance in terms of accuracy.

REFFERENCES

[1]. N. Uchenna, C. Chukwuma, (2012), “Improving Security and Privacy of Internet of Things In Healthcare”, Research Gate, 01-07.

[2]. H. Zakaria, N. Bakar, (2019), “IoT Security Risk Management Model for Secured Practice in Healthcare

Environment", Information Systems International Conference, 1241–1248.

[3]. S. Tsimenidis, T. Lagkas, (2020), "Deep Learning in IoT Intrusion Detection", Journal of Network and Systems Management, Vol 30, Issue 8, 07-47.

[4]. C. Shiranthika, N. Premakumara, H. Chiu, (2020), "Human Activity Recognition Using CNN & LSTM", IEEE Explore, pp. 01-06.

[5]. P. Pandey, S. Pandey, (2020), "Security Issues of Internet of Things in Health-Care Sector: An Analytical Approach", Algorithms for Intelligent Systems, 307-330.

[6]. S. More, J. Singla, (2020), "Security Assured CNN-Based Model for Reconstruction of Medical Images on the Internet of Healthcare Things", IEEE Access Journal, Vol 8, 126333- 126346.

[7]. S. Srinivasa Gopalan, Dr A. Raza, (2020), "IoT Security in Healthcare using AI: A Survey", IEEE Explore, 01-06.

[8]. L. Xu, X. Zhou (2021), "Intelligent Security Performance Prediction for IoT-Enabled Healthcare Networks Using Improved CNN", Journal of Latex Class Files, 01-10.

[9]. Anand, A.; Rani, S.; Anand, D; Aljahdali, H.M.; Kerr, D. (2021), "An Efficient CNN-Based Deep Learning Model to Detect Malware Attacks (CNN-DMA) in 5G-IoT Healthcare Applications", Sensors Journal, 21, 6346.

[10]. A. Aljumah, (2021), "IoT-based intrusion detection system using convolution neural networks", PeerJ Comput. Sci., 01-19.

[11]. L. Jeune, T. Goedemé, (2021), "Machine Learning for Misuse-Based Network Intrusion Detection: Overview, Unified Evaluation and Feature Choice Comparison Framework", IEEE Access, Vol 9, 63995- 64015.

[12]. Rodríguez, E.; Valls, P.; Otero, B.; Costa, J.J.; Verdú, J.; Pajuelo, M.A.; Canal, R. (2022), "Transfer-Learning - Based Intrusion Detection Framework in IoT Networks". Sensors 22, 5621.

[13]. B. Farhan, A. Jasim, (2022), "Survey of Intrusion Detection Using Deep Learning in the Internet of Things", Iraqi Journal for Computer Science and Mathematics, Vol. 3 No. 1, p. 83-93.

[14]. M. Kody, Z. Lu, K. Fok, (2022), "Intrusion Detection in Internet of Things using Convolutional Neural Networks", Journal for Computer Science and Mathematics, Vol. 3 No. 1, p. 01-10.

[15]. D.V. Jeyanthi, B. Indrani, (2022), "IoT Based Intrusion Detection System for Healthcare Using RNNBi LSTM Deep Learning Strategy with Custom Features", Research Square, 01-21.

[16]. Malliga, S., Nandhini, P. S., Kogilavani, S. V. (2022). "A Comprehensive Review of Deep Learning Techniques for the Detection of (Distributed) Denial of Service Attacks". Information Technology and Control, 51(1), 180-215

[17]. A. Khadidos , S. Shitharth, (2022), "Healthcare Data Security Using IoT Sensors Based on Random Hashing Mechanism", Hindawi Journal of Sensors Volume 5, p. 01-17.

[18]. Leila Mohammadpour, Teck Chaw Ling, (2022), "A Survey of CNN-Based Network Intrusion Detection", Appl. Sci. 12, 8162.

[19]. M. Radhi Hadi and A. Mohammed, (2022), "A Novel Approach To Network Intrusion Detection System Using Deep Learning For SDN: Futuristic Approach", Journal of Sensors Volume 5, p. 69-83.

[20]. R. Morshedi, S. Matinkhah, (2023), "Intrusion Detection for IoT Network Security with Deep Neural Network", Research Square, 01-23.

[21]. E. Shaoul, Prof. S. Sonare, (2023), "IoT Network attack detection and Classification using Standardized Recurrent Neural Network model", International Journal of Advances in Engineering and Management (IJAEM), Volume 5, Issue 5, pp: 157-164.