Anomaly-based Intrusion Detection System for IoT Networks through Deep Learning Model

Tanzila Saba[1], Amjad Rehman[1*], Tariq Sadad[2], Hoshang Kolivand[3], Saeed Ali Bahaj[4]

[1]Artificial Intelligence & Data Analytics Research Lab (AIDA) CCIS Prince Sultan University Riyadh,11586, Saudi Arabia.

[2]Department of Computer Science & Software Engineering, International Islamic University, Islamabad, Pakistan

[3] School of Computer Science and Mathematics, Liverpool John Moores University, Liverpool, UK and School of Computing and Digital Technologies, Staffordshire University, Staffordshire, UK

[4] MIS Department College of Business Administration, Prince Sattam bin Abdulaziz University, 11942, Alkharj 11942, Saudi Arabia.

***Crossponding author rkamjad@gmail.com**

Abstract:

The Internet of Things (IoT) idea has been developed to enhance people's lives by delivering a diverse range of smart interconnected devices and applications in several domains. However, security threats are main critical challenges for the devices in an IoT environment. Many approaches have been proposed to secure IoT appliances in state of the art, still advancement is desirable. Machine learning has demonstrated a capability to detect patterns when other methodologies have collapsed. One advanced method to enhance IoT security is to employ deep learning. This formulates a seamless option for anomaly-based detection. This paper presents a CNN-based approach for anomaly-based intrusion detection systems (IDS) that takes advantage of IoT's power, providing qualities to efficiently examine whole traffic across the IoT. The proposed model shows ability to detect any possible intrusion and abnormal traffic behavior. The

model is trained and tested using the NID Dataset and BoT-IoT datasets and achieved an accuracy of 99.51% and 92.85%, respectively.

Keywords: IoT; Intrusion detection; Deep learning; Anomalies; Technological development; Smart village

1. Introduction

The IoT facilitates individuals interacting with real-world applications over the internet in the IoT environment. Recent innovations in IoT have added computers, sensors, buildings, streets, and even communities to the impression of smartness. IoT devices operate in different environments to accomplish several goals; result in the variety of computational devices and communication technologies utilized in education, healthcare, agriculture, military, and commerce. It makes enormous contributions to almost every industry in modern society, such as surveillance, agriculture, medicine, etc. Furthermore, IoT is an interconnected system based on approved protocols that exchange knowledge [1]. Additionally, the diverse domains of appliances lead to the realization of several communication standards, devices, and protocols. Therefore, IoT is often referred to as the Internet of People (IoP) since it is used by almost everyone in their daily lives, from individuals to institutions.

There is a continuous rise in connected devices around the globe. Multiple sensors are included in embedded systems, allowing them to remotely gather real-time data from physical items. The data acquired from the devices enable us to create intelligent decision-making algorithms and effectively manage IoT settings. However, the link to the Internet of widely used real-world devices often raises questions about cybersecurity threats. Consequently, IoT device protection against anomalies is a major concern for institutions and countries. All necessary actions must measure the physical security and cybersecurity against significant attacks of the IoT architecture,

which needs to be confirmed. In addition, a thorough analysis of the network protection is required [2].

Due to resource constraints and complexity, traditional intrusion detection technologies are not secure enough for the Internet of Things (IoT). Therefore, there is a need to design and build smart intrusion detection techniques for IoT devices to protect them against attacks from compromised IoT devices. However, considerable computational power and storage are required for most intrusion detection systems [3].

This research is organized into four main sections. Section 2 presents the background and motivation of this research along with the main contributions. Section 3 details the materials and methods in detail. Section 4 exhibits the experimental results on two benchmark datasets. Finally, section 5 concludes this research.

2. Background

Due to the emergence of various anomalies, IoT systems face different security vulnerabilities than conventional computer systems. Firstly, IoT systems are quite varied in terms of devices, platforms, communication methods, and protocols. Second, IoT systems comprised of internet-connected components and control devices which are deployed to link physical structures. Thirdly, there are no well-defined boundaries in IoT systems which regularly change due to the mobility of individuals and devices. Fourthly, IoT systems or a component of them would be physically endangered. Fifthly, implementing sophisticated security mechanisms and software on IoT devices is often difficult due to its limited energy. Finally, because of the fast growth of IoT-based devices, such networks may be exposed to assaults on their privacy and security [4].

Several methods and frameworks have been developed to alleviate network attacks using machine-learning and deep-learning techniques by identifying anomalies in the IoT system.

Literature reports several state-of-the-art techniques to classify these anomalies using machine learning techniques in the IoT infrastructure. Still, a few have used deep learning techniques for the same purpose. Deep learning techniques have proven to be the best for pattern matching and could detect any IoT environment input as true or invalid requests. ID attacks can be classified into four major categories: signature-based methods, specification-based methods, anomaly-based approaches, and hybrid strategies [1].

Signature-based approaches first look for similarities between a collection of network data and a database containing features. The data will be treated as a violation of the law if the scanned data matches the signature database. This is very useful to decide on the type of attack accurately. It is a low labor-intensive and relatively demand-free operation. They allow the rules and thresholds to be defined in advance by the system managers. The existing guidelines will be followed, detects the current device and network status. The IDS will sense a rare condition and respond accordingly if the threshold is surpassed or the rules are broken [5].

Anomaly-based approaches focus on discovering which patterns are normal or abnormal. The benefit of detecting intrusions using this approach is identifying new possible intrusions. One drawback of this approach is that it is susceptible to false positives. Machine learning algorithms in anomaly-based intrusion detection methods are being researched to enhance their benefits. Machine learning algorithms can use anomaly-based intrusion detection techniques to track active behavior and compare them with established intrusion footprints to remain alert to possible future attacks. Hybrid approaches employ different identification methods in the same scheme. This approach will remove the vulnerabilities of a single process and provide better reliability to the entire IoT system.

However, the fully formed IDS would be incredibly broad and complicated. This will make the entire system more complex and need more resources. Since several protocols are involved, intrusion detection would take a lot of time and resources [6]. Diro et al. [7] proposed anomaly detection in IoT data using deep learning and it was demonstrated to be more effective than a traditional IDS for detecting IoT Fog coordinated attacks. Vigneswaran and Poornachandran [8] implemented an anomaly-based IDS which operates in conventional networks. It also used the KDDCup99 dataset to train and test the model. The suggested solution offers 95% precision and should be implemented. However, they used the KDDCup99 dataset, which lacks homogeneous data and few unique records. This makes it difficult to derive accurate results. Ajaeiya and Adalian [9] recommended anomaly-based IDS that only use the features of the network. Using different machine learning models, an R-tree algorithm produces the best results, with a 99.5% true positive rate and a 0.001 percent false-positive rate. Their findings demonstrated the usefulness of using statistical algorithms like Random Forest. However, their dataset is not a benchmark, which creates validity issues. Abubakar and Pranggono [10] suggested an identification method that works in SDN. The method consists of a signature-based ID and an anomaly-based ID that uses the NSL-KDD dataset for training and testing. The detection accuracy is higher than 97.4%. However, the intrusions detected only by anomaly detection cannot be differentiated from signature detection. Tang and Mhamdi [11] proposed an anomaly-based security architecture for SDN using only a given feature set. The researchers compared the effects of several machine learning approaches. Classifying images using a deep neural network with three hidden layers produced a 76% level of accuracy.

Kapitnov et al. [12] proposed a blockchain technology protocol to allow peer-to-peer communication for connected networks. The protocol helps to ensure the security of the contact

mechanism and handles heterogeneity in the working states. The field is currently investigating incorporating blockchain into a multi-agent scheme. Li et al. [13] proposed an improved strategy to extract IoT data features to detect IDS for smart cities using deep migration learning. They also claimed that their strategy would also cover the lack of a suitable training set. They also claimed that their methodology improved detection rates with a high level of performance compared to traditional methods, effectively reducing the clustering time. Hajiheidari et al. [14] introduced a deep learning model for intrusion detection in IoT. A structure for a feature engineering method has been developed to intelligently select intrusion features to reduce the dimension of the feature vector. This is an important factor in intrusion detection. The next move was to create and train multiple IDSs using the selected functions. The learning phase was performed using various profound learning methods, such as recurring neural networks (RNN). Two databases were used with intrusion footprint records with a very high classification accuracy.

Arshad et al. [3] presented an improved system for intrusion detection for resource-constricted IoT devices. Accordingly, IoT devices and the edge router are isolated from intrusion detection. To search network packets, IoT devices are employed as IDS nodes. However, it is limited in receiving raw packets from the host router node as they contain confidential information. Anthi et al. [2] suggested a three-layer IDS architecture for genuine time-destroying actions in domestic IoT gadgets. In this design, the security layers classify intrusions of the IoT systems according to their usual or unusual behavior.

2.1 Why IoT Protection is Necessary

In this research work, we were determined to find techniques in IoT environments to learn the various scenarios and vulnerabilities of IoT applications [15]. Furthermore, the following basic

security principle should be measured while strengthening an effective IoT security strategy. Thus, establishing an effective IoT security system was the research motivation of this manuscript.

a. Confidentiality

This is an essential element of protection for IoT networks. IoT devices can move and save precise information that is not necessarily illegitimately discovered by individuals. However, individual data, patient privacy, armed forces, and corporate information are unusually organized and demand to be tested against illegitimate users [16].

b. Integrity

Data across IoT devices is usually moved through remote communication and it must be changed in genuine ways. In this approach, reliability is a major concern when ensuring that a powerful monitoring tool is in place to recognize any modification during communication around an untrustworthy remote system.

c. Authentication

The IoT architecture requires a robust authentication mechanism that varies from one framework to another to provide strong protection instead of flexibility. Therefore, trade-offs are a significant challenge when creating an authentication design, such as considering the safety and security aspects in IoT employment while designing an authentication plan.

d. Authorization

The authorization provides privileges to the clients of an IoT framework. As a result, clients may utilize the people, systems, or administration information collected with the help of computing devices. This ensures that security is maintained according to the people, components, devices, and power resources involved [17].

e. Availability

IoT frameworks should be constantly available to authorized users for administrative and communication tasks. Accessibility is a key component of an effective organization of IoT frameworks. IoT devices can be made unavailable through several threats, for example, active jamming or DoS. Therefore, ensuring the continued availability of IoT processing to its users is an essential element of IoT security.

f. IoT Threat

Security attacks may be categorized as real or virtual. Thus, attacks on the internet can also be classified as passive or active [7, 18].

g. Passive Attacks

Usually, the attackers are hidden and the latent risk is engaged by observing the communication line to collect information from the appliance, the appliance owners, or both. Passive threats observe and monitor the information to use them for specific targets. Such a threat does not affect the instrument assets, and the data will stay unaffected. The user cannot see the presence of passive threats as it is performed furtively. Such a threat aims to get data or examine the vulnerabilities of the instrument. The most common sort of passive threat is eavesdropping. This is employed to snip info during communication between two machines over the internet and it is used for traffic analysis to take the network traffic information for future analysis.

Furthermore, some threats have occurred owing to the exponential interconnection of uncertain gadgets in IoT environments. These are wireless sensor networks-based and protocol-specific, for example, the RPL (Routing protocol for low-power and lossy networks) protocol [19]. Using this protocol in IoT instruments and avoiding traditional protocols is resource-constrained.

This aspect raises its openness to security threats and privacy concerns because it cannot employ standard protocols for secure transmission. Despite this, they are still being implemented without proper security arrangements.

h. Active threats

These attacks involve the skillful eavesdropping of the correspondence paths and the modification or altering of the IoT structures to control the system resources, as presented in Figure 1. Active attacks create damage and attempt to disrupt and interrupt the instrument. The users are notified regarding the active threat. This kind of threat will put their availability and integrity at risk. An active threat is difficult to achieve compared to a passive threat.

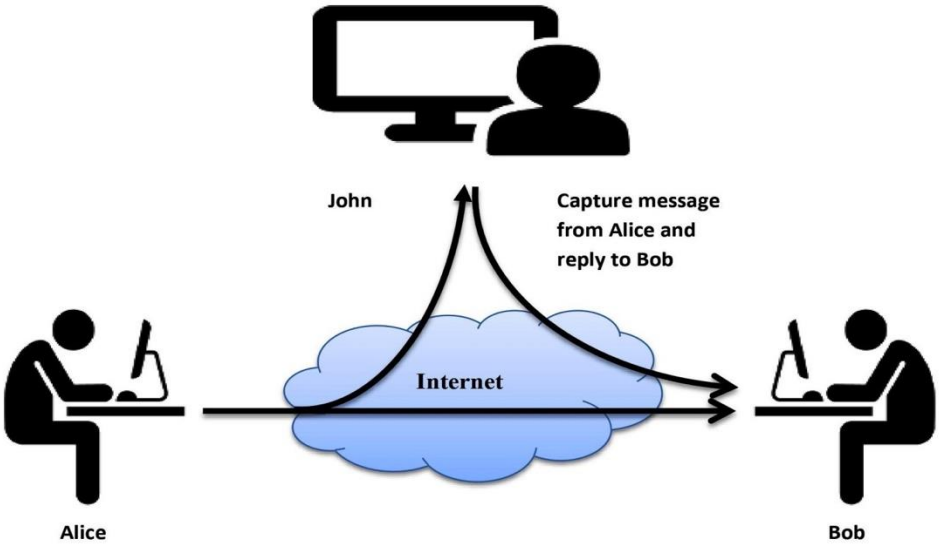

Figure 1. Active attack example

A Denial-of-Service attack (DoS) is a common example of an active threat that could be employed against an IoT. A DoS attack occurs when intruders take control to shut down an instrument. This will prevent authentic users from retrieving the specific appliance. Instead, the intruders will flood the focus machine with traffic until it does not reply or until it crashes. For example, buffer

overflow sends progressively heavier traffic to the machine beyond the threshold that a buffer can manage, causing a system crash.

Moreover, ping flood, also termed ICMP flood, is a kind of flooding attack. The disturbed services often include online bank accounts, websites, or emails. A DoS threat can be made from any place without difficulty. As has already been discussed, most smart systems such as the gadgets used in health systems, transportation systems, homes, cities, and wearable devices run on low-power and lossy networks, making it challenging to guarantee secure communication. This raises the risk of being attacked by intruders and other harmful things. Therefore, IoT requires arrangements for detection mechanisms and secure communication systems to support their practical and valuable implementation [20].

To summarize, nothing is fully secure in IoT appliances. This allows the users to retrieve their data without difficulty in the IoT environment. Despite this, it generates an unprotected climate for the intruders to retrieve any network segment. Figure 2 demonstrates the various dimensions of threat in an IoT environment. Users should be mindful of all IoT appliances' security flaws to defend themselves from cyber threats. Several approaches and structures to lessen the network threats have been formed. For example, machine learning can help to detect logs and classify attacks on an extensive network.

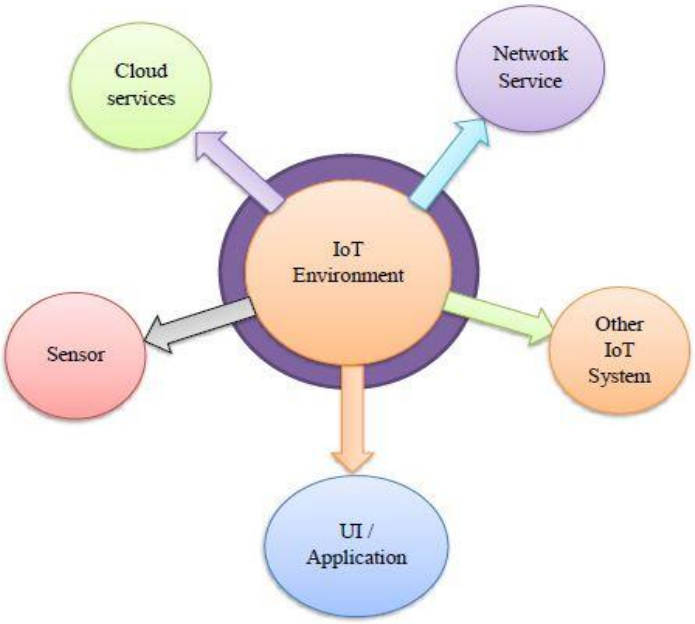

Figure 2. Threat dimensions of the IoT environment

2.2 Motivation

Since IoT devices operate in an interconnected and interdependent environment, new threats constantly emerge. Moreover, as IoT devices typically operate in an unattended environment, an intruder may maliciously access these devices. Eavesdropping can access privately-owned information from the communication channel because IoT devices are usually linked through wireless networks. In addition to these security issues, IoT devices cannot afford to incorporate advanced security features because of their limited energy and processing power. Therefore, an added line of protection should be built into IoT networks to defend IoT-based organizations from cyber threats. Deep learning techniques have recently become more credible in a popular application for detecting network assaults, like IoT networks. Deeply trained systems in IoT environments will mainly catch anomalous and benign behavior. IoT devices and network traffic could be registered and examined to learn the normal patterns. Irregular comportments can be

identified where they deviate from the normal pattern. These approaches have also been tested to predict new threats and provide comprehensive IoT device and network security protocols.

The main contribution of this work is to

- Categorize the attacks through the deep-learning method by employing existing datasets.
- Propose a framework to add IDS as a program within IoT networks.
- Design a protection strategy for the IoT network to maintain its integrity and seamlessly make it available to legitimate users.

3. Material and Methods

3.1 IDS and Deep Learning for IoT Security

IDSs mainly contain evidence of an attack in a data-gathering module and analysis module of attack detection. The IoT systems' input data in the data gathering module was investigated to find the behavior of interaction using various machine learning techniques in the analysis module. Deep learning has gained prominent achievements in different areas and has proven a better option than conventional machine learning. Additionally, IDS using deep learning has encouraging results. Deep learning-based approaches are more influential and suitable for traffic analysis to determine the normal and abnormal traffic in an IoT environment. Moreover, deep learning techniques can intelligently predict new attacks, unlike previous threats [21]. Figure 3 presents IDS using deep learning models in the IoT environment.

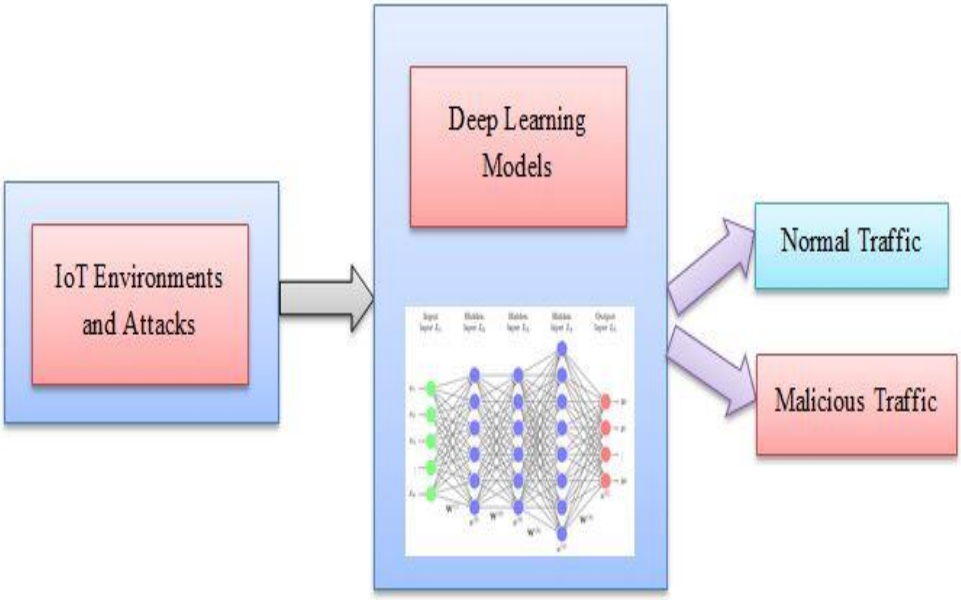

Figure 3. IDS using deep learning models

a. BoT-IoT Dataset

We employed a BoT-IoT dataset [22] for experiments. It was created at the Cyber Range Laboratory in UNSW Canberra Cyber. Different virtual machines connected to the LAN were used. PFSense firewall server was also installed in the linked VMware cluster via WAN interfaces to test bet configuration of the BoT-IoT dataset. Most of the researchers utilized this dataset to evaluate the data characteristics of the network. The dataset was divided into categories and subcategories based on the attacks [23]. The attacks are included in the dataset as presented in Table 1.

Table 1: Possible intrusion detection attacks on ports in the IoT environment

Grouped	Attack	Port
Denial of service	DoS	HTTP, TCP, UDP
	DDoS	HTTP, TCP, UDP
Information collecting	Reconnaissance (service scan, OS Finger Print)	
Information theft	Keylogging, theft	

b. Network Intrusion Detection (NID) Dataset

This dataset involved an extensive diversity of intrusions simulated in an armed forces environment [23]. It creates an environment to acquire raw TCP/IP data for a network by imitating a US Air Force LAN. The LAN set-up is as in a real-world setting to handle various attacks. For each TCP/IP connection, 41 features are acquired from malicious and normal data as presented in Figure 4. The category of the variable has been classified as both normal and anomalous.

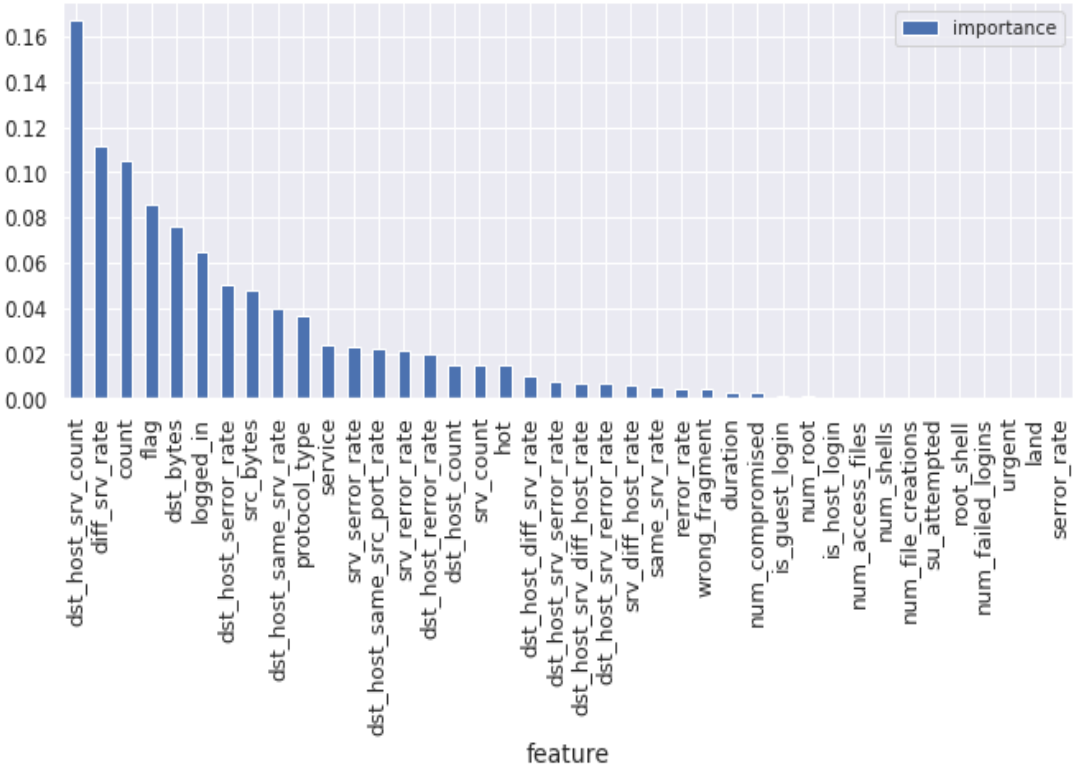

Figure 4: Features of the NID dataset

c. Convolutional Neural Network (CNN)

A CNN involves an input, multiple hidden layers, and an output layer like ANN. The information components are reduced by sharing a parameter, equivariant representation, and sparse connections. Diminishing links amid the layers extends the scalability and increases training time [21]. The sequential model of CNN is employed using the parameters illustrated in Table 2.

Table 2: Proposed deep learning model parameters.

Name	**Parameter**
Loss	Categorical cross-entropy (for multi-class)
	Binary cross-entropy (for binary class)
Optimizer	Adam
Dropout	0.5
Test size	0.2
Batch size	10
Shuffle	True
Epochs	30

4. Experimental results

The goal of this assessment is to determine the CNN model's outcome. The experiments were conducted using the proposed deep learning model on publicly available benchmark datasets. The standard metrics were employed to evaluate the model performance and examine their accuracy [24,25].

4.1 Performance evaluation using the NID dataset

The NID dataset contains 25,192 records that are used for training the model. The model is validated using 20% of the training data, i.e. 5,039 records are validated and acquired an overall accuracy of 99.51%. It was further evaluated through a confusion matrix as presented in Figure 5. Finally, the training and validation accuracies are illustrated in Figure 6.

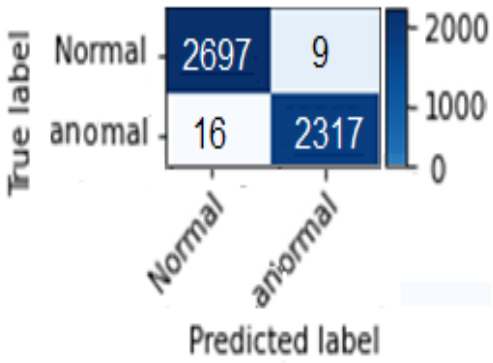

Figure 5: Confusion matrix of the NID Dataset

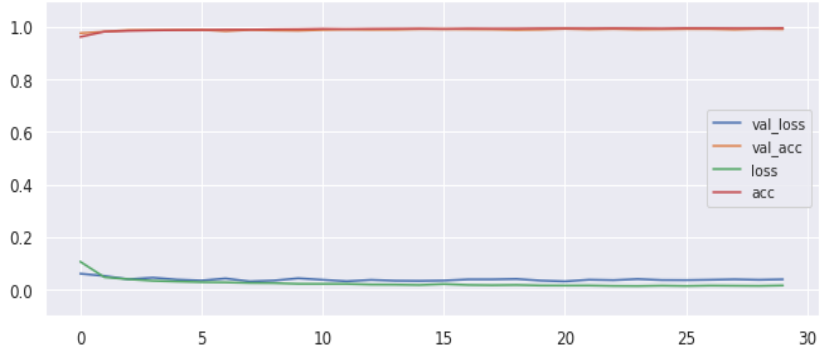

Figure 6: Training and validation accuracies on NID dataset

4.2 Performance evaluation using BoT-IoT dataset

The CNN model used the BoT-IoT dataset which contains multi-class, DoS, DDoS, Reconnaissance and Normal records. The data was splitted into a training and testing ratio of 80-20% and achieved a 95.55% accuracy. Furthermore, the results were also evaluated using a confusion matrix, as presented in Figure 7. The results displayed in Figure 7 demonstrated that 86.18%, 99.97%, 100% and 100% were achieved using the DDoS, DoS, Normal, and Reconnaissance traffic, respectively, through the BoT-IoT dataset. Moreover, the training and testing accuracies are illustrated in Figure 8.

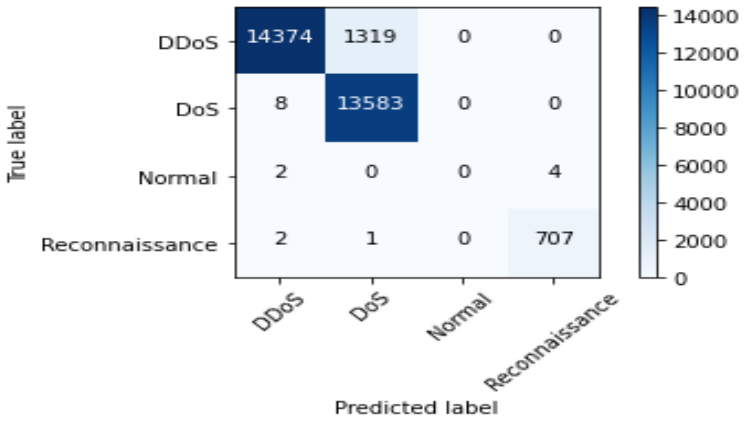

Figure 7. Confusion matrix of the BoT-IoT Dataset

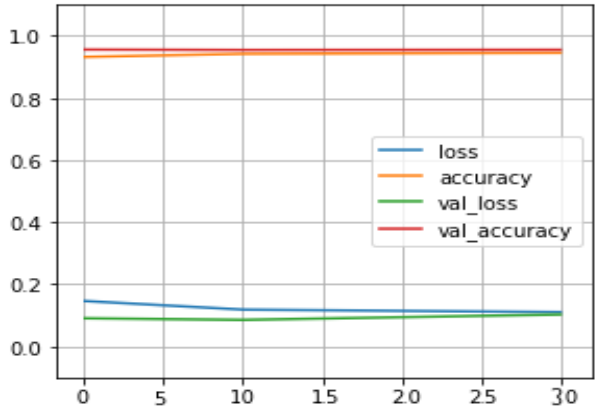

Figure 8: Training and validation accuracies on BoT-IoT dataset

The experiments display the effectiveness of the proposed model in the IoT environment. However, it could be improved by using different epochs, batch sizes, and a number of parameters.

5 **Conclusion and future work**

Many cybersecurity research studies have been conducted on IoT networks' security and privacy issues. However, the mildest method to counteract these threats depends on the circumstances.

This paper presented a convolutional neural network (CNN) based model to improve the IoT network's performance and security. We have investigated a deep-learning model in an IoT network for IDS was investigated. The proposed CNN-based model had also examined the traffic across the IoT to predict any possible intrusion and anomalous traffic behavior. The proposed model was trained and tested using the NID and BoT-IoT datasets and achieved 99.51% and 95.55% accuracy, respectively. We believe that significant research is still required for advancements in IoT to have a better threat detection rate with their progression in the industry. It is essential to build and design the security procedures inside and outside the IoT appliances because the IoT networks will be the core element. We intend to develop methods using various algorithms and to use numerous deep learning algorithms in the future.

Declaration: Authors declare no conflict of interest for this publication.

Acknowledgement

This work was supported by the research SEED project "Content Based Information Retrieval using RGB Channels, Shape Vectors based Sampling, Scoring and Scaling with Coefficient Formation." Prince Sultan University, Riyadh Saudi Arabia, (SEED-CCIS-2021{76}) under Artificial Intelligence & Data Analytics Research Lab. CCIS". The authors are thankful for the support.

References

[1] Tahaei, H., Afifi, F., Asemi, A., Zaki, F., & Anuar, N. B. (2020). The rise of traffic classification in IoT networks: A survey. Journal of Network and Computer Applications, 154, 102538.

[2] Anthi, E., Williams, L., Słowińska, M., Theodorakopoulos, G., & Burnap, P. (2019). A supervised intrusion detection system for smart home IoT devices. IEEE Internet of Things Journal, 6(5), 9042-9053.

[3] Arshad, J.; Azad, M.A.; Abdeltaif, M.M.; Salah, K. An intrusion detection framework for energy-constrained IoT devices. Mech. Syst. Signal Process. 2020, 136, 106436.

[4] Al-Hamar, Y., Kolivand, H., Tajdini, M., Saba, T., & Ramachandran, V. (2021). Enterprise Credential Spear-phishing attack detection. Computers & Electrical Engineering, 94, 107363.

[5] Saba, T., Sadad, T., Rehman, A., Mehmood, Z., Javaid, Q. (2021). Intrusion Detection System Through Advance Machine Learning for the Internet of Things Networks. IT Professional, 23(2), 58-64.

[6] Saba, T. (2020, December). Intrusion Detection in Smart City Hospitals using Ensemble Classifiers. In 2020 13th International Conference on Developments in eSystems Engineering (DeSE) (pp. 418-422). IEEE.

[7] Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems, 82, 761-768.

[8] Vigneswaran, R. and Poornachandran, P. "Evaluating shallow and deep neural networks for network intrusion detection systems in cybersecurity," in 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Bengaluru, 2018.

[9] Ajaeiya, G. and Adalian, N. "Flow-Based intrusion detection system for SDN," in 2017 IEEE Symposium on Computers and Communications (ISCC), Heraklion, 2017.

[10] Abubakar, A. and Pranggono, B. "Machine learning-based intrusion detection system for software-defined networks," in Seventh International Conference on Emerging Security Technologies (EST), Canterbury, 2017.

[11] Tang, T. and L. Mhamdi, L. "Deep learning approach for network intrusion detection in

software-defined networking," in International Conference on Wireless Networks and Mobile Communications (WINCOM), Morocco, 2016.

[12] Kapitonov, A.; Lonshakov, S.; Krupenkin, A.; Berman, I. Blockchain-based protocol of autonomous business activity for multi-agent systems consisting of UAVs. In Proceedings of the Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS), Linkoping, Sweden, 3–5 October 2017; pp. 84–89.

[13] Li, D.; Deng, L.; Lee, M.; Wang, H. IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning. Int. J. Inf. Manag. 2019, 49, 533–545.

[14] Hajiheidari, S., Wakil, K., Badri, M., & Navimipour, N. J. (2019). Intrusion detection systems in the Internet of things: A comprehensive investigation. Computer Networks, 160, 165-191.

[15] Elrawy, M. F., Awad, A. I., & Hamed, H. F. (2018). Intrusion detection systems for IoT-based smart environments: a survey. Journal of Cloud Computing, 7(1), 1-20.

[16] Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 65-88.

[17] Bate, K. O., Kumar, N., and Khatri, S. K. (2018). Framework for authentication and access control in IoT. 2nd International Conference on Telecommunication and Networks, TEL-NET 2017.

[18] Kaur, S., & Singh, M. (2020). Hybrid intrusion detection and signature generation using Deep Recurrent Neural Networks. Neural Computing & Applications, 32(12).

[19] A Almusaylim, Z., Jhanjhi, N. Z., & Alhumam, A. (2020). Detection and mitigation of RPL rank and version number attacks in the internet of things: SRPL-RP. Sensors, 20(21), 5997.

[20] Fatima-Tuz-Zahra, Jhanjhi, N. Z., Brohi, S. N., & Malik, N. A. (2019). Proposing a Rank and Wormhole Attack Detection Framework using Machine Learning. MACS 2019 - 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics.

[21] Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (IoT) security. IEEE Communications Surveys & Tutorials, 22(3), 1646-1685.

[22] Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B. (2019). Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-IoT dataset. Future Generation Computer Systems, 100, 779-796.

[23] https://www.kaggle.com/sampadab17/network-intrusion-detection

[24] Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. IEEE Access, 7, 41525-41550.

[25] Khan, A. Y., Latif, R., Latif, S., Tahir, S., Batool, G., & Saba, T. (2019). Malicious insider attack detection in IoTs using data analytics. IEEE Access, 8, 11743-11753.

Authors short bio

Mrs. Tanzila Saba

Research Prof. Tanzila Saba earned PhD in document information security and management from Faculty of Computing Universiti Teknologi Malaysia, Malaysia in 2012. She won best student award in the Faculty of Computing UTM for 2012. Currently, she is research prof. in CCIS Prince Sultan University Riyadh Saudi Arabia. Her primary research focus in the recent years includes security, bioinformatics, classification.

Mr. Amjad Rehman is a Senior Researcher in the AIDA Lab CCIS Prince Sultan University Riyadh Saudi Arabia. He received his PhD & Postdoc from Faculty of Computing Universiti Teknologi Malaysia in information security with honor in 2010 and 2011 respectively. He received rector award for 2010 best student in the university. His interests are in information security, health informatics, pattern recognition.

Mr. Tariq Sadad received the M.S. and Ph.D. degrees in computer science from International Islamic University, Islamabad. Currently, he is a Lecturer with the Department of Computer Science and Software Engineering International Islamic University Islamabad. His research interest includes, machine learning, image processing, health-informatics and decision support systems.

Mr. Hoshang Kolivand received his PhD from Media and Games Innovation Centre of Excellence (MaGIC-X) in Universiti Teknologi Malaysia in 2013. He has completed his Post-Doctoral in Augmented Reality in UTM. Currently he is reader in Liverpool John Moores University. He has published numerous articles in international journals, conference proceedings and technical papers, including chapters in books.

Mr. Saeed Ali Bahaj is Associated Professor in the Department of Computer Engineering at Hadramout University and also Assistant Professor at Prince Sattam bin Abdul-Aziz. He earned doctoral at Pune University India in 2006. His main research interests include information management, forecasting, information engineering and information security.