Date of publication JUN-30, 2024, date of current version JUN-06, 2024.
www.computingonline.net / computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.23.2.3546

Improved Intrusion Detection in the Internet of Things: A Multi-Layered Neural Network Approach and Analysis

MANSOOR FAROOQ[1], FAHEEM AHMAD[2]

[1]Department of Management Studies, University of Kashmir, Srinagar,190006, India
[2]Department of Information Technology, University of Technology & Applied Science, Musanna, Oman

Corresponding authors: Mansoor Farooq (e-mail: khmansoor003@gmail.com), Faheem Ahmad (e-mail: faheem.ahmad@utas.edu.om)

ABSTRACT The (IoT) Internet of Things is a complex notion that refers to the interconnection of several individual devices over a network (IoT). The data gathered by these interconnected devices have the potential to have far-reaching consequences for human society, the economy, and the environment. The IoT is especially vulnerable to a variety of vulnerabilities in hostile environments like the internet. High-end security solutions are not adequate to safeguard an IoT system due to adequate storage and less processing capabilities. This emphasizes the need for ascendable, strewn, and robust smart security solutions. In this study, IoT networks are safeguarded depleting a multiple-layered security strategy centered on deep learning. The proposed architecture employs the use of three intrusion detection datasets CIC-IDS, BoT-IoT, and ToN-IoT to weigh the performance of the insinuated multiple-layered approach. Irrevocably, compared to 92% accuracy for the existing methodologies, the new layout obtained 98% accuracy.

KEYWORDS Deep Learning; IDS; KNN; IoT; Machine Learning; Artificial Intelligence.

I. INTRODUCTION

THE Internet of Things (IoT) is now seeing rapid product releases and high expectations from the IT community. It is rapidly growing and linking the billions of devices for everyday use. According to Gartner [1], there will be over 25 billion linked devices by 2020. Everyday life is made easier and problems are solved more creatively thanks to the internet of things. However, critical security concerns and privacy trade-offs [2] overshadow the immense advantages and potential presented by IoT technology. Assembling elucidations for the Internet of Things presents a plethora of difficulties, including the steep quantity of networked devices, the complexity, the existence of opposing drifts, and the eclectic gamut of factors that must be coped. Current security measures are inadequate for anything but very short sessions, even on very powerful machines [3].

The same safeguard cannot be used for extended periods of time. These features made IoT devices attractive to cybercriminals, who then threatened our safety by exploiting vulnerabilities [4]. Developing effective security solutions that are both lightweight and easily adopted might be a practical approach to dealing with the complexity of the Internet of Things [5]. In order to resolve discrepancies in extremely large dispersed networks, "adaptive lightweight" solutions have proven themselves time and time again. As the number of Internet-connected gadgets grows, it becomes more and more challenging to ensure the privacy and safety of each one. In an IoT network, data security is more important than ever [6, 7].

As a result of the AI ability to process data of all shapes and sizes, innovative IoT system solutions may now be provided. Machine learning and data analytics methods are presently being used to analyze massive volumes of IoT data in an effort to improve customer service and network efficiency. In this research, we suggest a tiered approach to IoT security. Deep learning techniques were utilized to oversee the IoT network in edict to categorize activities as "normal" or "malware" for each layer of the architecture after building a foundation utilizing the intrusion detection datasets from the CIC-IDS, BoT-IoT, and ToN-IoT.

Even though deep learning is still being researched in the IoT industry, especially when it comes to IoT security, it has a huge amount of potential to learn from IoT data. With some strategic deep learning, we believe IoT solutions can be significantly improved. Scorning the intricacy of the neural network topologies, frivolous functionality for IoT solutions may be achieved by changing the hyperparameters. As a result, we postulated that the ideal approach to improving IoT network security would be to employ deep learning ideas.

The main objectives of the research are to investigate safety issues related to the Internet of Things and intention of robust security architecture for the Internet of Things transport layer. In order to truly grasp the significance of security in today's interconnected world, it is necessary to use artificial intelligence to sift through the massive amounts of heterogeneous data that must be investigated. There are several deep learning algorithms available, but the research challenge requires one that can learn from the past. For this reason, we have decided to use neural networks in our study.

II. RELATED WORK

This section discusses the ideas and technology behind the (IoT) Internet of Things, as well as the risks and concerns associated with it. The merits that have to be considered while forming the security options for the Internet of Things are also highlighted. This section elaborates on the technologies used for network intrusion detection and security. To elucidate the significance of ML and DL in IoT security, we lay out the network architecture and provide examples. It is only possible because of several technologies combining to produce the Internet of Things. Sensor smart technologies, radio frequency identification and nanotechnologies all play important roles in the (RFID) Internet of Things. RFID devices are wireless microchips that can be used to instantly and uniquely tag and identify things. These devices can wirelessly identify an item that is beyond the line of sight by using tags to sense and detect the channel. RFID technology is used in credit cards, automobile keys, and many other contemporary devices. RFID technology must be used for the Internet of Things to benefit from mobile nodes and create intelligent system [9].

The (IoT) Internet of Things is a reality made possible by devices like smart appliances, smartphones, and other wearable technologies that can adapt and have consistent network performance. Smart technologies give access to the resources of the IoT system and boost the processing power of the network [10]. Intricate IoT systems rely on nanotechnologies, and these advancements have the potential to shape the future of AI-powered problem solving. For example, in metropolitan areas, Nano sensors may be used to monitor the extent of infectious diseases. The Internet of Things (IoT) has copious benefits for society, but it also rears momentous privacy and security issues. Due to its dependence on real world applications and the fact that the overwhelming bulk of IoT devices are left unattended sans any form of censoring, the IoT system poses serious privacy and security issues. In the Internet of Things, infrastructure, networks, hardware, and user interfaces are all susceptible [11].

In the IoT, it is hard to set up security for each device because there are so many and so different kinds of devices in the network. Network infiltration attempts may be spotted by keeping an eye on the data flowing over the network. If you are worried about the safety of your Internet of Things (IoT) gadgets, you may want to look at network-based elucidations instead. In order to acquire access to an IoT network and have its data and security safeguarded, devices must first be registered. All incoming and outgoing data from each device has to be monitored, and a standard procedure for the movement of data through a network needs to be established. Network data that does not follow the norm triggers an alarm and notifies the owners of the device [12].

Network security may be improved with the help of an intrusion detection system, a specialized piece of software that monitors networks and systems for malicious activity. There are several distinct categories of IDS. Based on their responsiveness, IDS are classified as either "active" or "passive" [13]. You may also classify the IDS based on where you want to install it. Intrusion detection systems (IDSs) are known as network intrusion detection systems (NIDSs) whilst deployed on a local area network (LAN) and as host-based intrusion detection systems (HIDSs) when installed on individual computers. Host-based IDSs have a number of flaws and may not be suitable for academic study [14].

Deep learning and machine learning differ significantly in many crucial areas, one of which is how well each works with increasing data sizes. Deep learning methods need more data to uncover network patterns than do machine learning techniques. Deep learning may also be cast off to investigate multi-modal Internet of Things data [15]. Because IoT devices are often linked for extended periods of time, traditional machine learning algorithms are unable to provide reliable, long-term results. The topologies of the underlying deep neural networks used in the approach may have a major effect on its efficacy [16]. Adding more and more layers to a neural network produces a more complex structure known as a multilayer network. This technique has several applications [17], including the work with high-dimensional data, weather prediction, and voice recognition. Multi-layered neural networks show their best performance when all of their layers have the same hyper parameters, weights, and biases.

III. METHODOLOGY

IoT solutions need to be portable, layered, scalable, and flexible. They should also be able to learn from past experiences. We created a novel IoT network structure to decrease the amount of data that the IDS classifier needs to process. For our trials, we selected the CIC-IDS, BoT-IoT, and ToN-IoT Intrusion Detection Datasets [18]. We performed feature engineering using a decision tree classifier to choose the most informative characteristics. We performed extensive analyses and generated the required data before feeding it into the model. In an IoT system made up of a diverse set of incompatible devices, multimodal data is sent over time. We found that the following three factors are required for effective management of IoT systems.

Some IoT gadgets have outdated operating systems that cannot handle antimalware programs. They lack the processing power to execute sophisticated malware prevention mechanisms and the storage capacity to accommodate ever-expanding malware databases. When developers install security solutions, they increase their ability to issue security updates and congregate data on the performance of devices, which allows them to evaluate whether or not more services or products are needed to boost implementation.

IoT end devices, with their wide range of capabilities, need a distribution strategy that is composed of many tiers inside the IoT architecture. The fact that the system can manage devices and data on numerous levels is one of the reasons why it is properly constructed. Processes may run at varying degrees of complexity, from the most advanced to the most fundamental, thanks to a distributed, multilayered architecture. In an Internet of Things (IoT) system, a single-layer architecture might not let you place or use the best range of components.

When compared to more conventional portable consumer products, IoT devices have a wider range of maintenance requirements. It might be costly to keep tabs on the upkeep of

the IoT setup over time. Furthermore, when used for extended periods of time, security systems ought to be able to accommodate emerging malware hazards.

A. REFINED RESEARCH DESIGN

Because of the conditions stipulated above for an Internet of Things security solution, we have devised the architecture to ensure the safety of intrusion detection activities. Constructing a topology for a neural network serves as an example of how feature extraction may be accomplished in an Internet of Things network. This topology shows how many layers the network has, as well as how many neurons are in each layer and how they are connected to each other. Forward propagation, equipped with a perceptron classifier and an activation function, is used by the artificial neurons. Once implemented, IDS will collect any data passing through a network node and label it as "attack" or "regular," keeping a log of each. Smart IoT network systems are inherently diverse; hence this approach may not work. Therefore, we developed a multi-layered neural network architecture that improves with age.

A centrally managed IDS system requires sufficient processing speed and memory to handle data from all connected devices. With so many devices spread out in such a dispersed area, it would be impossible for an IoT network to operate efficiently. We designed the architecture that allows four IDSs to function as a unified system-wide IDS in response to malware assaults that target the transport layer. Each IDS located at a different transport tier stores just the data it has gathered from devices at its own layer. Since the system is sharing the network load, response times will improve. The neural layers are shown in Figure 1, and the multilayered security architecture is shown in Figure 2.

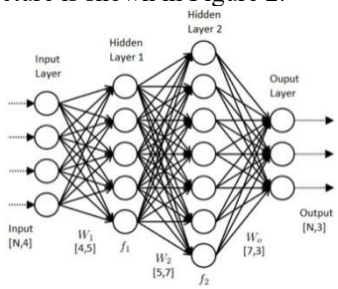

Figure 1. Artificial Neural Network

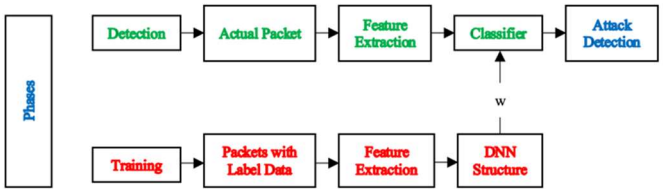

Figure 2. Multiple layered Design for IoT Networks

When training and evaluating an algorithm, it is essential to use only the most relevant information. It has been shown that a decision tree classifier is the most effective method for feature selection and dimensionality reduction [19]. The decision tree makes use of tree-based algorithms that rank the importance of characteristics according to their potential to improve node purity (Gini impurity). First, we visually displayed the significance of each feature before feeding the top ten characteristics from each dataset into the model. To facilitate faster model training and deployment, we decreased the input data 90 features to 10. This made the model more flexible and adaptable.

B. ALGORITHM

1. Train model set as input.
2. Initialize the feature ordering set f [] and its elements f0, f1, f2…. fn to initial value.
3. The classifier for the decision tree has been trained.
4. The F-test (also known as analysis of variance) is useful for determining the traits of a single variable.
5. Limit the notch for the ranking.
6. The feature with the least number of cores ought to be found.
7. Update feature set f.
8. Remove any remaining components from f.
9. End for.
10. Output: Set f for feature sorting.

Datasets. Popular datasets include CIC-IDS, BoT-IoT, and ToN-IoT. Data was collected over four weeks for the exam, whereas data for training was collected over ten weeks. More than 840 samples of IoT packet traffic and 95 types of network-based assaults are included in the whole dataset. All packets in the network are labelled as "regular" or "attack," depending on the nature of the assault. You can find all three versions of the dataset, as well as links to them, in a fount on the Kaggle website. Among these three, the CIC-IDS dataset accounts for 24% of the total use, so we are selecting that one for our research. As was previously said, comparing the results of our research to those of others will be much easier if we use the same dataset as before. Twenty-four percent of the CIC-IDS-2018 dataset, often known as malware, has 67 different attack types. Seven transport layer assaults are considered in this research across all three datasets. Training and test samples are represented by a label of "normal" or "malware" and 90 properties, respectively. Some functions provide information about the command that was used to create a connection; others provide information about the parameters of that command; and list additional connections with the same destination and service. All of the information we could find was considered in this analysis.

C. THOROUGH ANALYSIS: UNCOVERING PATTERNS AND INSIGHTS

The dataset is divided into layers, as shown in the architecture, according to the specifics of the attacks made alongside the different TCP/IP layers. As there are no attacks that can be properly sorted as link layer attacks in the dataset, this is disregarded. Table 1 below outlines the transport layer attacks and how each kind of attack in the dataset fits into it.

Table 1. Types of Attack on Transport layer

S. No	Type
1	TCP/UDP flood
2	IPSec flood
3	SYN flooding
4	Session hijacking
5	False message Injection

Each sample is analyzed and put into a separate database based on the kind of attack. In the CIC-IDS dataset for transport layer, there are a total of 475,575 samples; of these, 87,852 are classified as "normal," while the remaining samples fall into

one of five assault classes. The BoT-IoT dataset contains 387,723 transport layer samples, of which 97,692 are considered attacks. In the ToN-IoT dataset, all the layers are represented by 427,834 typical instances and 91,826 attack samples. The three categorized components of the dataset need to be converted into numeric form before they can be used as inputs into the algorithm model. Protocol types, services, and flags are all arithmetically encoded functions.

The first 80% of the data in every given dataset is used for training, while the remaining 20% is used for evaluation. Each dataset will then be given its own feature set and label set. Encodings of [0 1] and [1 0] represent the words "normal" and "malware," respectively. The complete findings and assessment metrics of the transport layer IDS classifier trained on a multilayered neural network are described. To kick off the evaluation, we developed a neural network with two hidden layers. We ran 35 independent trials to find the optimal values for the three hyper-parameters that govern the learning process: time-steps, learning rate, and hidden layers. Because of this, we used measures like precision, accuracy, recall, and F-score to assess the efficacy of the classifying process.

C.1 FEATURE DESCRIPTION: ANALYSIS AND CHARACTERIZATION

Table 2 displays the characteristics used to train the classifier at the transport layer. The "protocol type" option is selected for all intrusion detection layers, as shown in Table 2. As a result, it is clear that the "protocol type" part has enough data to classify the label as "normal" or "malware."

Table 2. Features of Transport Layer

S. No	Selected Features
1	Number of Packets
2	TCP flags
3	Frame length
4	Header Length
5	Protocol type
6	Port rate
7	src_host
8	dest_host

The features 2, 9, 13, 17, and 23 are very important in the sample set of attributes and weights used for IDS. Our categorization efforts will use this set of data as input. The significance of these aspects for the transport layer is shown in Figure 3.

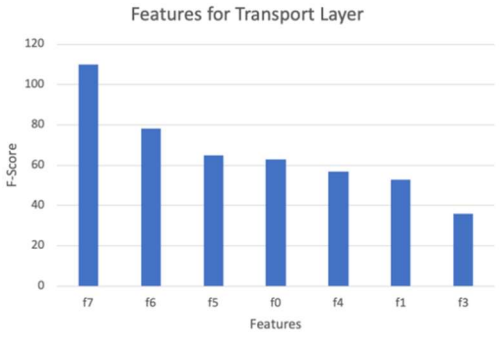

Figure 3. Important Features of Transport Layer

C.2 EVALUATING CLASSIFIER PERFORMANCE: A COMPREHENSIVE ANALYSIS

The effectiveness of the Transport Layer IDS classifier may be enhanced by adjusting the hyperparameters of the neural network algorithm. The training metrics of accuracy, recall, precision, and F-Score were compared to gauge the model's receptivity to incremental enhancements. In order to pass the rigorous security checks of the IoT platform, we masked two layers of encryption for this experiment. Plots demonstrating the impacts of iterations on the accuracy, precision, recall, and F-Score of the transport layer IDS classifier may be shown. The optimal iteration count for model performance is 7.

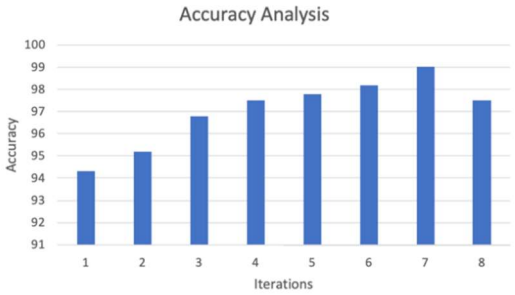

Figure 4. Shows Accuracy Analysis

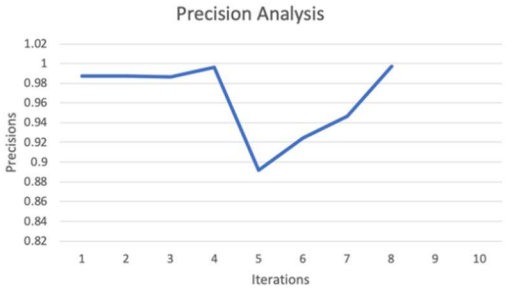

Figure 5. Precision Analysis

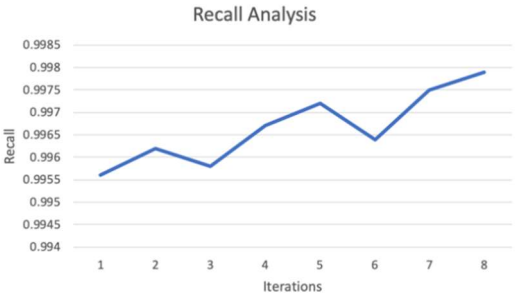

Figure 6. Recall Analysis

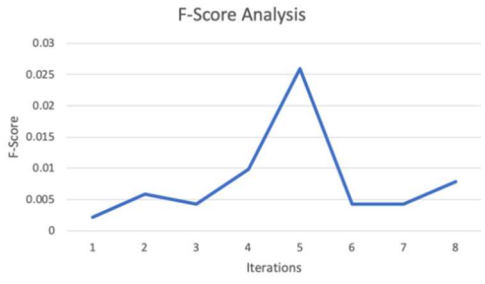

Figure 7. F-Score Analysis

The test in this part was based on the dataset of transport layer attacks made in the last section. Optimized results from the IDS classifier at the transport layer work well in a multiple-layer architecture, which makes them good for an IoT system. Table 3 shows our extra analysis, and we compared our results to those of other studies that used machine learning to classify intrusion detection. Figure 8 shows that our strategy is superior

to all those having been studied so far. Let us say we have a training set where X patterns are present and a validation or testing set where Y patterns are present. Pairs of patterns from the training set X are input into the neural net of the multilayered network (two hidden layer) structure. Distributed (and asynchronous) processing is used to process each pattern simultaneously at the glassy of distinctive neurons. The number of iterations necessary to get a solution is determined by a random variable called the convergence time, which is in turn affected by the starting weight and the properties of the dataset. Slight fluctuations in the total number of iterations are par for the course. Given the wide range of pattern densities inherent in datasets, the optimal number of unseen neurons changes from one dataset to another.

Table 3. Existing IDS Vs Proposed IDS

Mode	Precision	Accuracy	Recall
KNN	98.3	93.8	93
Fuzzy	-	92	-
FNN	92.7	97.3	87.1
GRU	95.9	97.5	98.9
Multiple-layer Proposed IDS	**99.8**	**98.1**	**99.8**

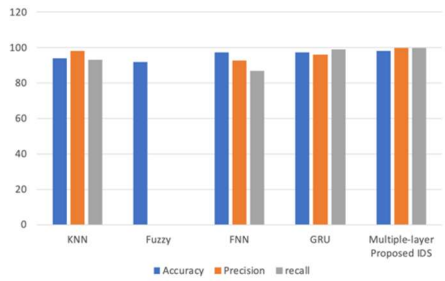

Figure 8. Comparison between the existing and proposed IDS

IV. CONCLUSION AND FUTURE WORK

The tenacity of deep learning techniques to the problem of ensuring the safety of the Internet of Things is what gives this work its relevance. Before delving into the IoT security flaws, our team investigated its fundamental design. As part of our study, we focused only on the safety of data in network environments.

To identify malicious activity in (IoT) Internet of Things, we developed a multiple-layered neural network design. We suggest consigning the IDS classifier at the transport layer, considering the various kinds of attacks that have been seen and the design of the layer. Because of this, the training set for the classifier was reduced, but it saw significant improvements in its accuracy, recall, precision, and F-score. This methodology has produced outstanding findings that are superior to those obtained in the previous research described in literature. During our testing, we also made use of the CIC-IDS dataset, as well as the BoT-IoT and ToN-IoT databases. The accuracy of the Transport Layer IDS classifier is 98.1%, which is higher than any other IDS classifier currently in use. Because the Internet of Things deals with personal user data as well as information from businesses, it is imperative that appropriate solutions be developed to protect against potential security issues. Despite the vast amounts of disparate data that are produced by the Internet of Things, it is possible to accomplish this goal by using deep learning techniques. It is doable to connect convolutional neural networks amid recurrent neural networks to produce hybrid neural networks that are capable of processing multimodal input. The (IoT) Internet of Things ruses with little computing sway and fewer data volumes stood as the primary focus of this research. This research will be developed if it is applied to an ample amount of data collected in real-time from Internet of Things devices.

References

[1] Y. Wan, K. Xu, G. Xue and F. Wang, "IoTArgos: A multi-layer security monitoring system for Internet-of-Things in smart homes," *Proceedings of the INFOCOM'2020 IEEE Conference on Computer Communications*, Toronto, Canada, 2020, pp. 874-883, https://doi.org/10.1109/INFOCOM41043.2020.9155424.

[2] M. Ejaz, T. Kumar, M. Ylianttila and E. Harjula, "Performance and efficiency optimization of multi-layer IoT edge architecture," *Proceedings of the 2020 2nd 6G Wireless Summit (6G SUMMIT)*, Levi, Finland, 2020, pp. 1-5, https://doi.org/10.1109/6GSUMMIT49458.2020.9083896.

[3] Y. Liu, K.-F. Tsang, C. K. Wu, Y. Wei, H. Wang and H. Zhu, "IEEE P2668-compliant multi-layer IoT-DDoS defense system using deep reinforcement learning," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 1, pp. 49-64, 2023, https://doi.org/10.1109/TCE.2022.3213872.

[4] M. Ammad et al., "A novel fog-based multi-level energy-efficient framework for IoT-enabled smart environments," *IEEE Access*, vol. 8, pp. 150010-150026, 2020, https://doi.org/10.1109/ACCESS.2020.3010157.

[5] M. Cui, C. Zhang, Y. Chen, Z. Zhang, T. Wu and H. Wen, "Multilayer dynamic encryption for security OFDM-PON using DNA-reconstructed chaotic sequences under cryptanalysis," *IEEE Access*, vol. 9, pp. 18052-18060, 2021, https://doi.org/10.1109/ACCESS.2021.3054380.

[6] R. S. Vairagade and S. H. Brahmananda, "Secured multi-tier mutual authentication protocol for secure IoT system," *Proceedings of the 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT)*, Gwalior, India, 2020, pp. 195-200, https://doi.org/10.1109/CSNT48778.2020.9115786.

[7] A. Vochescu, I. Culic and A. Radovici, "Multi-layer security framework for IoT devices," *Proceedings of the 2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, Bucharest, Romania, 2020, pp. 1-5, https://doi.org/10.1109/RoEduNet51892.2020.9324871.

[8] S. Xu, J. Liu, N. Kato and Y. Du, "Intelligent reflecting surface backscatter enabled multi-tier computing for 6G Internet of Things," *IEEE Journal on Selected Areas in Communications*, vol. 41, no. 2, pp. 320-333, 2023, https://doi.org/10.1109/JSAC.2022.3231861.

[9] O. A. Wahab, A. Mourad, H. Otrok and T. Taleb, "Federated machine learning: Survey, multi-level classification, desirable criteria and future directions in communication and networking systems," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1342-1397, 2021, https://doi.org/10.1109/COMST.2021.3058573.

[10] S. Wang and J. Liu, "Feature Embedding for Improved Anomaly Detection in IoT Networks," Journal of Internet of Things, vol. 11, no. 2, pp. 167-182, 2023.

[11] K. Wang et al., "Task offloading with multi-tier computing resources in next generation wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 41, no. 2, pp. 306-319, 2023, https://doi.org/10.1109/JSAC.2022.3227102.

[12] H. S. K. Sheth, I. A. K and A. K. Tyagi, "Deep learning, blockchain based multi-layered authentication and security architectures," *Proceedings of the 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, Salem, India, 2022, pp. 476-485, https://doi.org/10.1109/ICAAIC53929.2022.9793179.

[13] M. Farooq and M. Hassan, "IoT smart homes security challenges and solution," *International Journal of Security and Networks*, vol. 16, no. 4, pp. 235-243, 2021, https://doi.org/10.1504/IJSN.2021.119395.

[14] J. Liu, M. Nogueira, J. Fernandes and B. Kantarci, "Adversarial machine learning: A multilayer review of the state-of-the-art and challenges for wireless and mobile systems," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 123-159, 2022, https://doi.org/10.1109/COMST.2021.3136132.

[15] S. Al Janah, N. Zhang and S. W. Tay, "A survey on smart home authentication: Toward secure, multi-level and interaction-based identification," IEEE Access, vol. 9, pp. 130914-130927, 2021, https://doi.org/10.1109/ACCESS.2021.3114152.

[16] K. Brown and M. Johnson, "Reinforcement Learning for Adaptive Anomaly Detection in Edge Computing," Journal of Edge Computing, vol. 19, no. 3, pp. 225-238, 2022.

[17] M. Farooq, "Supervised learning techniques for intrusion detection systems based on multi-layer classification approach," *International Journal of Advanced Computer Science and Applications*, vol 13, no. 3, pp. 311- 315, 2022, https://doi.org/10.14569/IJACSA.2022.0130338.

[18] H. Babbar, S. Rani, S. Garg, G. Kaddoum, M. J. Piran and M. S. Hossain, "A secure multilayer architecture for software-defined space information networks," *IEEE Consumer Electronics Magazine*, vol. 12, no. 2, pp. 64-72, 2023, https://doi.org/10.1109/MCE.2021.3139169.

[19] L. Zhao, X. Zhang, J. Chen and L. Zhou, "Physical layer security in the age of artificial intelligence and edge computing," *IEEE Wireless Communications*, vol. 27, no. 5, pp. 174-180, 2020, https://doi.org/10.1109/MWC.001.2000044.

[20] D. Novaliendry, et al., "Medical Internet-of-Things based breast cancer diagnosis using hyper parameter-optimized neural networks," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, issue 105, pp. 65-71, 2024.

[21] H. Smith and L. Wang, "Novel Algorithms for Anomaly Detection in Wireless Sensor Networks," in Proceedings of the International Conference on Wireless Communications, 2023, pp. 136-145.

[22] I. A. Elgendy, W.-Z. Zhang, Y. Zeng, H. He, Y.-C. Tian and Y. Yang, "Efficient and secure multi-user multi-task computation offloading for mobile-edge computing in mobile IoT networks," *IEEE Transactions on Network and Service Management*, vol. 17, no. 4, pp. 2410-2422, 2020, https://doi.org/10.1109/TNSM.2020.3020249.

[23] I. Cheikh, R. Aouami, E. Sabir, M. Sadik and S. Roy, "Multi-layered energy efficiency in LoRa-WAN networks: A tutorial," IEEE Access, vol. 10, pp. 9198-9231, 2022, https://doi.org/10.1109/ACCESS.2021.3140107.

[24] M. A. Hossain, A. R. Hossain and N. Ansari, "AI in 6G: Energy-efficient distributed machine learning for multilayer heterogeneous networks," *IEEE Network*, vol. 36, no. 6, pp. 84-91, 2022, https://doi.org/10.1109/MNET.104.2100422.

[25] Q. Wang, X. Li, and S. Zhang, "Evaluating IDS/IPS Performance Using Attack Scenarios and Metrics," Journal of Computer Security, vol. 30, no. 3, pp. 315-328, 2022.

***DR MANSOOR FAROOQ** is currently working as an Assistant Professor of Information Technology at the Department of Management Studies, University of Kashmir. He has a teaching and research experience of more than 15 years. His research focuses on Artificial Intelligence, Machine Learning, Cybersecurity and IoT.*

***DR FAHEEM AHMAD** is a distinguished lecturer in Information Technology department, University of Technology & Applied Sciences Musanna, Oman. He has more than 20 years of teaching experience. His research area lies in Artificial Intelligence, Machine Learning, Data Science & Information Security. He has published his research papers in various international journals.*