Providing a Method to Improve the Level of Trust in IOT Networks Using Deep Learning Structure

Parham Kiyoumarsi[1], Farshad Kiyoumarsi[2, *], Behzad Zamani[2]

[1]Department of Engineering, Faculty of Computer, Esfahan University, Esfahan, Iran

[2]Department of Engineering, Faculty of Computer, Shahrekord Branch, Islamic Azad University, Shahrekord, Iran

Received 8 October 2022; Revised 10 February 2023; Accepted 5 March 2023

Abstract

The Internet of Things (IoT) technology has been integrated into various aspects of life, including transportation, healthcare, and even education. This technology encompasses intelligent services that enable devices to interact with the physical world and provide appropriate services to users at any time and place. The current study aims to propose a model for trust management in IoT devices and services that effectively addresses the existing challenges in this domain. With the remarkable advancement of IoT technology, the number and complexity of attacks have increased significantly. Attackers exploit the heterogeneity of IoT to create trust issues and manipulate device behavior. Existing trust management techniques face limitations, such as ineffectiveness in handling large volumes of data and adapting to continuously changing behaviors. This research proposes a model that combines the Simple Multi-Attribute Rating Technique (SMART) and the Long Short-Term Memory (LSTM) algorithm. SMART is employed to calculate trust values, while LSTM is utilized to identify behavioral changes based on trust thresholds. The proposed model leverages the integration of SMART and LSTM, where SMART calculates trust values and LSTM identifies and analyzes behavioral variations. The model's effectiveness has been evaluated using metrics such as accuracy, loss rate, precision, recall, and F-measure. Compared to existing deep learning and machine learning methods, the model demonstrates superior performance. With 100 iterations, the model achieved an accuracy of 99.87% and an F-measure of 99.76%.

Index Terms— **IoT Services, Long Short-Term Memory, Multi-Criteria Decision Making, Trust Management**

I INTRODUCTION

The Internet of Things (IoT) is a network in which various intelligent objects and devices communicate through the Internet [1, 2]. The total number of connected devices worldwide is approximately 17 billion, with IoT devices accounting for 7 billion (excluding smartphones, tablets, and laptops). Forecasts show that this number will reach 0.75.44 billion devices worldwide by 2025 [3, 4]. IoT technologies are critical in advancing various applications in healthcare [5], home automation, agriculture, transportation [6, 7], and education [8, 9]. With continuous technological advancements and expanding application domains [10], the Internet of Things has evolved into customized solutions designed for specific purposes [11].

The proposed model in this research is specifically designed for health applications by using new technologies such as deep learning a*lg*orithms (LSTM) and advanced structures in complex data analysis. This model has several innovative aspects that are mentioned below:

Considering the ever-increasing growth of data generated by medical devices and health applications, the proposed model provides a new solution to strengthen cybersecurity. This model uses an LSTM architecture to identify and prevent cyber threats and provides the possibility of protecting sensitive patient data against cyberattacks. The proposed model uses an advanced architecture including three LSTM layers and three dense layers, which improves its ability to process large amounts of data with temporal relationships and long-term trends. This capability is very valuable in applications such as time series forecasting and medical data classification.

To deal with the challenge of overfitting, the model uses techniques such as dropout rate and kernel regularization. These features help the model to best generalize training data and be more accurate in real data processing. Considering the complexity of the data generated by IoT devices in the health field, the model uses the Rectified Linear Unit (ReLU) activation function to analyze the nonlinear relationships between the data. This feature allows the model to extract more complex features and provide more accurate predictions. The proposed model has a flexible architecture that allows it to be used in binary and multi-class classification. This flexibility enables the model to be used in a wide range of health applications, including identifying cyber-attacks and predicting the health status of patients. For the best performance, the model uses advanced optimization algorithms to adjust the hyperparameters. In addition, the cross-class entropy function is used to reduce losses and improve model efficiency in the training process. By combining the LSTM algorithm and dense layers, this research provides a flexible and efficient model for health data processing in IoT environments.

This model is specifically focused on security, accuracy, and sustainability and can meet the growing needs of the digital health field. The innovative aspects of the model, including complex data processing, dealing with cyber threats, and using optimal architectures for data classification, make it an advanced and distinctive solution in this field.

The architecture of the Internet of Things consists of three layers: the application layer, the perception layer, and the network layer. These layers work together to facilitate the operation of IoT systems. Figure 1 shows the architecture of the Internet of Things.

The Internet of Things has significantly affected industries and people's daily lives. The Internet of Things aims to integrate the physical and digital worlds as a bridge between them. People aim to improve their lives by using the Internet of Things, looking for simplicity, comfort, and well-being. As the Internet of Things continues to grow in popularity and use, so do security and cyber challenges. These challenges significantly affect the efficiency and performance of IoT systems. IoT devices present a range of complex security concerns due to the open nature of the IoT ecosystem that operates over the Internet. As a result, these devices are often exposed to damage and attacks from various factors and external factors. Hence, there is a critical need for early detection of security vulnerabilities in the IoT environment. IoT devices and ecosystems face a wide range of threats and vulnerabilities. A threat is an activity that exploits the security flaws of a system, which can compromise its security and performance. These threats can have severe consequences for individuals and organizations.

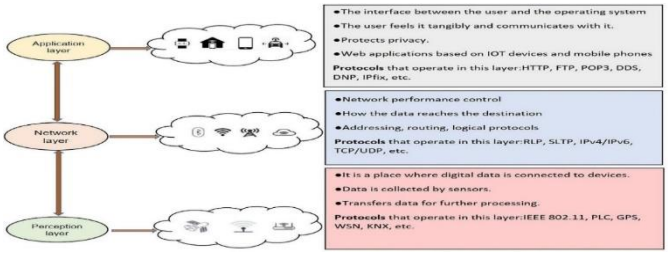

Fig. 1. Internet of Things architecture [13]

II Related works

Ebrahimi (2023) [7] Trust algorithms in the Internet of Things: review, analysis and presentation of evaluation criteria. This article examines the trust management algorithms in the Internet of Things (IoT) and provides criteria for evaluating these algorithms. The main goal of the research is to analyze the existing methods for establishing trust in IoT networks and their impact on security and privacy. The authors emphasize the importance of building trust as one of the main components of cybersecurity in IoT. Research findings have shown that the implementation of trust management systems can help improve security, privacy, and reliability in IoT communications. Based on the data obtained, systems that manage trust criteria well reduce the probability of cyber intrusions by 25%. The conclusion of this paper emphasizes the key role of trust in IoT security. The authors point out that building trust can help improve users' adoption of IoT technology and increase their level of confidence.

Baksham (2023), [12] The effect of the technological **applications of the Internet of Things on the development of** dynamic capabilities in knowledge-based companies in the agricultural sector. This research has investigated the effect of using Internet of Things (IoT) technology in improving dynamic capabilities in agricultural knowledge-based companies. The main goal of the paper is to show how to improve performance and productivity through the use of IoT data in smart agriculture. The results have shown that the implementation of IoT has improved productivity by up to 30% and reduced costs by up to 20% in agricultural processes. The use of smart sensors to monitor soil, temperature, and humidity has increased agricultural production and reduced waste. In the conclusion of the article, it is pointed out that IoT can be an effective tool for sustainable development in the agricultural sector. Especially in knowledge-based companies, this technology can play a key role in increasing efficiency and reducing production costs.

Bhoi, (2023), [13] Application of Internet of Things in providing a model of an intelligent irrigation system of fields with optimal consumption management approach. In this article, an intelligent irrigation system based on the Internet of Things has been designed and evaluated. The main goal of the research is to reduce water consumption in agriculture and improve product productivity through the use of IoT. The proposed system includes humidity and temperature sensors that automatically analyze environmental conditions and adjust irrigation based on plant needs. The findings of the research show that this system has been able to reduce water consumption by 35% and increase the productivity of products by 20%. The conclusion of the article emphasizes the importance of using smart technologies in the management of natural resources. The authors suggest that this approach be used in other agricultural areas to spread its positive effects.

Rajabzadeh (2023) [14] The impact of Internet of Things technology on the performance of the storage sector of the supply chain of the strategic wheat product. This article has investigated the impact of IoT on the improvement of storage management in the supply chain of wheat. The main goal of the research is to reduce waste and improve storage quality using smart technologies. The findings show that the use of IoT sensors to monitor storage conditions, such as temperature and humidity, has been able to reduce wheat waste by 40% and improve product quality. This technology has made it possible to prevent damage caused by environmental changes. The conclusion of the article emphasizes that IoT can play a key role in optimizing the supply chain of agricultural products. Especially in strategic product storage management, this technology can help reduce costs and increase quality.

Al-Ghafili (2024) [15] Trust management model for Internet of Things devices and services. Based on a multi-criteria decision-making method and short-term and long-term memory algorithms, this article has presented a new model for trust management in Internet of Things devices and services. The proposed model uses multi-criteria decision-making methods (MCDM) and long-short-term memory (LSTM) algorithms to identify and manage unreliable behaviors. The main goal of this research is to increase the accuracy in identifying threats and predicting behavioral changes of devices connected to IoT. The research findings showed that the proposed model could achieve 98.7% accuracy in identifying unreliable behaviors and 97% in predicting behavioral changes. This method has been able to show superior performance compared to previous approaches. The conclusion emphasizes that using the combination of MCDM and LSTM can significantly improve the security and reliability of IoT devices and be recognized as an effective solution for .

Ghafari, (2024) [16] Ensuring the security of the Internet of

Things using machine learning and deep learning methods: a review. This article examines the security techniques based on machine learning and deep learning in the Internet of Things. The main goal of this study is to analyze different methods and identify the best methods to reduce security threats and improve reliability in IoT. The results have shown that deep learning algorithms such as LSTM and CNN can increase the accuracy of threat detection by up to 95%. Also, methods based on machine learning have been able to reduce the error rate by 20%. The conclusion of the paper shows that the use of a combination of deep learning and machine learning methods can significantly improve IoT security. However, challenges such as the need for voluminous data still exist.

Cherbal (2024), [17] Security in the Internet of Things: A Review of Blockchain, Machine Learning, Cryptography, and Quantum Computing-Based Methods. This article provides a comprehensive overview of IoT security approaches and discusses methods such as blockchain, machine learning, cryptography, and quantum computing. The purpose of this research is to provide a comprehensive security framework and reduce the risks of penetration. The findings show that using blockchain can reduce the penetration rate by 50%, and machine learning has helped to improve the accuracy of threat identification by 30%. The study emphasizes that combining these methods can develop a comprehensive security framework for IoT. However, implementation costs are considered a critical challenge.

Jani, (2024), [18] Long-short-term memory-based approach to detect cyber-attacks in IoT using CIC-IoT2023 dataset. This paper investigates using the LSTM algorithm to detect cyberattacks in IoT systems. The main goal of the research is to improve the accuracy of threat detection and reduce the error rate using the CIC-IoT2023 dataset. The results show that the proposed model can achieve 96.5% accuracy in identifying cyber-attacks and reduce the error rate by 15% compared to previous methods. The study indicates that LSTM can be an efficient tool to deal with cyber threats, and the high accuracy of this model shows its ability to analyze IoT data.

Tseng, (2024) [19] Identifying multi-class intrusions in IoT networks using a transformer and CIC-IoT2023 dataset. This paper has used a transformer architecture to identify multi-class intrusions in IoT networks. The main goal of the research is to improve accuracy and reduce processing time in identifying security threats. The results have shown that the transformer model can achieve 97.8% accuracy and a processing time of less than 0.5 seconds for each sample. The study emphasizes that transformers can be a suitable alternative to LSTM in IoT security issues and provide better performance in data analysis.

Vardhan (2024) [20] Title: Resilient intrusion detection system for IoT environment based on modified cumulative classification. This paper has developed a resistant intrusion detection system for IoT networks. The proposed model uses a modified cumulative classification algorithm involving several machine learning models. The findings have shown that the proposed model was able to achieve 94.3% accuracy in identifying multi-class threats and showed significant resistance against DDoS attacks and malware. The study emphasizes the importance of using hybrid methods to improve security in IoT networks and suggests that this approach be used in dynamic environments.

III Proposed method

In the proposed method, the goal is to improve the performance and also to increase the trust and reliability in the Internet of Things networks with moving nodes, for this reason, and to optimize the research of Base [13], we use the vector machine algorithm, the goal of LSTM is to find the best state. The classification is in such a way that the maximum margin is created for the classifier line. In the Internet of Things networks, the delay in sending data packets and interference a huge challenge that always causes a loss of trust and confidence in the network.

The source-to-destination delay includes the transmission delay on intermediate links, the contention delay caused by the competition of nodes for the shared channel, and the queuing delay induced in each intermediate node due to the policy/or strict channel conditions. Transmission delay is the time for a successful transmission, defined as the period from the time a packet is first transmitted. After which moment, it is either successfully transmitted or dropped after a predefined number of retransmissions. Competition delay is access delay. And each retransmission will delay new access. The queuing delay at an intermediate node can be interpreted as the time between when a packet arrives at a node and when this packet is transmitted. However, transmission failure occurs repeatedly, and retransmission delay must be considered.

1. Feature extraction

The primary goal of feature engineering is to generate or extract features from existing data. Therefore, in this sub-step, some existing features are used to create additional features (eg, packet loss, delay, and throughput). The amount of packet loss can be calculated using Equation 1:

(1)

$$Packet\ Loss = \frac{Packet\ sent - Packet\ recived}{Packet\ sent} \times 100$$

Latency - The delay caused by the transfer from one point to another point that becomes the destination is known as latency. Equation 2 is used to calculate the delay:

Delay = propagation delay + transmission delay + queuing delay + processing delay (2)

Propagation delay: The amount of time it takes for a bit to travel from the source to the destination. The propagation delay is calculated by dividing the distance by the propagation speed, as shown in Equation 3:

$$\text{Propagation delay} = \frac{\text{distance}}{\text{Propagation Speed}} \quad (3)$$

where the average distance of the package size * 1000 and the propagation speed is a constant value (=3 108 m/s)

Transmission delay - the amount of time it takes for a packet to be sent from the source to the transmission medium, as shown in Equation 4:

$$\text{Transmission delay} = \frac{\text{length of packets}}{} \quad (4)$$

Bandwidth

where the bandwidth indicates the maximum number of packets.

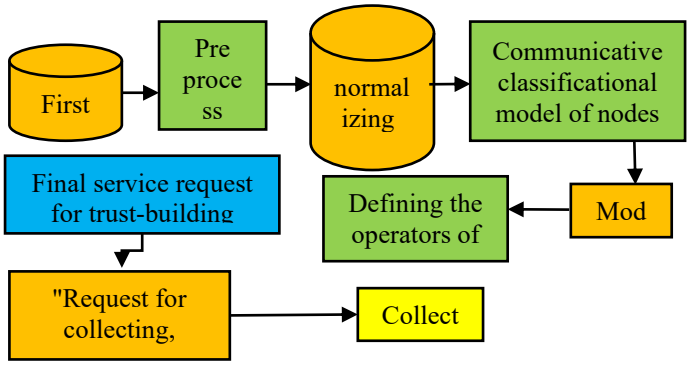

Fig. 2. Flowchart of the proposed method

Queuing delay: This delay is caused by the time required for routers to handle packet transmission queues across the network. Processing Latency: The time it takes for a network device to see the route, update headers, and switch tasks is called processing latency. Actual bandwidth is measured at a specific time and under specific network conditions for transferring files of a specific size. The total speed of data sent to all terminals of a network is known as throughput, which can be calculated using equation 5:

(5)

$$Throughput = \frac{\sum Packet\ sent(bits)}{Time\ of\ data\ deilvary\ (s)} \times 100$$

2.

Normalization

In this process, the features are scaled to values from 0 to 1 to produce an accurate result. This step is necessary to convert the numeric column values in the dataset. Therefore, it may be used on a common scale without distorting changes in value ranges or loss of data. Normalization is done using equation 6:

(6)

$$z_i = \frac{x_i - \min(x)}{\max(x) - \min(x)}$$

where xi is the ith value of the data set, (min(x) is the minimum value of the data set, and (max(x) is the maximum value of the data set.

3. Trust Prediction Stage

The trust prediction stage is divided into two sub-stages: trust value calculation and misbehavior detection. In the trust value calculation sub-step, the simple multi-attribute ranking technique (SMART) is used, which determines the trust value based on the node information extracted in the previous step (data preparation). In the sub-step of misbehavior detection, the long-term short-term memory (LSTM) technique is used for classification/prediction tasks, which is an excellent technique for detecting changes in behavior. During this sub-step, the learned model classifies new unknown data (included in the test set) that the model has never seen before to evaluate the capabilities of the learned model (initially, the model's intelligence is evaluated, and if it is acceptable). The learned model can then be used for diagnosis.

4. Calculating the value of trust

In this sub-step, the data are identified as reliable or unreliable using the SMART technique. It is based on the concept that each alternative consists of several criteria with values, and each criterion has a weight that indicates its relevance. Compared to other criteria.

IV Simulation

The first step is to use the node LSTM approach to find the most optimal points in the region, and then consider the nearest node as the cluster head. The number of particles and the speed are calculated according to the size of the area. Initially, the number of particles that work together equals 20 bits, and the speed equals 4. It is compared and changes with the increase of the current number of nodes in the environment. A misbehavior detection model was developed with LSTM cells, shedding, and dense output layers. Explain the layers and parameter values used. The model was run using periods of 50 and 100 nm, and a batch size equals 72. In addition, the model used the modified linear unit (ReLu) and MATLAB optimizer, and sigmoid activation functions. In Figure 3, the desired output results are displayed based on the maximum error that may occur in selecting cluster heads and, finally, clustering. In fact, in this figure, the ideal conditions for clustering are green, and for the result of the previous work in the original research, the red color, and the result of our work, the blue color is specified. By observing the result, we find that the best result for the output has occurred, and our result is lower than the limit.

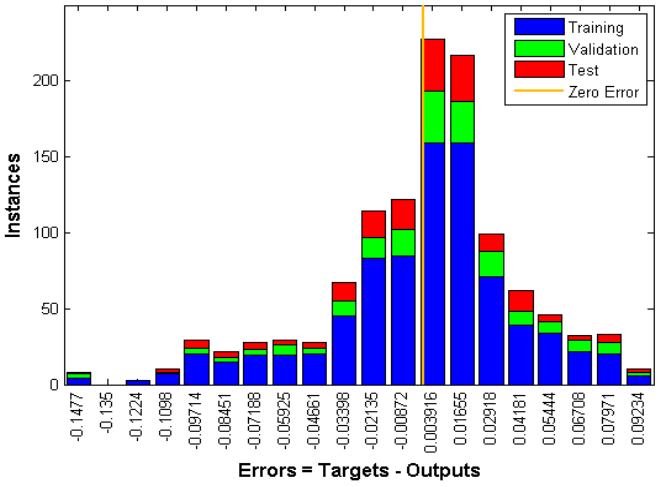

Fig. 3. The error based on the layers used to select the classes

In Figure 4, we see the constant process of changes for clustering, which, after some time, takes on a completely uniform process. In all these cases, the process of change is such that the LSTM algorithm reaches a specific process for any number of nodes. This issue will eliminate the unconscious choice and uncertainty for choosing the heads of the clusters.

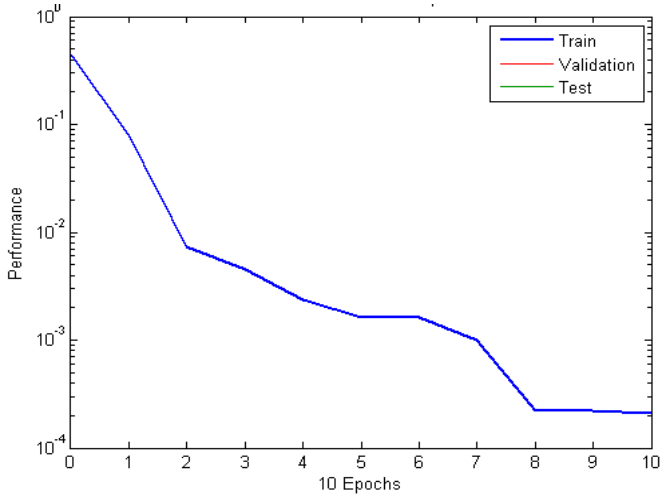

Fig. 4. Assimilation of clustering results with the LSTM algorithm

We can also show the desired work results for comparing the useful life for nodes in the clustering of the proposed method with an arbitrary algorithm called Ant, and a neural network in Figure 3. If we consider the process of changes and optimization for different periods and different nodes, then we can show the process of changes in Figure 4.

Fig. 5. The death timing of the number of different nodes at different times and different classes

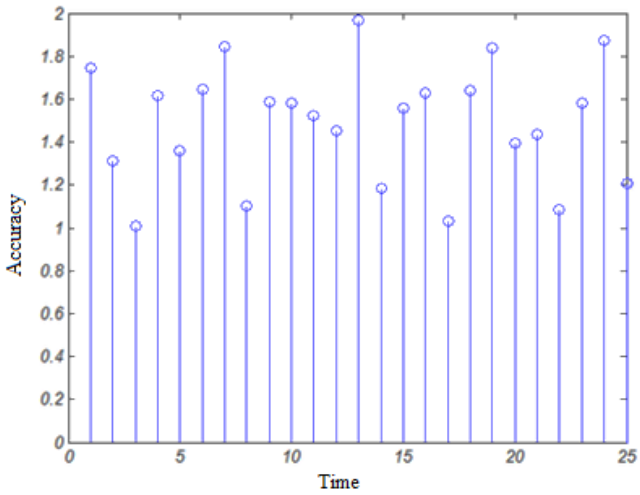

Figure 5 shows the death timing of nodes in different classes. As we can see in this figure, we display the timing of death for different nodes in three time periods. In these three cases, the dead time of the nodes is higher for our proposed method due to the correct clustering that has been done. (Figure 6)

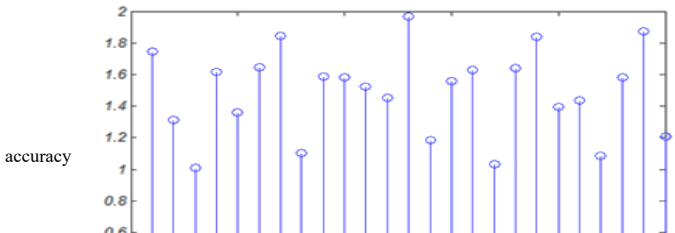

Fig. 6. Statistical display for final knotting and clustering using LSTM

V Conclusion

These results showed clear evidence that the performance of the proposed model improves with the increase of the sample size used, unlike other models whose performance decreases with the increase of the sample size. Furthermore, changing samples provide evidence that deep learning models are more robust, as results show more stable performance despite different samples, making them excellent candidates for dealing with continuous changes in IoT devices and detecting misbehavior. As a result, it seems that the proposed model outperforms other machine learning models, while these models do not achieve significant performance. This proves that LSTM can be adapted to tackle "big data" challenges and can train complex behavior patterns of IoT devices more successfully than machine learning models.

VI References

[1] Mukherjee, S., Kumar, R., Banerjee, S. (2022). Smart Healthcare Remote Monitoring System Using Internet of Things. In: Mukherjee, S., Muppalaneni, N.B., Bhattacharya, S., Pradhan, A.K. (eds) Intelligent Systems for Social Good. Advanced Technologies and Societal Change. Springer, Singapore. https://doi.org/10.1007/978-981-19-0770-8_9

[2] Ruby Dwivedi, Divya Mehrotra, Shaleen Chandra, (2022), Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review, Journal of Oral Biology and Craniofacial Research, Volume 12, Issue 2,2022, Pages 302-318, ISSN 2212-4268.

[3] Michael Abner, Peter Kok-Yiu Wong, Jack C.P. Cheng, (2022), Battery lifespan enhancement strategies for edge computing-enabled wireless Bluetooth mesh sensor network for structural health monitoring, Automation in Construction, Volume 140,2022,104355, ISSN 0926-5805.

[4] S. Bajpai, K. Sharma, B.K. Chaurasia, Intrusion detection framework in IoT networks, SN Comput. Sci. 4 (4) (2023) 350.

[5] Farahani B, Firouzi F, Chang V, Badaroglu M, Constant N, Mankodiya K (2021) Towards fog-driven IoTeHealth: promises and challenges of IoT in

medicine and healthcare. Futur Gener Comput Syst 78:659 676. https://doi.org/10.1016/j.future.2021.04.036

[6] Azimi I, Anzanpour A, Rahmani AM, Liljeberg P, Salakoski T (2020) Medical warning system based on Internet of Things using fog computing. In: International workshop on big data and information security (IWBIS), pp 19–24. https://doi.org/10.1109/IWBIS.2020.7872884

[7] M. Ebrahimi, A. Continella, A. Bianchi, Aot-attack on things: A security analysis of IoT firmware updates, in: 2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P), 2023.

[8] Javadpour, P. Pinto, F. Ja'fari, W. Zhang, DMAIDPS: a distributed multi-agent intrusion detection and prevention system for cloud IoT environments, Cluster Comput. 26 (1) (2023) 367–384.

[9] Sen AAA, Yamin M (2021). Advantages of using fog in IoT applications. Int J Inf Technol 13:829 837. https://doi.org/101007/s41870-020-00514-9

[10] Isa IS, El-Gorashi TE, Musa MO, Elmirghani JM (2020) Energy efficient fog-based healthcare monitoring infrastructure. IEEE Access 8:197828 197852. https://doi.org/10.1109/ACCESS.2020.3033555

[11] M. M. Kamruzzaman, Bingxin Yan, Md Nazirul Islam Sarker,(2022), Blockchain and Fog Computing in IoT-Driven Healthcare Services for Smart Cities, Volume 2022 | Article ID 9957888 | https://doi.org/10.1155/2022/9957888

[12] Bakhsham, M. (2021). The Impact of IoT technological applications on the development of dynamic capabilities in agricultural knowledge-based companies. Journal of Entreneurship and Agriculture, 8(15), 67-75.

[13] Bhoi, A., Nayak, R. P., Bhoi, S. K., Sethi, S., Panda, S. K., Sahoo, K. S., & Nayyar, A. (2021). IoT-IIRS: Internet of Things based intelligent-irrigation recommendation system using machine learning approach for efficient water usage. PeerJ Computer Science, 7, e578

[14] Rajabzadeh, M., Elahi, S., Hasanzadeh, A., & Mohammad, L. (2020). The impact of internet of things deployment on the storage performance of wheat strategic product supply chain in Khorasan Razavi Province

[15] Alghafaili, Y., & Rassam, M. A. (2024). A Trust Management Model for IoT Devices and Services Based on the Multi-Criteria Decision-Making Approach and Deep Long Short-Term Memory Technique. *Sensors*, 24(2), 634.

[16] Ghaffari, A., Jelodari, N., Pouralish, S., Derakhshanfard, N., & Arasteh, B. (2024). Securing Internet of Things Using Machine and Deep Learning Methods: A Survey. *Cluster Computing*, 27, 9065–9089.

[17] Cherbal, S., Zier, A., Hebal, S., Louail, L., & Annane, B. (2024). Security in Internet of Things: A Review on Approaches Based on Blockchain, Machine Learning, Cryptography, and Quantum Computing. *The Journal of Supercomputing*, 80, 3738–3816.

[18] Jany, A. I., & Arnob, A. K. B. (2024). A Long Short-Term Memory-Based Approach for Detecting Cyber Attacks in IoT Using CIC-IoT2023 Dataset. *Journal of Edge Computing*, 3(1), 28–42.

[19] Tseng, S.-M., Wang, Y.-Q., & Wang, Y.-C. (2024). Multi-Class Intrusion Detection Based on Transformer for IoT Networks Using CIC-IoT-2023 Dataset. *Future Internet*, 16(8), 284.

[20] Vardhan, A., Kumar, P., & Awasthi, L. K. (2024). A Resilient Intrusion Detection System for IoT Environment Based on a Modified Stacking Ensemble Classifier. *SN Computer Science*, 5(8).