ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 7 July 2024

Insight of Learning Approaches for Thwarting Security Threats in Internet-of-Things

[1] Chethana M, [2] Dr.R.Nagaraj

[1] Department of Information Science & Engineering Bangalore Institute of Technology Bengaluru, India

[2] AMC Engineering College Bengaluru, India

Corresponding Author Email: [1] Chethanayasmita9@gmail.com, [2] prof.rnagaraja@yahoo.com

Abstract*— Security has been always a serious concern in Internet-of-Things (IoT) that is characterized by highly interconnected devices and appliance thereby forming a complex form of network. At present, there are various form of solution that are chosen as security measures to safeguard IoT devices and services from various form of lethal threats. However, all the solutions are mainly in form of encryption, which has quite a limitation towards resisting dynamic threats. It is noted that Artificial Intelligence (AI) based scheme has been making a potential contribution towards solving the similar security threats in IoT in predictive manner. Ir-respective of archives of literatures where AI has been implemented in the form of machine learning and deep learning methods; however, no conclusive information is yet stated towards its effectiveness. Hence, this paper reviews the existing AI based approaches and contributes towards this issue by offering a com-pact, precise, and effective findings stating the true effectiveness of existing learn-ing-based methods. Further, it is noted that existing system suffers from various limitation that are associated with issues with various learning approaches as well as dataset too. The impact of such limitation is that reduced strength to identify and resist dynamic forms of complex security threats in IoT. Finally, the paper contributes towards offering a suggested methodology where adoption of hybrid learning approach can be used to address the identified gaps in existing learning approaches towards strengthening IoT security.

Index Terms*— artificial intelligence, internet-of-things, machine learning, deep learning, security.

I. INTRODUCTION

Internet of things (IoT) refers to form of highly interconnected network of various technologies, software, sensors, etc., commonly known as things in order to facilitate data exchange among connected devices [1]. The utilization of IoT has been realized via its efficiency towards automation [2], data collection and insights [3], enhanced connectivity [4], enhanced quality of life [5], environmental sustainability [6], safety and security [7]. However, irrespective of potential beneficial features in IoT, there are various technological challenges too viz. security [7], cost of operation [8], power consumption [9], data management and analytics [10], scalability [11], and interoperability. Out of all the above-mentioned challenges, security has been always a bigger concern in IoT. Many IoT devices have limited processing power and memory, making them vulnerable to various security threats such as malware, ransomware, and unauthorized access. IoT devices often communicate over wireless networks, which can be susceptible to interception and eavesdropping. IoT devices collect vast amounts of data about users' behaviour, preferences, and surroundings. If this data is not adequately protected, it can be exploited for malicious purposes or unauthorized surveillance, raising serious privacy concerns. IoT devices deployed in uncontrolled environments, such as industrial facilities or public spaces, may be physically accessible to unauthorized individuals. The complexity of IoT supply chains introduces additional security risks. Malicious actors may compromise components or software during the manufacturing or distribution process, leading to vulnerabilities in the final product. IoT devices can be hijacked and used as part of botnets to launch large-scale distributed denial-of-service (DDoS) attacks. These attacks can overwhelm networks and servers, causing disruption to critical services and systems. At present, there are various studies being carried out towards addressing the security loopholes in IoT [12]-[14]. The most frequently adopted solution towards resisting threat entry and propagation are authentication and access control [15], encryption [16], secure communication protocols [17], network segmentation and firewall [18], and identity management [19]. However, almost all the existing approaches do have beneficial features as well as limiting attributes too, which has been reported in multiple pre-existing studies itself. Hence, the research problem is to make a conclusive decision towards identifying the most optimal and effective solution towards IoT security threats.

Artificial Intelligence (AI) have been found to make some of the noteworthy contribution in IoT security; however, its degree of effectiveness is still less clearly report-ed. Therefore, this paper aims towards presenting a snapshot of effectiveness of AI-based schemes for realizing its effectivity. The organization of the paper is: Section 2 outlines the adopted research methodology while Section 3 presents review findings, and Section 3 and Section 4 discusses about conclusive remarks and future proposed method.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 7 July 2024

II. RESEARCH METHOD

The prime aim of the proposed study is to carry out a compact review work towards exploring the usage of the two dominant AI-based schemes for securing IoT i.e., machine learning and deep learning techniques. A desk research methodology is adopted for this purpose, where the review work has emphasized reviewing research articles published in last decade till date. Although, there are massive number of publications, but certain filtering is carried out to all the aggregated document in order to explore more accurate and precise review findings. According to the adopted sample filtering technique, only the implementation research articles with an inclusion of elaborative algorithm design and illustrative result discussion have been chosen. It is also ensured that only the papers with unique techniques are considered for review work. Any form of duplicated implementation or similar methodology have been discarded for review work. After the final shortlisted research articles have been collected, the presented review work also discusses about the research trends towards the usage of each individual approaches involved in both the form of learning approaches. Effort is also put forwarded towards understanding the trend of usage of varied forms of dataset used in investigating IoT security modelling. Finally, discussion of unsolved problems is carried out in the form of identified research gap. The next section discusses about the accomplished study findings.

III. RESULT & DISCUSSION

The prior section has discussed about the research method that has been adopted in order to carry out this review work while this section presents the findings of the review outcomes towards deploying learning-based approaches for leveraging IoT Security. There are various cadre of learning methodologies where machine learning and deep learning schemes are found to be the dominant one applied towards modelling. Each approaches have its own beneficial perspective as well as limiting attributes that calls for further investigation. The briefing of findings of current reviewed literatures are as follows:

A. Summary of Findings of Learning-Approaches

It was noted that deep learning-based approaches are quite evolving and increasing in its proliferated utilization towards solving various prominent issues in IoT. Followings are the discussion about these two prominent techniques:

Deep Learning Approaches: The adoption of an improved version of Convolution Neural Network (CNN) has been witnessed in work of Zhou et al. [20] with an agenda towards enhancing the quality of predictive performance associated with wearable devices in IoT. Unlike typical security approaches, the model uses Bayesian network which is capable of resisting potential threats while Autoencoders (AE) are considered along with it. Deep learning towards IoT security was also reported in work of Taiwo et al. [21] where a prototyping has been carried out towards safeguarding appliances connected to IoT network using CNN. The adoption of CNN was also seen in work of More et al. [22] with an agenda for secure medical image transmission over IoT ecosystem. Adoption of CNN with varied forms was also witnessed in work of Jeon et al. [23], Zhang et al. [24], Okey et al. [25], Li et al. [26]. It was also noted that autoencoder usage is also proven better for IoT security controls as seen in work of Salahuddin et al. [27] and Alshudukhi et al. [28]. The idea is to identify the anomaly using temporal features. Recurrent Neural Network (RNN), a variant of deep learning, was used by Liao et al. [29] for securing IoT storage units. Another type of deep learning approach called as Long Short-Term Memory (LSTM) has been shown to resist potential threats of DDoS along with usage of RNN as noted in work of Alasmary et al. [30]. Adoption of LSTM was discussed by Zeeshan et al. [31]. Work of Ullah et al. [32] has reported use of bidirectional LSTM, RNN, and Gated Recurrent Unit (GRU) towards anomaly detection. Usage of autoencoder was seen in work of Vu et al. [33] and Lee et al. [34] emphasizing mainly on attack feature modelling in IoT. Deep learning has been also combined with machine learning approach as reported in work of Zhou et al. [35], Tran et al. [36], Sudhakaran et al. [37], Savic et al. [38], and Naula et al. [39].

Machine Learning Approaches: There are different variants of machine learning-based approaches witnessed to be used for improving security features in IoT. Decision Tree (DT) is one such machine learning approach adopted by Zarzoor et al. [40] and Ferrag et al. [41] with the core idea of extracting the unique patterns of an attacker for detecting the threats. Artificial Neural Network (ANN) is another frequently adopted machine learning scheme where the core idea was to perform an identification of attacker (Latif et al. [42], Sarkar et al. [43], Pacheco et al. [44], Al-Mohammed et al. [45]). ANN could be used as standalone approach as well as it was also used in integrated with bio-inspired approach as well (e.g., Sarkar et al. [43]). Support Vector Machine (SVM) is another frequently deployed machine learning approach where the agenda is to perform classification for leveraging the detection performance in IoT environment (Vassiliou et al. [46], Ezhilarasi and Clement [47], Bagga et al. [48]). Just like ANN, SVM was also reported to be used in integration with Gated Recurrent Unit (Ezhilarasi and Clement [47]) and Software Defined Network (Bagga et al. [48]). Usage of Logistic Regression (LR) is more associated with anomaly detection by combining with other machine learning approaches for threat identification (Subramaniam et al. [49], Li et al. [50], Korystin et al. [51]). Another supervised approach known as Naïve Bayes (NB) is also used for solving classification problems in studies of IoT security (Setiadi et al. [52], Majeed et al. [53], Jadhav et al. [54]). There are also various mixed models of machine learning approach used for IoT security viz. i) integrated model of DT with AdaBoost and Random Forest (RF) (Wu et al. [55]), ii) integrated with

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 7 July 2024

federated learning (Yadav et al. [56]), iii) integrated with clustering (Kammoun et al. [57]), and iv) integrated model of NB with K-Nearest Neighbor (KNN) and SVM (Jadhav & Pellakuri [54]).

B. Identified Drawbacks of Existing System

The identified drawbacks of the deep learning based approaches are as follows: Complex features of motion not involved (Taiwo et al. [21]), study applicable for grayscale images only (More et al. [22]), Overfitting issues (Jeon et al. [23]), Dynamic information not included in study (Zhang et al. [24]), Negative transfer issue not sorted (Okey et al. [25]), Study specific to attack model (Li et al. [26]), Cannot classify dynamic input error (Salahuddin et al. [27]), Vital information gets eliminated (Alshudukhi et al. [28]), Traffic flow constraint affecting storage is not analyzed (Liao et al. [29]), Needs large training data (Alasmary et al. [30]), Study specific to particular attack models only (Zeeshan et al. [31]), Massive dependency of data for accuracy (Ullah et al. [32]), Higher consumption of training time (Vu et al. [33]).

The identified drawbacks of the machine learning based approaches are as follows: Scalability affects in larger network size (Zarzoor et al. [40]), Works on predefined attacks only (Ferrag et al. [41]), Study specific to dataset, doesn't work on noisy dataset (Latif et al. [42]), Induces complexity for large network (Sarkar et al. [43]), No Benchmarking (Pacheco et al. [44]), Accuracy depends upon dataset size (Al-Mohammed et al. [45]), Slightly Reduced accuracy (82.45%) (Ezhilarasi and Clement [47]), Not applicable for dynamic attackers (Bagga et al. [48]), No benchmarking (Subramaniam et al. [49]), Not applicable for complex intrusion (Li et al. [50]), Lack of extensive analysis to prove (Korystin et al. [51]), lower 64.02% accuracy of detection (Setiadi et al. [52]), lack of benchmarking (Majeed et al. [53]), Sophisticated learning approach (Jadhav et al. [54]), Sophisticated approach for large network of IoT (Wu et al. [55]), No benchmarking or extensive analysis (Yadav et al. [56]), analysis doesn't include benchmarking (Kammoun et al. [57]).

C. Current Research Trends

The current research trends have been observed for last 10 years with a target to understand the significance of adoption of varied learning-based techniques by existing researcher. From the Fig.1, it is noted that number of publications for machine learning-based approach is 42040 while that of deep learning approach is 35,585. Hence, more studies have been still been undertaken using machine learning approach in contrast to deep learning approach.

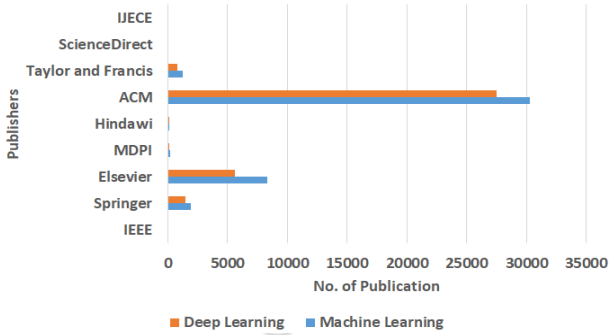


Fig. 1. Research trends for publications for machine-deep learning approach

Fig.2 showcases the publications trends towards various form of machine learning. From the perspective of classification-based machine learning approaches, Fig.2(a) exhibits that there are total of 318 publications where SVM and DT are frequently used. In regression-based approach, LR methods is the most prominent approach in comparison to Lasso-based Regression (LassoR) and Support Vector Regression (SVR), as shown in Fig.2(b). In viewpoint of clustering approach, adoption of K-Means clustering is again found to be more used in comparison to Gaussian Mixture, Agglomerative Hierarchical Approach, and DBScan as shown in Fig.2(c).

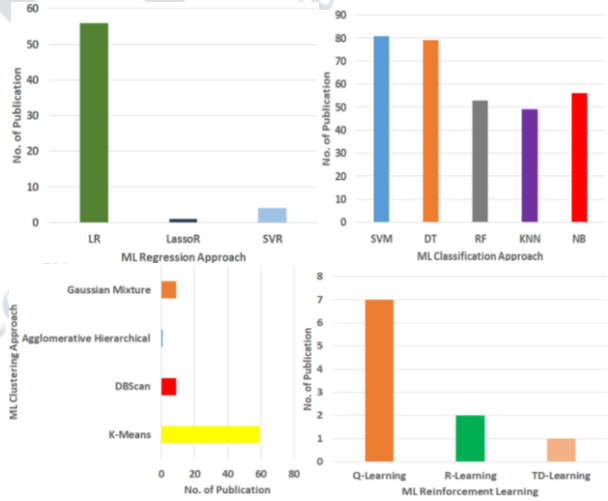


Fig. 2. Research trends for machine learning approach

Finally, there are only 7 publications in Q-Learning approach while 2 publications is observed for R-Learning approach and only 1 publications in Temporal Difference (TD) scheme under reinforcement learning scheme as shown in Fig.2(d).

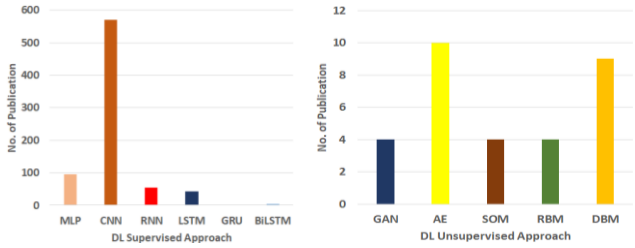
Similar investigation has been carried out towards extracting the supervised and un-supervised methodologies used in deep learning approaches towards IoT security. According to the outcome exhibited in Fig.3(a), it is noted that CNN has the highest number of publications (571) which is significantly higher than other supervised deep learning approaches e.g. bidirectional LSTM (BiLSTM), GRU, GRU, RNN, Multi-layered Perceptron (MLP). Similarly, AE has

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 7 July 2024

witnessed the highest number of publications (10) compared to other unsupervised deep learning approaches viz. Generative Adversarial Network (GAN), Self-Organizing Map (SOM), Restricted Boltzmann ma-chine (RBM), and Deep Belief Network (DBN).



(a) (b)

Fig. 3. Research trends for deep learning approach

D. Usage of Dataset in IoT Security

At present, there are various publicly available dataset utilized towards investigating IoT security modelling. Some of the dataset that are publicly used are as follows:

- **UNSW-NB15, NIMS dataset:** Adoption of this dataset has been reported in work of Mostafa [58] which is used basically for detection of bot attacks. The accuracy scored while using this dataset was observed to be approximately 99%.
- **KDD99 dataset:** This is another frequently used dataset reported in work of Dawoud [59] used mainly for threat detection with accuracy scoring of approximately 94%.
- **NSL-KDD dataset:** This is the most frequently adopted dataset reported to be used by multiple researchers e.g., Angelo [60], Diro [61], Pajouh [62], and Rathod [63]. This dataset is used for anomaly detection over networks as well as determination of presence of varied threat identification and distributed attacks too. The reported accuracy range of using this dataset is within the minimum range of 86% to maximum range of 98%.

Apart from the above-mentioned publicly available standard dataset, there are various research work which encouraged the usage of synthetic dataset too (Azmoodeh [64], Chatterjee [65], Chauhan [66], Li [67]). It was noted that research work carried out using such synthetic dataset offers satisfactory accuracy with minimum range of 93% and maximum range of 99%. Deployment of such synthetic dataset was witnessed towards investigating malware threat detection, botnet attacks, as well as used for solving spam-based classification problems too. Such dataset was also used for solving authentication-based intrusion. There are less studies towards much augmentation work on such dataset too with respect to lethal threats in IoT environment.

E. Identified Research Gap

After reviewing the collected research articles included in the study, it was explored that both the learning schemes in AI has both beneficial perspective as well as limiting attributes too. The study came across certain loopholes that have been found yet unaddressed and has presented them in the form of research gap as follows:

- **Issues with Deep Learning Approaches:** Although adoption of deep learning approaches is found to offer higher accuracy ranges but it still suffers from various problems viz. lack of benchmarking (Sudhakaran [37]). The frequent adoption of CNN is also witnessed with overfitting issues (Jeon [23]), non-applicable to different threats (Zhou et al. [20]), non-inclusion of complex features (Taiwo [21], Zhang [24]), unsolved problem of negative transfer (Okey [25]). Even adoption of LSTM and RNN is also noted with similar form of issues (Zeeshan [31], Ullah [32], Alasmary [30]).
- **Issues with Machine Learning Approaches:** Interestingly, the reviewed papers with machine learning approaches were witnessed with higher accuracy score (~99%); however, issues still exist. Adopted ANN-based approaches are witnessed with introducing computational complexity (Sarkar [43]), lack of benchmarking (Pacheco [44]). The frequently used SVM approach was found to encounter from attack specific solution (Ioannou [46]) and sophisticated learning technique (Jadhav [54]). LR approach is a cost-effective approach but suffers from its less applicability on complex form of network (Subramaniam [49], Li [50]), while NB approach is found for either lower accuracy score (Setiadi [52]) or lack of benchmarking (Majeed [53])
- **Issues with Dataset:** There is a significant shortcoming of the dataset usage too. The usage of UNSW-NB15, NIMS dataset lacks inclusion of relevant features of IoT, while KDD99 dataset is witnessed with sub-optimal performance. Similar issue was also found towards usage of NSL-KDD dataset with inclusion of periodic training and lower accuracy performance. Apart from this, synthetic dataset usage lacks inclusion of various perspective of lethal attacks in IoT.

F. Core Research Implication towards AI in IoT Security

On the basis of the accomplished review findings, there are yet a better scope of using varied forms of AI based learning approaches to overcome the highlighted gaps.

The applicability of AE approaches is not much considered in existing solution towards thwarting IoT threats. Hence, one better possibility will be to investigate the usage of AE scheme focusing more on its unsupervised operation.

Existing studies are not reported towards addressing dynamic threats and one better solution will be to deploy reinforcement learning approach for this purpose. Reinforcement learning is capable of solving complicated issues in the due course of learning; hence, there is a fair possibility of its applicability towards solving dynamic threats in IoT.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 7 July 2024

IV. CONCLUSION

This paper has presented discussion about varied forms of AI-based approaches mainly in the form of machine learning and deep learning approaches that has been used for solving security issues in IoT. The prime contribution of the proposed study are as follows:

The study reviews all the prominent technical implementations associated with both the form of learning approaches in order to realize their beneficial as well as limiting attributes.

One of the significant contributions in this study is in the form of study findings showing that machine learning has been widely adopted compared to deep learning approach.

Updated research trends with exhibits of publications towards each individual standalone approaches involved in both the learning approaches is another significant study contribution.

The identified research gap explored after the deeper insight of the technical implementation of both the form of learning approaches exhibit that there is a wider scope of revision required to solve the security issues in IoT.

The paper also suggests a better scope of improving the learning-based approaches using autoencoders and reinforcement learning towards solving the identified research gap.

V. PROPOSED METHODOLOGY

The direction of future work will to develop a novel form of computational model where the preference will be given to solve the issues of dynamic threats using a novel machine learning algorithm. The idea will be also towards retaining a maximum balance between the optimal security performance and computational efficiency over a large scale IoT network. The proposition towards implementation of proposed methodology will be as follows:

A novel computational framework can be developed that can perform identification of dynamic threats as there are no significant literatures addressing this problem.

Instead of using standalone learning approaches, the proposed methodology can be carried out considering hybrid approach using both machine and deep learning technique that can optimize the threat detection and prevention as well.

An extensive case-study analysis can be carried out considering novel modelling of dynamic threat followed by performing benchmarking with comparison with existing learning-based methods in order to show evidence of possibilities towards resisting dynamic threats practically.

Finally, proposed methodology can be also carried out to optimize the working principle of learning mechanism in order to balance the computational efficiency, communication performance upgrades in IoT use-case, and higher resiliency against dynamic threats.

In simpler form, the proposed study can be classified into detection and optimizing the prevention methodology against potential dynamic adversaries. The detection approach principle of proposed methodology will focus on formulating algorithmic-based adaptive strategy using machine learning for facilitating detection. The prevention approach will further focus on harnessing deep learning method for facilitating granular classification of lethal adversaries in IoT.

REFERENCES

[1] J. C. M. Lai, C. L. Wang, and M. Y. Hsieh, “An Essential Study on IoT Applications on Community Development Association Development Advancement,” An Essential Study on IoT Applications on Community Development Association Development Advancement. Engineering Proceedings, vol. 38, no. 1, 2023.

[2] R. Chataut, A. Phoummalayvane, and R. Akl, “Unleashing the power of IoT: A comprehensive review of IoT applications and future prospects in healthcare, agriculture, smart homes, smart cities, and industry 4.0,” Sensors (Basel), vol. 23, no. 16, 2023, doi: 10.3390/s23167194.

[3] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, “A survey of IoT security based on a layered architecture of sensing and data analysis,” Sensors (Basel), vol. 20, no. 13, p. 3625, 2020, doi: 10.3390/s20133625.

[4] Y.-J. Choi, H.-J. Kang, and I.-G. Lee, “Scalable and secure Internet of things connectivity,” Electronics (Basel), vol. 8, no. 7, p. 752, 2019, doi: 10.3390/electronics8070752.

[5] H. M. Rai, Atik-Ur-Rehman, A. Pal, S. Mishra, and K. K. Shukla, “Use of Internet of Things in the context of execution of smart city applications: a review,” Discov. Internet Things, vol. 3, no. 1, 2023, doi: 10.1007/s43926-023-00037-2.

[6] Z. Muhammad, Z. Anwar, B. Saleem, and J. Shahid, “Emerging cybersecurity and privacy threats to electric vehicles and their impact on human and environmental sustainability,” Energies, vol. 16, 2023.

[7] A. Abdulhamid, S. Kabir, I. Ghafir, and C. Lei, “An Overview of Safety and Security Analysis Frameworks for the Internet of Things,” Electronics, vol. 12, no. 14, 2023.

[8] A. M. Rahmani, S. Bayramov, and B. Kiani Kalejahi, “Internet of Things applications: Opportunities and threats,” Wirel. Pers. Commun., vol. 122, no. 1, pp. 451–476, 2022, doi: 10.1007/s11277-021-08907-0.

[9] M. H. Alsharif, “Green IoT: A review and future research directions,” Symmetry, vol. 15, 2023.

[10] Saqlain, Piao, Shim, and Lee, “Framework of an IoT-based industrial data management for smart manufacturing,” J. Sens. Actuator Netw., vol. 8, no. 2, p. 25, 2019, doi: 10.3390/jsan8020025.

[11] Q. A. Shah, I. Shafi, J. Ahmad, S. Alfarhood, M. Safran, and I. Ashraf, “A meta modeling-based interoperability and integration testing platform for IoT systems,” Sensors (Basel), vol. 23, no. 21, p. 8730, 2023, doi: 10.3390/s23218730.

[12] D. Mendez Mena, I. Papapanagiotou, and B. Yang, “Internet of things: Survey on security,” Inf. Secur. J. Glob. Perspect., vol. 27, no. 3, pp. 162–182, 2018, doi: 10.1080/19393555.2018.1458258.

[13] L. Javed, B. M. Yakubu, M. Waleed, Z. Khaliq, A. B. Suleiman, and N. G. Mato, “BHC-IoT: A Survey on Healthcare IoT Security Issues and Blockchain-Based Solution,” International Journal of Electrical and Computer Engineering Research, vol. 2, no. 4, pp. 1–9, 2022, doi:

10.53375/ijecer.2022.302.

[14] M. H. Ali et al., "Threat analysis and Distributed Denial of Service (DDoS) attack recognition in the Internet of Things (IoT)," Electronics (Basel), vol. 11, no. 3, p. 494, 2022, doi: 10.3390/electronics11030494.

[15] J. H. Kang and M. Seo, "Enhanced Authentication for Decentralized IoT Access Control Architecture," Cryptography, vol. 7, no. 3, 2023.

[16] M. Rana, Q. Mamun, and R. Islam, "Enhancing IoT security: An innovative key management system for lightweight block ciphers," Sensors (Basel), vol. 23, no. 18, 2023, doi: 10.3390/s23187678.

[17] H. Alasmary and M. Tanveer, "ESCI-AKA: Enabling secure communication in an iot-enabled smart home environment using authenticated key agreement framework," Mathematics, vol. 11, 2023.

[18] A. Razaque et al., "Efficient internet-of-things cyberattack depletion using blockchain-enabled software-defined networking and 6G network technology," Sensors (Basel), vol. 23, no. 24, 2023, doi: 10.3390/s23249690.

[19] K. M. Sadique, R. Rahmani, and P. Johannesson, "DIdM-EIoTD: Distributed identity management for edge Internet of Things (IoT) devices," Sensors (Basel), vol. 23, no. 8, 2023, doi: 10.3390/s23084046.

[20] Z. Zhou, H. Yu, and H. Shi, "Human activity recognition based on improved Bayesian convolution network to analyze health care data using wearable IoT device," IEEE Access, vol. 8, pp. 86411–86418, 2020, doi: 10.1109/access.2020.2992584.

[21] O. Taiwo, A. E. Ezugwu, O. N. Oyelade, and M. S. Almutairi, "Enhanced intelligent smart home control and security system based on deep learning model," Wirel. Commun. Mob. Comput., vol. 2022, pp. 1–22, 2022, doi: 10.1155/2022/9307961.

[22] S. More et al., "Security assured CNN-based model for reconstruction of medical images on the internet of healthcare things," IEEE Access, vol. 8, pp. 126333–126346, 2020, doi: 10.1109/access.2020.3006346.

[23] J. Jeon, J. H. Park, and Y.-S. Jeong, "Dynamic analysis for IoT malware detection with convolution neural network model," IEEE Access, vol. 8, pp. 96899–96911, 2020, doi: 10.1109/access.2020.2995887.

[24] P. Zhang, Y. Wang, N. Kumar, C. Jiang, and G. Shi, "A security- and privacy-preserving approach based on data disturbance for collaborative edge computing in social IoT systems," IEEE Trans. Comput. Soc. Syst., vol. 9, no. 1, pp. 97–108, 2022, doi: 10.1109/tcss.2021.3092746.

[25] O. D. Okey, D. C. Melgarejo, M. Saadi, R. L. Rosa, J. H. Kleinschmidt, and D. Z. Rodriguez, "Transfer learning approach to IDS on cloud IoT devices using optimized CNN," IEEE Access, vol. 11, pp. 1023–1038, 2023, doi: 10.1109/access.2022.3233775.

[26] Q. Li, J. Mi, W. Li, J. Wang, and M. Cheng, "CNN-based malware variants detection method for internet of things," IEEE Internet Things J., vol. 8, no. 23, pp. 16946–16962, 2021, doi: 10.1109/jiot.2021.3075694.

[27] M. A. Salahuddin, V. Pourahmadi, H. A. Alameddine, M. F. Bari, and R. Boutaba, "Chronos: DDoS Attack Detection Using Time-Based Autoencoder," IEEE Trans. Netw. Serv. Manag., vol. 19, no. 1, pp. 627–641, 2022, doi: 10.1109/tnsm.2021.3088326.

[28] A. F. Alshudukhi, S. A. Jabbar, and B. Alshaikhdeeb, "A feature selection method based on auto-encoder for internet of things intrusion detection," Int. J. Electr. Comput. Eng. (IJECE), vol. 12, no. 3, p. 3265, 2022, doi: 10.11591/ijece.v12i3.pp3265-3275.

[29] C.-H. Liao, H.-H. Shuai, and L.-C. Wang, "RNN-assisted network coding for secure heterogeneous internet of things with unreliable storage," IEEE Internet Things J., vol. 6, no. 5, pp. 7608–7622, 2019, doi: 10.1109/jiot.2019.2902376.

[30] F. Alasmary, S. Alraddadi, S. Al-Ahmadi, and J. Al-Muhtadi, "ShieldRNN: A distributed flow-based DDoS detection solution for IoT using sequence majority voting," IEEE Access, vol. 10, pp. 88263–88275, 2022, doi: 10.1109/access.2022.3200477.

[31] M. Zeeshan et al., "Protocol-based deep intrusion detection for DoS and DDoS attacks using UNSW-NB15 and bot-IoT data-sets," IEEE Access, vol. 10, pp. 2269–2283, 2022, doi: 10.1109/access.2021.3137201.

[32] I. Ullah and Q. H. Mahmoud, "Design and development of RNN anomaly detection model for IoT networks," IEEE Access, vol. 10, pp. 62722–62750, 2022, doi: 10.1109/access.2022.3176317.

[33] L. Vu, Q. U. Nguyen, D. N. Nguyen, D. T. Hoang, and E. Dutkiewicz, "Deep transfer learning for IoT attack detection," IEEE Access, vol. 8, pp. 107335–107344, 2020, doi: 10.1109/access.2020.3000476.

[34] S. J. Lee et al., "IMPACT: Impersonation attack detection via edge computing using deep autoencoder and feature abstraction," IEEE Access, vol. 8, pp. 65520–65529, 2020, doi: 10.1109/access.2020.2985089.

[35] X. Zhou, W. Liang, W. Li, K. Yan, S. Shimizu, and K. I.-K. Wang, "Hierarchical adversarial attacks against graph-neural-network-based IoT network intrusion detection system," IEEE Internet Things J., vol. 9, no. 12, pp. 9310–9319, 2022, doi: 10.1109/jiot.2021.3130434.

[36] M.-Q. Tran et al., "Reliable deep learning and IoT-based monitoring system for secure computer numerical control machines against cyber-attacks with experimental verification," IEEE Access, vol. 10, pp. 23186–23197, 2022, doi: 10.1109/access.2022.3153471.

[37] P. Sudhakaran, C. Malathy, T. H. Vardhan, and T. Sainadh, "Detection of malware from IOT devices using deep learning techniques," J. Phys. Conf. Ser., vol. 1818, no. 1, p. 012219, 2021, doi: 10.1088/1742-6596/1818/1/012219.

[38] M. Savic et al., "Deep learning anomaly detection for cellular IoT with applications in smart logistics," IEEE Access, vol. 9, pp. 59406–59419, 2021, doi: 10.1109/access.2021.3072916.

[39] N. M. Yungaicela-Naula, C. Vargas-Rosales, and J. A. Perez-Diaz, "SDN-based architecture for transport and application layer DDoS attack detection by using machine and deep learning," IEEE Access, vol. 9, pp. 108495–108512, 2021, doi: 10.1109/access.2021.3101650.

[40] A. R. Zarzoor, N. A. Shiltagh Al-Jamali, and D. A. Abdul Qader, "Intrusion detection method for internet of things based on the spiking neural network and decision tree method," Int. J. Electr. Comput. Eng. (IJECE), vol. 13, no. 2, p. 2278, 2023, doi: 10.11591/ijece.v13i2.pp2278-2288.

[41] M. A. Ferrag, L. Maglaras, A. Ahmim, M. Derdour, and H. Janicke, "RDTIDS: Rules and decision tree-based intrusion detection system for Internet-of-Things networks," Future Internet, vol. 12, no. 3, p. 44, 2020, doi: 10.3390/fi12030044.

[42] S. Latif, Z. Zou, Z. Idrees, and J. Ahmad, "A novel attack detection scheme for the industrial internet of things using a lightweight random neural network," IEEE Access, vol. 8, pp. 89337–89350, 2020, doi: 10.1109/access.2020.2994079.

[43] A. Sarkar, M. M. Singh, M. Z. Khan, and O. H. Alhazmi, "Nature-inspired gravitational search-guided artificial neural key exchange for IoT security enhancement," IEEE Access, vol. 9, pp. 76780–76795, 2021, doi: 10.1109/access.2021.3082262.

[44] J. Pacheco, V. H. Benitez, L. C. Felix-Herran, and P. Satam, "Artificial neural networks-based intrusion detection system for internet of things fog nodes," IEEE Access, vol. 8, pp. 73907–73918, 2020, doi: 10.1109/access.2020.2988055.

[45] H. A. Al-Mohammed et al., "Machine learning techniques for detecting attackers during quantum key distribution in IoT networks with application to railway scenarios," IEEE Access, vol. 9, pp. 136994–137004, 2021, doi: 10.1109/access.2021.3117405.

[46] C. Ioannou and V. Vassiliou, "Network attack classification in IoT using support vector machines," J. Sens. Actuator Netw., vol. 10, no. 3, p. 58, 2021, doi: 10.3390/jsan10030058.

[47] E. E. I and J. C. Clement, "GRU-SVM based threat detection in cognitive radio network," Sensors (Basel), vol. 23, no. 3, p. 1326, 2023, doi: 10.3390/s23031326.

[48] M. Bagaa, T. Taleb, J. B. Bernabe, and A. Skarmeta, "A machine learning security framework for iot systems," IEEE Access, vol. 8, pp. 114066–114077, 2020, doi: 10.1109/access.2020.2996214.

[49] A. K. Subramanian, A. Samanta, S. Manickam, A. Kumar, S. Shiaeles, and A. Mahendran, "Linear Regression Trust Management System for IoT systems," Cybern. Inf. Technol., vol. 21, no. 4, pp. 15–27, 2021, doi: 10.2478/cait-2021-0040.

[50] F. Li, A. Shinde, Y. Shi, J. Ye, X.-Y. Li, and W. Song, "System statistics learning-based IoT security: Feasibility and suitability," IEEE Internet Things J., vol. 6, no. 4, pp. 6396–6403, 2019, doi: 10.1109/jiot.2019.2897063.

[51] O. Korystin, State Scientifically Research Institute of the MIA of Ukraine, Kyiv, Ukraine, S. Nataliia, and O. Mitina, "Risk forecasting of data confidentiality breach using linear regression algorithm," Int. J. Comput. Netw. Inf. Secur., vol. 14, no. 4, pp. 1–13, 2022, doi: 10.5815/ijcnis.2022.04.01.

[52] F. F. Setiadi, M. W. A. Kesiman, and K. Y. E. Aryanto, "Detection of dos attacks using naive bayes method based on internet of things (iot)," J. Phys. Conf. Ser., vol. 1810, no. 1, p. 012013, 2021, doi: 10.1088/1742-6596/1810/1/012013.

[53] R. Majeed, N. A. Abdullah, and M. F. Mushtaq, "IoT-based Cyber-security of Drones using the Naïve Bayes Algorithm," Int. J. Adv. Comput. Sci. Appl., vol. 12, no. 7, 2021, doi: 10.14569/ijacsa.2021.0120748.

[54] A. D. Jadhav and V. Pellakuri, "Highly accurate and efficient two phase-intrusion detection system (TP-IDS) using distributed processing of HADOOP and machine learning techniques," J. Big Data, vol. 8, no. 1, 2021, doi: 10.1186/s40537-021-00521-y.

[55] Y. Wu, X. Jin, H. Yang, L. Tu, Y. Ye, and S. Li, "Blockchain-based Internet of Things: Machine learning tea sensing trusted traceability system," J. Sens., vol. 2022, pp. 1–16, 2022, doi: 10.1155/2022/8618230.

[56] K. Yadav and B. B. Gupta, "Clustering based rewarding algorithm to detect adversaries in federated machine learning based IoT environment," in 2021 IEEE International Conference on Consumer Electronics (ICCE), IEEE, 2021.

[57] N. Kammoun, R. Abassi, and S. Guemara, "Towards a new clustering algorithm based on trust management and edge computing for IoT," in 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), IEEE, 2019.

[58] N. Moustafa, B. Turnbull, and K.-K.-R. Choo, "An ensemble intrusion detection technique based on proposed statistical _ow features for protecting network traf_c of Internet of Things," IEEE Internet Thing J, vol. 6, no. 3, pp. 4815–4830, 2019.

[59] A. Dawoud, S. Shahristani, and C. Raun, "Deep learning and software-defined networks: Towards secure IoT architecture," Internet of Things, vol. 3–4, pp. 82–89, 2018, doi: 10.1016/j.iot.2018.09.003.

[60] G. D'angelo, F. Palmieri, M. Ficco, and S. Rampone, "An uncertainty-managing batch relevance-based approach to network anomaly detection," Appl. Soft Comput., vol. 36, pp. 408–418, 2015, doi: 10.1016/j.asoc.2015.07.029.

[61] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," Future Gener. Comput. Syst., vol. 82, pp. 761–768, 2018, doi: 10.1016/j.future.2017.08.043.

[62] H. H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha, and K.-K. R. Choo, "A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks," IEEE Trans. Emerg. Top. Comput., vol. 7, no. 2, pp. 314–323, 2019, doi: 10.1109/tetc.2016.2633228.

[63] S. Rathore and J. H. Park, "Semi-supervised learning based distributed attack detection framework for IoT," Appl. Soft Comput., vol. 72, pp. 79–89, 2018, doi: 10.1016/j.asoc.2018.05.049.

[64] A. Azmoodeh, A. Dehghantanha, and K.-K.-R. Choo, "Robust malware detection for Internet of (battle_eld) Things devices using deep eigenspace learning," IEEE Trans. Sustain. Comput, vol. 4, no. 1, pp. 88–95, 2019.

[65] B. Chatterjee, D. Das, S. Maity, and S. Sen, "RF-PUF: Enhancing IoT security through authentication of wireless nodes using in-situ machine learning," arXiv [cs.CR], 2018. [Online]. Available: http://arxiv.org/abs/1805.01374.

[66] J. Chauhan, S. Seneviratne, Y. Hu, A. Misra, A. Seneviratne, and Y. Lee, "Breathing-based authentication on resource-constrained IoT devices using recurrent neural networks," Computer (Long Beach Calif.), vol. 51, no. 5, pp. 60–67, 2018, doi: 10.1109/mc.2018.2381119.

[67] W. Li, W. Meng, Z. Tan, and Y. Xiang, "Design of multi-view based email classification for IoT systems via semi-supervised learning," J. Netw. Comput. Appl., vol. 128, pp. 56–63, 2019, doi: 10.1016/j.jnca.2018.12.002.