

# Learning methodologies towards leveraging security resiliency in internet-of-things environment

Sowmya Somanath<sup>1,2</sup>, Usha Banavikal Ajay<sup>3</sup>

<sup>1</sup>Department of Computer Science and Engineering, BMS Institute of Technology and Management, Visvesvaraya Technological University, Belagavi, India

<sup>2</sup>School of Computer Science and Engineering, REVA University, Yelahanka Bangalore, India

<sup>3</sup>Department of Information Science and Engineering, BMS Institute of Technology and Management, Visvesvaraya Technological University, Belagavi, India

## Article Info

### Article history:

Received Nov 28, 2023

Revised Feb 9, 2024

Accepted Mar 2, 2024

### Keywords:

Deep learning  
Internet-of-things  
Intrusion detection  
Machine learning  
Security

## ABSTRACT

The evolution of artificial intelligence (AI) has facilitated a significant contribution of machine learning and deep learning in order to improve the security features of large internet-of-things (IoT) environment. Since last decade there has been different variants of learning-based methodologies towards leveraging security improvements among communication in IoT devices; however, it is yet to know the strength and weakness of them. Hence, this paper presents a review of security methodologies adopted in machine learning and deep learning-based techniques in IoT to understand the degree of resiliency and effectiveness of these techniques. The paper further contributes towards highlighting the current methodologies with respect to benefits and limiting factors along with exclusive highlights of research trends while the research gap explored assists in offering these insights. The distinct findings of the study assist in paving the work direction in future by harnessing better form of learning scheme.

*This is an open access article under the [CC BY-SA](#) license.*



## Corresponding Author:

Sowmya Somanath

School of Computer Science and Engineering, REVA University

Rukmini Knowledge Park, Yelahanka, Kattigenahalli, Bengaluru, Karnataka 560064, India

Email: sowmyasadish@gmail.com

## 1. INTRODUCTION

The internet-of-things (IoT) offers a comprehensive deployment of larger number of heterogeneous connected nodes in order to formulate a well-developed networked system. With a vast number of projected applications in IoT, the number of evolving applications is still on rise [1]. However, there are some of the potential issues too associated with it. The first challenge is associated with the weaker's authentication which renders the IoT devices exposed to various vulnerable threats and attacks [2]. Different types of IoT devices also lacks robust and sustainable encryption schemes which let the malicious node to intrude the network by bypassing the weaker security system and gain an illegitimate access to the sensitive and confidential information [3]. Apart from this, the processing power is quite limited within an IoT device which renders inapplicability towards processing high end algorithms towards intrusion detection system. At present, the manufacturing of the IoT devices is carried out using varied ranges of software and hardware which has a reported cases of vulnerabilities while the security updates in the form of patches may not be facilitated by the manufacturers. Further, a distributed nature of IoT makes the nodes working at different geographical location that are interconnected with different network using different set of protocols, which cannot be controlled so effectively in case of serious threats [4]. Needless to mention that human factor is another reason for multiple security breaches in IoT. It is to be noted that there are various study models

towards strengthening IoT security in current times using different methodologies; however, the prime obstacle of successful implementation of same models in practical scenario is less assessed due to complexity associated with it. IoT system is characterized by high end complexity where incorporating a potential security solution can be carried out only by expertise in multiple advanced areas of cryptography, network security, software development, and hardware design. From the perspective of solution towards IoT security, machine learning approach has proven to its higher degree of effectiveness that emphasized on algorithms and data using artificial intelligence (AI) for better solutions. Machine learning offers a set of features which is useful for protecting the IoT devices as well as network from multiple forms of threats [5].

Following are the set of problems associated with implying machine learning for IoT security viz. i) the explainability and interpretability of machine learning models are quite challenging for large IoT security, ii) adversarial attacks are still the large level of security problems in machine learning models which leads to outliers by tampering the data in order to deceive the learning algorithm, iii) resource constraint has been always a bigger impediment to implement even a strongest encryption algorithm or iterative learning schemes, iv) machine learning algorithm performance is highly sensitive towards the data quality, v) the success of accuracy towards detection and mitigation largely depends upon training data, which may not be facilitated in large IoT environment in security perspective.

For the purpose of realization of above-mentioned problem statement, it is necessary to brief relevant literatures. Several researchers have presented discussion of solution and issues associated with IoT threats [6], [7]. Al-Garadi *et al.* [8] have presented discussion about various security methods lined with both machine learning and deep learning followed by highlights of comprehensive evaluation of security trends in [9], [10]. Nguyen *et al.* [11] have discussed about usage of federated learning approach while discussion of reinforcement learning-based approach is discussed in [12], [13] towards IoT security. Wu *et al.* [14] have presented discussion about AI based security solutions, while Zhou *et al.* [15] have presented discussion of methodologies to identify bugs in systems and platforms in IoT.

From the insight of the research-based articles, it is clear that there are various deployment of learning-based scheme targeting protection of IoT security; however, there is a need to further update the information with latest studies as well as there is need to explicitly identify the degree of effectiveness in existing studies. Therefore, the proposed manuscript presents a compact and yet resourceful information associated with strength and weakness of current significant methodologies of both machine and deep learning approaches for IoT security. The new value added in this work are i) explicit highlights of machine/deep learning approaches with respect to specific problems being addressed, advantage, and limitation, ii) compact snapshot of current research trend, iii) arriving at research gap as the prime contribution of study, and iv) inferring learning outcomes of proposed study to be helpful for upcoming research work direction.

## 2. METHODOLOGY

The prime intention of the proposed study is to carry out review of effectiveness associated with the learning-based algorithms and methodologies involved in accomplishing a common goal of optimal IoT security. For this purpose, this review study has adopted a desk research methodology [16] exhibited in Figure 1. According to adopted research methodology, the preliminary search was carried out from Google Scholar as well as reputed technical journal publications. The next step of the adopted method is to perform an initial filtering on the basis of inclusion and exclusion criteria. The primary inclusion criteria of filtering are that the published article to mainly posse's methodological elaboration with results accomplished in order to understand the effectiveness of approach. The second inclusion criteria also consider the research articles with technical implementation published between 2013-2023.

The third inclusion criteria are that research articles are only associated with either machine learning or deep learning as the core implementation. The exclusion criteria are any theoretical papers without results or implementation model and papers published before 2013. Also, the exclusion criteria include any paper which has used non-learning-based approach towards improving IoT security as the target of this paper is to understand the potential of learning-based schemes. The next round of the operation is to perform removal of the duplicates. The proposed method considers duplicated as i) same author with two extended study models, ii) usage of exactly similar concept in two different research articles is also considered as duplicates as the idea is to obtain completely unique study model. The preliminary search yield approximately 31,000 results, while the initial filtering has resulted in 270 paper. Finally, the removal of the duplicates has resulted in 54 number of research articles which has been reviewed in this manuscript. The learning outcome of the proposed study further contributes towards exploring research gap, research trend, and exploring distinct study findings.

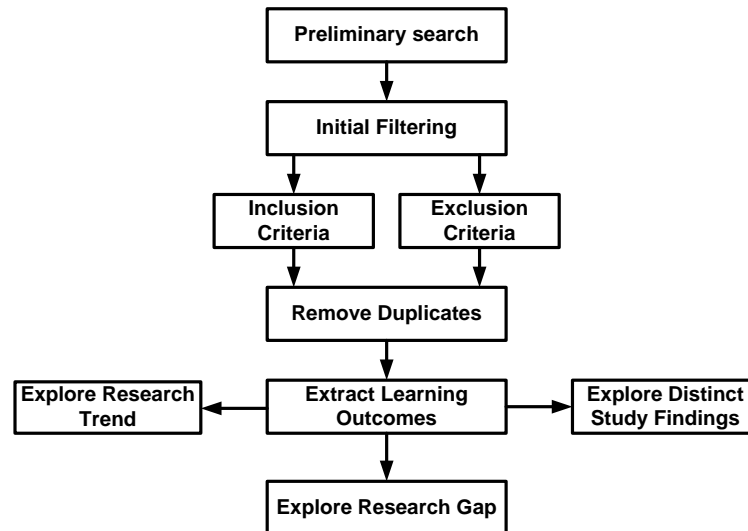


Figure 1. Method adopted in proposed study

### 3. RESULTS

This section presents discussion about the various learning-based techniques which were utilized for identifying and preventing various forms of threats and thereby acted as a unique threat mitigation scheme in IoT environment. It has been also noted that adoption of learning-based schemes is of varied forms where some of the study models have used individual learning scheme while some of them has used a combined implementation of learning schemes. Broadly, it is classified into machine learning and deep learning-based schemes towards threat mitigation in an IoT environment. This section showcases the outcome of these reviewed approaches.

#### 3.1. Literature survey for machine learning scheme

The study model of Majeed *et al.* [17] have used naïve Bayes along with blockchain for detecting the security threats in the data captured by the drone. Adoption of naïve Bayes was also witnessed in work of Setiadi *et al.* [18] in order to identify the denial-of-service (DoS) attack in IoT. However, the work carried out by Jadhav and Pellakuri [19] have developed a detection scheme by integrating naïve Bayes with other learning approaches e.g., support vector machine (SVM), and K-nearest neighbor (KNN), which are also another variant of classification algorithms in machine learning.

Existing IoT security approaches have also been reported to use logistic regression (LR). Korystin *et al.* [20] have used LR method towards assessing predictive risk associated with the data of cybersecurity. Li *et al.* [21] have developed a LR-based scheme in order to identify the anomaly in the system behaviour in IoT using statistical learning scheme of neural network. Adoption of LR is also reported in work of Subramanian *et al.* [22] towards developing a trust model for identifying the malicious node. Further, clustering approaches has been reported in machine learning approach towards grouping the types of identified threat. Kammoun *et al.* [23] have presented a unique clustering approach towards strengthening the trust system in IoT powered by edge computing. Further adoption of clustering approach is also carried out by Yadav and Gupta [24] where a reward system has been introduced in order to promote the detection system. The scheme has also used federated learning for increasing the detection accuracy. The work carried out by Wu *et al.* [25] have presented a unique scheme of machine learning integrated with blockchain for tracing the trust factor. The multiple learning models of random forest, AdaBoost, and decision tree ensembled with boosting.

Apart from this, SVM is another frequently used classification approach towards addressing security concerns in IoT. Bagaa *et al.* [26] have used single class SVM for classifying the threats along with using network virtualization and software defined network (SDN). Ezhilarasi and Clement [27] have used SVM along with gated recurrent unit (GRU) in order to difference between malicious and legitimate user in cognitive radio network, which is another integral part of an IoT system. Ioannou and Vassiliou [28] have presented a unique mechanism to implement SVM for identifying the normal and abnormal behaviour in IoT associated with anomaly detection. Existing scheme has also witnessed usage of artificial neural network (ANN) for improving security performance in IoT. Al-Mohammed *et al.* [29] have integrated ANN with deep

learning technique in order to secure the key distribution process in IoT by detecting the presence of attacker. Pacheco *et al.* [30] have also used ANN for identifying intrusion towards the fog nodes in IoT by investigating the adaptive behaviour of nodes. Further, Sarkar *et al.* [31] have presented a scheme where ANN is combinely used with nature-inspired search technique for solving key exchange problem in IoT. Further, adoption of random neural network is seen in work of Latif *et al.* [32] in order to predict the detection of an attacker in industrial IoT use case. Ferrag *et al.* [33] have used decision tree integrated with rule-based scheme in order to develop a unique classifier for attack detection in IoT. Adoption of decision tree approach is also seen in work of Zarzoor *et al.* [34] where decision tree is integrated with spiking neural network for minimizing latency while performing predictive attack detection.

### 3.2. Literature survey for deep learning scheme

Apart from machine-learning based schemes, adoption of deep learning scheme is equivalently on rise towards improving the security features in IoT. Alasmay *et al.* [35] have deployed recurrent neural network (RNN) and long short-term memory (LSTM) for identifying distributed denial-of-service (DDoS). The study model emphasized more on classification of the DDoS attacks. Further adoption of RNN is reported in work of Liao *et al.* [36] towards securing the unreliable storage units in IoT. The model has used network coding for this purpose. Nearly similar like of research work is also witnessed in the study model of Ullah and Mahmoud [37] where an anomaly detection model has been developed using RNN. This scheme has used GRU along with birectional long short-term memory (BiLSTM), and conventional LSTM for this purpose. The study has been assessed with multiple standard datasets to find its higher accuracy in its threat detection performance. Zeeshan *et al.* [38] have developed a scheme to identify both DoS and DDoS attack on specific dataset of IoT. The scheme has used LSTM for this purpose of detection under varied threat scheme while the study has selected equal number of data packets from different threat categories in order to address the overfitting problem.

Adoption of autoencoder towards detection of intrusion is carried out by Alshudukhi *et al.* [39] with an idea to select the feature that can contribute towards treat identification. Study towards similar direction is also carried out by Lee *et al.* [40] in order to identify the impersonation attack. Further adoption of autoencoder along with consideration of temporate attribute was reported in work of Salahuddin *et al.* [41] where the study model targets to identify the DDoS attack. The study model uses multiple time window considering temporal-based attributes rowards identifying anomaly behaviour of DDoS attackers. It is also noted that integration of autoencoder and transfer learning too offers a better attack detection performance as noted in work of Vu *et al.* [42]. The predictive model is capable of analyzing both labelled and unlabelled data acquired from multiple IoT devices using two type soft autoencoders in both supervised and unsupervised form. Further, the hidden representation of unsupervised autoencoder is subjected to transfer learning that is further used for detection of attacks.

In the area of deep learning, convolution neural network (CNN) is another frequently deployed threat detection scheme in IoT. Jeon *et al.* [43] have developed a security model using CNN for dynamically investigating propagation of malware in nested environment of cloud. Adoption of CNN is also reported in work of Li *et al.* [44] towards identification of malware in IoT. The study model revises CNN scheme by integrating spatial pyramid pooling with self-attention approach towards classifying different variants of malwares. Another model developed by More *et al.* [45] have used CNN with a core idea of this implementation is to ensure secure transmission of medical images in IoT along with resolving the computational speed towards processing large number of images. Existing scheme has also witnessed deployment of optimized version of CNN by adding transfer learning for improving security threat detection as noted in work of Okey *et al.* [46]. The model has also implemented quantile transformer for finetuning the feature vector obtained from images which are then subjected to ensemble algorithms of transfer learning. Another unique adoption of deep learning towards leveraging IoT security was seen in work carried out by Taiwo *et al.* [47]. The study has used CNN for detection of intrusion associated with the automation of home. Zhang *et al.* [48] have constructed a security model towards strengthenin the privacy of the data considering social IoT environment. The study has used CNN integrated with firefly algorithm in order to accomplish the security features. The firefly algorithm is used for generating adversarial sample while CNN is used for analyzing similarity of the data. Zhou *et al.* [49] have used enhanced Bayesian convolution network for improving the predictive quality of data in wearable IoT.

There are also studies where machine learning and deep learning has been combinely used to mitigate the potential threat in IoT [50]-[54]. The frequently identified limitation of all the studies is lack of benchmarking, usage of sophisticated learning approach, lack of extensive analysis to prove, not applicable for complex intrusion, not applicable for dynamic attackers, and accuracy depends upon dataset size, induces complexity for large network.

### 3.3. Research trend

This part of study will only emphasize towards understanding the trends of adoption of machine learning and deep learning-based schemes towards effective threat control in IoT. A closer look into the Table 1 showcases that there are a greater number of research articles published for machine learning-based approaches total 42,040 publications, in comparison to deep learning-based approaches total 35,585 publications in IoT. These outcomes of publications correspond to research articles published during 2013-2023 only. Table 1 showcases that there are approximately 63 implementation approaches for classification methods, 20 approaches of regression, 19 approaches for clustering, and approximately 3 approaches for reinforcement based IoT security solution. Number of studies using regression-based machine learning approaches are still very less to be noticed. Further, it was seen that adoption of supervised deep learning methods (approximated mean number of publications = 128) are fairly more in contrast to that of unsupervised deep learning methods (approximated mean number of publications = 6) towards addressing security issues in IoT as seen in Table 2.

Table 1. Frequently used approaches in machine learning-based IoT security models

Classification	No. of publication
Support vector machine	81
Decision tree	79
Random forest	53
K-nearest neighbor	49
Naïve Bayes	56
Regression	No. of publication
Logistic regression	56
Lasso regression	1
Support vector regression	4
Clustering	No. of publication
K-Means	59
DBScan	9
Agglomerative hierarchical	1
Gaussian mixture	9
Reinforcement learning	No. of publication
Q-Learning	7
R-Learning	2
Temporal difference-learning	1

Table 2. Frequently used approaches in deep learning-based IoT security models

Supervised	No. of publication	Unsupervised	No. of publication
Multilayered-perceptron	96	Generative adversarial network	4
CNN	571	Autoencoder	10
RNN	54	Self-organizing map	4
LSTM	43	Restricted Boltzman machine	4
GRU	2	Deep belief network	9
BiLSTM	3		

### 3.4. Research gap

There is no denying the fact that a significant number of research work has been carried out towards strengthening the IoT security system in modern era where machine learning schemes acts as a significant contributor. Irrespective of evolving dedicated research contribution, there are various open-ended shortcoming which are required to be addressed. Following are some of the significant research gap identified from the proposed review work:

- Issues with data acquisition and analysis: majority of the existing approaches using machine learning has been witnessed to directly subject its algorithm either on publicly available dataset or on its synthetic data. This task is carried out without any realization that IoT environment is usually massive and potentially generates unstructured data which further poses potential challenges in analytical operations. Hence, the higher ranges of acquired accuracy is not rationalized with adopted dataset in existing machine learning-based techniques on IoT security.
- Lack of device constraint modelling: the different ranges of devices used in IoT doesn't have much resources nor the processing capability. Apart from this, the processing power is highly limited. Adoption of deep learning-based scheme as well as iterative machine learning will always demands higher processing power which cannot be facilitated owing to lack of device constraint modelling. There are few reported studies where different constraints of device has been considered in implementation.

- Non-inclusion of compatibility factors: there is no doubt that both machine and deep learning-based approaches towards identifying and mitigating IoT security is quite proven productive. However, there are various variants of learning schemes within the above two standard mechanism which has different working principle. For an example, the studies using decision tree approach may yield better result in normal IoT scenario, however, when the scenario becomes complex with sophisticated variables, they suffer from overfitting. At the same time, KNN-based approach may offer better classification accuracy but they demand higher memory. Similarly, RNN and CNN offers robust anomaly detection with highest accuracy; however, they have dependency of labelled data as well as specific set of computational resources in order to carry out training.
- Less effective privacy preservation: there are various studies carried out towards privacy preservation in IoT security; however, such models are designed under restricted research environment. On the other hand, the aggregation and transmission of data by an IoT device in practical scenario lacks such consideration on higher scale of deployment. At the sametime, when such higher sensitive information is exposed to learning algorithm for training purpose, the algorithms itself is at risk. Current, no benchmarked model is stated to resist learning-based approach to go rogue.
- Less emphasis towards computational burden: almost all the studies carried out using learning-based scheme emphasized towards accomplishing a superior accuracy; however, there is less justification offered to state the reduced computational effort or burden. Accuracy accomplishment may offer better security service but practical viability of the study model cannot be offered without benchmarking or without proving reduction in computational burden over extensive test environment.

#### 4. CONCLUSION

This paper has presented discussion about the effectiveness of machine learning as well as deep learning approaches towards identifying the threats and mitigating them in an IoT environment. Following are some of the essential findings of the study: i) the security system used by machine learning models are found to learn towards mapping the input to the output for detecting the anomalies or threatful pattern of the data. ii) the security solutions introduced by deep learning approaches is mainly witnessed to deploy a neural network-based approach in order to perform learning and constructing decision towards threat detection. It was also noted that deep learning models are found to offer an advantage from its counterpart machine learning models by making themselves independent of linear models. Various forms of complex operations can be handled by the deep learning model with an aid of activation function of non-linear forms over every layer of neural network. iii) both the AI approaches is characterized by dependencies of performing an iterative and training operation which largely demands either higher central processing unit (CPU) for machine learning or graphics processing unit (GPU) for deep learning. Unfortunately, such a large demand of resources for performing analytical operation is not suitable for resource-constraint sensor nodes. Existing security mechanism has showcased the accomplishment of accuracy, however, there is no much potential evidence for their viability when exposed to dynamic practical environment. iv) apart from DDoS attack, which is highly frequent in IoT environment, there are also evolving number of attacks i.e., botnets, malware, side-channel attack, domain name server (DNS) spoofing, man-in-middle attack, and physical attack, which has not received much attention in the form of solution. v) majority of the security solution presented in existing studies are highly specific of attack model, which renders inapplicability of those models when exposed to different attack environment. As IoT is a large network of heterogeneous IoT devices and protocols, a security solution must be intelligent enough to understand the vulnerability and resist them. vi) existing security solutions using learning-based approach has been developed using pre-defined information of attack strategies which doesn't work when encountered with dynamic form of attackers. The future work will be indirection towards improving machine learning scheme for developing better form of evolving security approaches in IoT. Further, the study can be to optimize the deep learning autoencoders which can offer better data quality and reliability towards deep learning approach. Hence, a hybrid scheme can be designed for IoT security.

#### REFERENCES




- [1] M. H. Ali, M. M. Jaber, S. K. Abd, A. Alkhayat, M. R. Q, and M. H. Ali, "Application of internet of things-based efficient security solution for industrial," *Production Planning & Control*, pp. 1–15, 2023, doi: 10.1080/09537287.2023.2169647.
- [2] S. Yempally, S. K. Singh, and V. Sarveshwaran, "A secure and efficient authentication and multimedia data sharing approach in IoT-healthcare," *Imaging Science Journal*, vol. 71, no. 3, pp. 277–298, 2023, doi: 10.1080/13682199.2023.2180140.
- [3] H. N. Khan, A. Das, and A. Chaudhuri, "Unique video encryption technique intended for smart city application," *IETE Journal of Research*, vol. 69, no. 9, pp. 5830–5839, 2023, doi: 10.1080/03772063.2023.2190543.
- [4] J. Bacquet, R. Riemenschneider, and P. W. -Jensen, "Future trends in IoT," in *Next Generation Internet of Things – Distributed Intelligence at the Edge and Human-Machine Interactions*, New York: River Publishers, 2022, pp. 9–17. doi: 10.1201/9781003338963-2.

- [5] L. Sana, M. M. Nazir, M. Iqbal, L. Hussain, and A. Ali, "Anomaly detection for cyber internet of things attacks: a systematic review," *Applied Artificial Intelligence*, vol. 36, no. 1, Dec. 2022, doi: 10.1080/08839514.2022.2137639.
- [6] P. Anand, Y. Singh, A. Selwal, M. Alazab, S. Tanwar, and N. Kumar, "IoT vulnerability assessment for sustainable computing: threats, current solutions, and open challenges," *IEEE Access*, vol. 8, pp. 168825–168853, 2020, doi: 10.1109/ACCESS.2020.3022842.
- [7] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/access.2019.2924045.
- [8] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (IoT) security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020, doi: 10.1109/comst.2020.2988293.
- [9] Y. Harbi, Z. Aliouat, A. Refoufi, and S. Harous, "Recent security trends in internet of things: a comprehensive survey," *IEEE Access*, vol. 9, pp. 113292–113314, 2021, doi: 10.1109/ACCESS.2021.3103725.
- [10] P. L. S. Jayalaxmi, R. Saha, G. Kumar, M. Conti, and T.-H. Kim, "Machine and deep learning solutions for intrusion detection and prevention in IoTs: a survey," *IEEE Access*, vol. 10, pp. 121173–121192, 2022, doi: 10.1109/ACCESS.2022.3220622.
- [11] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. Vincent Poor, "Federated learning for internet of things: a comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1622–1658, 2021, doi: 10.1109/comst.2021.3075439.
- [12] A. Uprety and D. B. Rawat, "Reinforcement learning for IoT security: a comprehensive survey," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8693–8706, 2021, doi: 10.1109/IIOT.2020.3040957.
- [13] M. Venkatasubramanian, A. H. Lashkari, and S. Hakak, "IoT malware analysis using federated learning: a comprehensive survey," *IEEE Access*, vol. 11, pp. 5004–5018, 2023, doi: 10.1109/ACCESS.2023.3235389.
- [14] H. Wu, H. Han, X. Wang, and S. Sun, "Research on artificial intelligence enhancing internet of things security: a survey," *IEEE Access*, vol. 8, pp. 153826–153848, 2020, doi: 10.1109/ACCESS.2020.3018170.
- [15] W. Zhou *et al.*, "Reviewing IoT security via logic bugs in IoT platforms and systems," *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11621–11639, Jul. 2021, doi: 10.1109/IIOT.2021.3059457.
- [16] Y. Kunneman, M. A. D. M. -Filho, and J. V. D. Waa, "Data science for service design: an introductory overview of methods and opportunities," *The Design Journal*, vol. 25, no. 2, pp. 186–204, 2022, doi: 10.1080/14606925.2022.2042108.
- [17] R. Majeed, N. A. Abdullah, and M. F. Mushtaq, "IoT-based cyber-security of drones using the naïve Bayes algorithm," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 7, 2021, doi: 10.14569/ijacsa.2021.0120748.
- [18] 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)," *Journal of Physics: Conference Series*, vol. 1810, no. 1, 2021, doi: 10.1088/1742-6596/1810/1/012013.
- [19] 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," *Journal of Big Data*, vol. 8, no. 1, 2021, doi: 10.1186/s40537-021-00521-y.
- [20] O. Korystin, S. Nataliia, and O. Mitina, "Risk forecasting of data confidentiality breach using linear regression algorithm," *International Journal of Computer Network and Information Security*, vol. 14, no. 4, pp. 1–13, Aug. 2022, doi: 10.5815/ijcnis.2022.04.01.
- [21] 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 of Things Journal*, vol. 6, no. 4, pp. 6396–6403, 2019, doi: 10.1109/IIOT.2019.2897063.
- [22] A. K. Subramanian, A. Samanta, S. Manickam, A. Kumar, S. Shialeles, and A. Mahendran, "Linear regression trust management system for IoT systems," *Cybernetics and Information Technologies*, vol. 21, no. 4, pp. 15–27, 2021, doi: 10.2478/cait-2021-0040.
- [23] N. Kammoun, R. Abassi, and S. Guemara, "Towards a new clustering algorithm based on trust management and edge computing for IoT," *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*. IEEE, 2019, doi: 10.1109/iwcmc.2019.8766492.
- [24] 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, Jan. 2021, pp. 1–6, doi: 10.1109/ICCE50685.2021.9427586.
- [25] 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," *Journal of Sensors*, vol. 2022, pp. 1–16, 2022, doi: 10.1155/2022/8618230.
- [26] 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.
- [27] I. E. Ezhilarasi and J. C. Clement, "GRU-SVM based threat detection in cognitive radio network," *Sensors*, vol. 23, no. 3, Jan. 2023, doi: 10.3390/s23031326.
- [28] C. Ioannou and V. Vassiliou, "Network attack classification in IoT using support vector machines," *Journal of Sensor and Actuator Networks*, vol. 10, no. 3, 2021, doi: 10.3390/jsan10030058.
- [29] 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.
- [30] J. Pacheco, V. H. Benitez, L. C. F. -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.
- [31] 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.
- [32] 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.
- [33] 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, 2020, doi: 10.3390/fi12030044.
- [34] A. R. Zaroor, N. A. S. Al-Jamali, and D. A. A. Qader, "Intrusion detection method for internet of things based on the spiking neural network and decision tree method," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 2, pp. 2278–2288, 2023, doi: 10.11591/ijece.v13i2.pp2278-2288.
- [35] 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.
- [36] 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 of Things Journal*, vol. 6, no. 5, pp. 7608–7622, 2019, doi: 10.1109/IIOT.2019.2902376.
- [37] 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.
- [38] 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.
- [39] A. F. Alshudukhi, S. A. Jabbar, and B. Alshaikhdeeb, "A feature selection method based on auto-encoder for internet of things intrusion




- detection,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 3, pp. 3265–3275, 2022, doi: 10.11591/ijece.v12i3.pp3265-3275.
- [40] 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.
- [41] M. A. Salahuddin, V. Pourahmadi, H. A. Alameddine, M. F. Bari, and R. Boutaba, “Chronos: DDoS attack detection using time-based autoencoder,” *IEEE Transactions on Network and Service Management*, vol. 19, no. 1, pp. 627–641, 2022, doi: 10.1109/TNSM.2021.3088326.
- [42] 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.
- [43] 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.
- [44] Q. Li, J. Mi, W. Li, J. Wang, and M. Cheng, “CNN-based malware variants detection method for internet of things,” *IEEE Internet of Things Journal*, vol. 8, no. 23, pp. 16946–16962, 2021, doi: 10.1109/jiot.2021.3075694.
- [45] 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.
- [46] 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.
- [47] 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,” *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–22, 2022, doi: 10.1155/2022/9307961.
- [48] 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 Transactions on Computational Social Systems*, vol. 9, no. 1, pp. 97–108, Feb. 2022, doi: 10.1109/TCSS.2021.3092746.
- [49] 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.
- [50] N. M. Y. -Naula, C. V. -Rosales, and J. A. P. -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.
- [51] 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.
- [52] P. Sudhakaran, C. Malathy, T. H. Vardhan, and T. Sainadh, “Detection of malware from IoT devices using deep learning techniques,” *Journal of Physics: Conference Series*, vol. 1818, no. 1, 2021, doi: 10.1088/1742-6596/1818/1/012219.
- [53] 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.
- [54] 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 of Things Journal*, vol. 9, no. 12, pp. 9310–9319, Jun. 2022, doi: 10.1109/JIOT.2021.3130434.

## BIOGRAPHIES OF AUTHORS



**Sowmya Somanath**    received the B.Eng. degree in Computer Science and Engineering from VTU University in 2008, M.Tech. degree in Computer Science and Engineering from VTU university in 2015, and currently pursuing Ph.D. under Visvesvaraya Technological University Belgavi, in security in IoT using machine learning domain. Currently, she is an assistant professor at the Department of Computer Science and Engineering, REVA University. She is a member of International Association of Engineers (IAENG). Her research interests include internet of things, network security, and machine learning. She can be contacted at email: sowmyasadish@gmail.com.



**Dr. Usha Banavikal Ajay**    is a dedicated motivational individual committed to maximizing learning opportunities in diverse academic settings using consistent and organized practices. Energetic and ambitious professional with 18 years of experience in teaching. She has completed her research in the area of information security. She Obtained her Ph.D. from Visvesvaraya Technological University, Belagavi, Karnataka, India in the year 2016. She has published more than 35 research papers in reputed international journal and conferences where some of them are Scopus indexed and also has good impact factors. Currently, she is working as professor in the Department of Information Science and Engineering, BMS Institute of Technology and Management, Bengaluru. Her research interests include IoT, information security, cyber security, data mining, artificial intelligence, and machine learning. She can be contacted at email: ushaajay1@gmail.com.