INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Implementation of Machine Learning and Deep Learning for Securing the Devices in IOT Systems

Salunkhe Madhav Jagannath[1], Rajendra B Mohite[2], Mukesh Kumar Gupta[3]*, Onkar S Lamba[4]

1 Research Scholar, Department of ECE, Suresh Gyan Vihar University, Jaipur, India
2 Assistant Professor, Department of EXTC, Bharati Vidyapeeth College of Engineering Navi Mumbai, India
3 Professor, Department of Electrical Engineering, Suresh Gyan Vihar University, Jaipur, India
4 Professor, Department of ECE, Suresh Gyan Vihar University, Jaipur, India

OPEN ACCESS

Received: 14-01-2023

Accepted: 05-02-2023

Published: 05-03-2023

Citation: Jagannath SM, Mohite RB, Gupta MK, Lamba OS (2023) Implementation of Machine Learning and Deep Learning for Securing the Devices in IOT Systems . Indian Journal of Science and Technology 16(9): 640-647. https://doi.org/10.17485/IJST/v16i9.99

* **Corresponding author**.

mkgupta72@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: To fix the security issues of devices in internet of things (IOT) systems that arise when Machine learning (ML) and Deep Learning algorithm (DLA) are implemented in the IOT systems. **Methods:** Each packet of IoT threats has been filtered by using suitable attack model for primary attack detection. In deep learning, network traffic field's information is extracted from of packet and is used as the training features. Attack is proposed to be detected by the use of database-based features of attack. If attack is found then packet will be discarded along with update feedback to filtering stage for primary attack detection. Knowledge Discovery and Data Mining (KDD) dataset is used in this study**.** Different types of Mirai attack are considered for classification. The performance of the proposed method has been compared in terms of accuracy and execution time with earlier work using traditional ML-DL methods. **Findings:** The proposed technique is seen to achieve high accuracy level at the least computational time, concurrently with much higher recall and G-mean values Several algorithms are used to secure the IOT devices from various types of threats and a comparison is depicted with their accuracy and execution time. Results show that the proposed methodology using Convolution neural network (CNN) for classification, can achieve the accuracy ~0.9976 with execution time1.30 sec and G-mean 0.7865 only. **Novelty:** The proposed method is essentially a judiciously configured ML- DL technique which is novel and exhibits better performance in terms of mitigating IoT threats.

Keywords: IOT devices and threats; Machine Learning; Deep Learning; KDD; Security and privacy

1 Introduction

Internet of things (IoT) realizes the concept of connecting electronics devices like sensors, mobiles, television, computers, home security, vehicles, cameras etc through wired or wireless network to the internet protocol suite (TCP/IP); this makes it possible to monitor, control, communicate and interact among themselves without the need for human intervention. The ”things” in implies those sensor-based things which collect information and transfers to connected devices for subsequent actions or decisions [1–3]. Owing to the fact that IoT development deals with huge information, a privacy hole is created due to data being improperly checked and insecurely sent. Such inherent weakness is prone to invoke the unique botnet ”Mirai” a subject to widespread distributed denial of service (DDoS) attacks [4,5]. The four DL and ML privacy technologies viz. homomorphic encryption, trusted execution, differential privacy, and secure multiparty computing environment homomorphic encryption, trusted execution, differential privacy, and secure multiparty computing environment are most frequently utilised to prevent the attacker from discovering which instances were used to create the target model; the trusted execution environments make use of hardware-based security and isolation for training code security and sensitive data security [6,7].

It is known that the prime security challenges in IoT are confidentiality, integrity, privacy, availability, authentication, non-repudiation etc. Researchers are continuously working on security standards and measures on frameworks for IoT based smart environment. LSTM IDs (Intrusion detection systems using long short-term memory) is a powerful technique to secure IoT network. LSTM algorithm is good for handling long term dependencies in data due to its ability to remember information for extended periods of time. Moreover, LSTM algorithms are less susceptible to the vanishing gradient problem. However, the main drawbacks of LSTM algorithm are that require more training data and long training time. Moreover, LSTM algorithm is not suitable for online learning tasks [8–10]. On the other hand, game theory technique is efficient under certain assumptions for prediction and classification tasks where the input data is not in sequence. These assumptions are not realistic in most of the times. LSTM algorithm with game theory techniques for a mixed Nash balance (NE) approach has been adapted to address the security problem in IoT network [11,12]. Although the implantation complexity of game theory and the higher computation time are claimed to be taken care by the constituent counterparts of NE approach, the mitigation of either difficulties are not fully overcome. This necessitates evolving an alternative strategy to take care of security threats in IoT systems. In view the potential of deep learning in yielding least error in accomplishing one AI task, it is thought prudent to devise means to extract attack features by suitable data filtering followed by classification and then subjecting the classified data sets to attack prevention algorithm a suitable decision support system may be embedded.

The proposed method using CNN classifier has the advantages to update the model by using feedback system to improve the results in terms of accuracy, recall and G-mean to handle security and privacy threats in IoT like Malware, denial of service and MiTM etc.

1.1 Gap analysis of existing methods

- Low accuracy of existing method like CNN, and SMOTE-SLFN(150)-LSTM(150,150) on network dataset.
- High execution time of existing method like CNN in batch size 128.
- G-mean value is also low in case of the existing methods

1.2 IoT Threat

In IOT, it is found that there are two types of threats are very important as given below:

1.3 Privacy threats

- Man-in-the-Middle (MiTM) which are two types: Passive MiTM attacks, and active MiTM attacks.
- Privacy in data with MiTM attacks which is categorized as: passive data privacy attacks, and active data privacy attacks.

1.4 Security threats

- Malware: Injection and execution of malicious code into IoT systems through the creation of already existing vulnerabilities in IoT systems is one of the most well-known assaults being practised.
- Man-in-the-Middle. One of the earliest kinds of cyber threats was the man-in-the-middle (MiTM) assault [5]. Impersonation and spoofing are examples of MiTM attacks.

1.5 Other threats to privacy and security

- Physical threats or destruction is one type of threat where a cyberattack is not usually possible.
- Cyber threat is classified as active threats, and passive threats.

The different kind of threats one has encounter in IoT systems are shown in Figure 1.

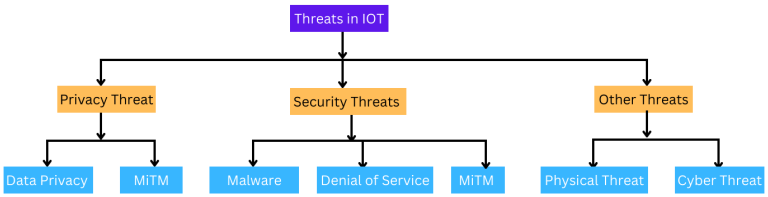

Fig 1. Types of threats in IOT

2 Methodology

The proposed work can be understood with the help of block diagram shown in Figure 2.

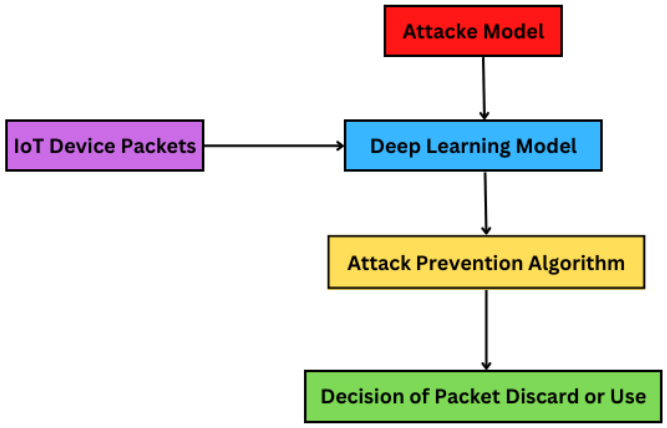

Fig 2. Block diagram of proposed system

Figure 3 shows the details of procedure to be implemented in algorithm for detecting and preventing the attack using deep learning.

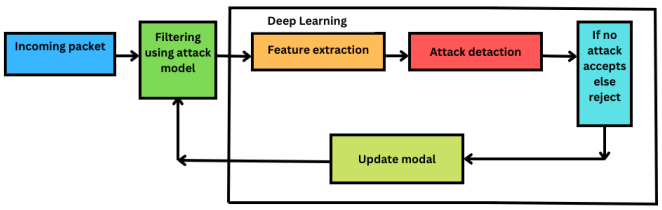

Fig 3. Proposed work procedure for security

It is observed that there is lack of focus on security of the devices in IOT system at the time of design and implementation process of such system. IoT devices in the system are very vulnerable and more often privacy sensitive which are easily targeted by attackers as tools for DDoS attacks. Each packet can be filtered using attack model for primary attack detection The features related information already extracted through Python is subjected to deep learning technique. In the instant case CNN is used for deep learning and it uses the extracted information to accomplish training of the dataset, its testing and then the validation

of results. Using database-based features for attack, any type of attack can be detected. If attack is found, the packet will be discarded along with update feedback into the filtering stage so as to go for primary attack detection.

2.1 DL and ML for IoT Security and Privacy

2.1.1 ML in IOT security. Privacy and security are intertwined. It is imaginable to have a secure environment without any form of personal privacy. While the presence of windows may provide the impression that a home is private, intruder security is not always guaranteed by this feature. While obtaining privacy, it is often required to give up some amount of security, though the contrary is not true. When security is weak or exposed, privacy is always jeopardised. The most popular ML and DL models for categorising IoT security factors are shown in the Figure 4.

Supervised and unsupervised approaches are both included in ML. The constituent techniques are known as Naive Bayes (NB), random forests (RF), support vector machines (SVM), decision trees (DT), K-nearest neighbours (KNN), ensemble learning (EL) etc. Additionally, the principal component analysis (PCA) and K-means are the only two unsupervised methodologies, seemingly known up till now. Similarly, categories for DL techniques include unsupervised, supervised, and hybrid approaches.

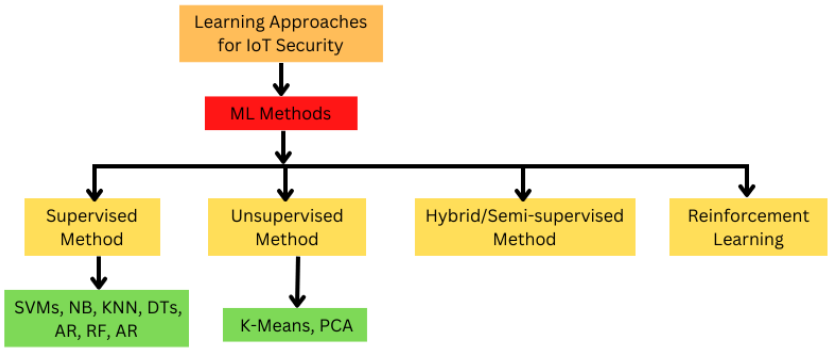

Fig 4. ML methods and techniques for IoT

2.1.2 DL in IoT security. In IoT systems, deep learning has recently been a hot area of research[11,12]. The fundamental benefit of deep learning over traditional machine learning is that it performs much better on large datasets. Since many IoT projects generate enormous amounts of data, DL techniques are thought to be a good fit for such systems. Additionally, DL builds dynamic data representations on the fly[13–15]. With DL techniques, the IoT ecosystem may be connected seamlessly. A uniform protocol called deep connection makes it possible for computers and other apps connected to the Internet of things to communicate automatically.

For instance, IoT gadgets in an intelligent house automatically communicate with one another to create a fully intelligent home[16]. To learn various levels of abstraction in data structures, DL techniques employ a computational framework that incorporates several layers. Modern methodologies have been substantially improved by DL techniques when compared to conventional ML approaches[17–19]. DL is a branch of machine learning (ML) that abstracts and transforms generative or discriminatory pattern analysis operations utilising various non-linear layers of computing. Since DL techniques may recognise hierarchical pictures in deep architecture, they are sometimes referred to as hierarchical learning techniques. The interpretation of impulses by human neurons and the brain serves as the driving force behind the operational theory of DL. Several DL classifiers for IoT security are shown in Figure 5.

Supervised DL: The most popular controlled DL techniques are covered in this section. There are two different categories of discriminative DL algorithms: recurrent neural networks (RNNs) and convolutional neural networks (CNNs).

Unsupervised DL: The most popular unsupervised DL methods are known to be DBNs, RBMs and AEs etc.

Hybrid or Semi-Supervised DL: The most traditional deep hybrid learning strategies are covered in this section. Generative adversarial networks (GANs) and network communities are two hybrid deep learning methods (EDLNs).

Reinforcement learning (RL) has been developed as a powerful strategy for enhancing a learning agent's approaches and identifying the optimum course of action by assessing and failing to reach the best long-term objective without prior knowledge of the environment[20,21]. A subset of ML is RL. It determines the reward for each action taken before moving on to the next

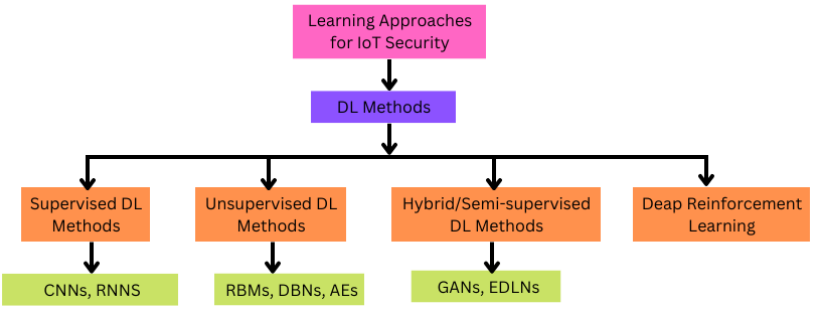

Fig 5. DL methods and techniques for IoT

step [22,23].

2.2 Application of DL in IoT Security

In IoT environments, DL approaches have been devised for signal authentication [11,12]. The LSTM architecture is used to extract an array of features from inputs of IoT device. Then, the characteristics of cyberattack control in IoT systems were watermarked, and the intricate function extraction frequently assisted in identifying eavesdropping attacks. However, because it would be prohibitively difficult to verify every IoT device via a centralised cloud service, this technique is not applicable to very large IoT setups.

This method can manage several IoT modules, however it is also very dynamic and unsuited for IoT situations. Since LSTM was created for device recognition to be impervious to signal flaws, it is also advised for use in IoT situations for DL-based system authentication. However, the technique only works for system recognition and misses more serious threats. DNN has been upgraded [24,25] by using intrusion detection systems (IDSs) to categorise significant threats in IoT system.

2.3 Solution of IoT Threat using DL and ML Algorithms

There are various strategies to reduce worries about privacy and security. Discussions and answers on how to guarantee security or privacy in the IoT system were non-existent. In this part, we focus on current publications that propose IoT security and privacy-preserving approaches. We demonstrate how DL or ML algorithms may be used as a tool to ensure privacy and security threats.

It emphasises statistics and other data rather than focusing on the personal information of individuals. On the other hand, the main goals of privacy programmes are passwords, login details, and other sensitive data. The three pillars of security are preserving privacy, preserving the integrity of data and information, and making sure it is easily available.

All data processing pipelines for frameworks use the machine learning (ML) data processing technology. For instance, to obtain an up-to-date judgement, a machine learning model may evaluate the data flow into a network. There is a chance that the IoT nodes connecting to the ML model might be subject to exploratory or poisoning assaults. On the output, inversion and integrity attacks are possible [19]. As a result, a system's security and privacy cannot be compromised at the same time.

3 Results and Discussion

We have used seven different algorithms along with a few distinctly different methods of machine learning and deep learning for analysis the performance of the proposed methodology (Figure 3); it is intended to resolve the problem of IOT threats and security of devices. A comparison of different algorithms implemented through the proposed methodology for the sake of imparting the desirable security in IOT system is made and the results are shown in Table 1. Experimental results for accuracy and recall are shown in Figure 6, similarly result for accuracy and false alarm, as well as accuracy and G-mean are shown in Figures 7 and 8 respectively. It is observed that DT algorithm exhibits least performance in terms of accuracy (0.8964), Recall value (0.9476) and the G-mean value (0.4107), whereas, on the same dataset KDD, the experimental results of CNN algorithm is found to be excellent when its results of accuracy (0.9976), Precision (0.9952), Recall (0.9967) and G-mean (0.7865) values are compared with those obtainable from the other tested algorithms. The proposed methodology using CNN classifier outperforms the other techniques in terms of G-mean, and hence satisfies the major objective of this study.

Table 1. Comparison in different algorithms implemented on proposed methodology

Algorithm	Execution Time	Accuracy	Precision
KNN	2.02 s	0.9332	0.9317
SVM	5.05 s	0.9381	0.9353
LR	1.32 s	0.9473	0.9424
ANN	2.04 s	0.9924	0.9916
CNN	1.30 s	0.9976	0.9952
RF	2.11 s	0.9723	0.9696
DT	1.86 s	0.8964	0.8942

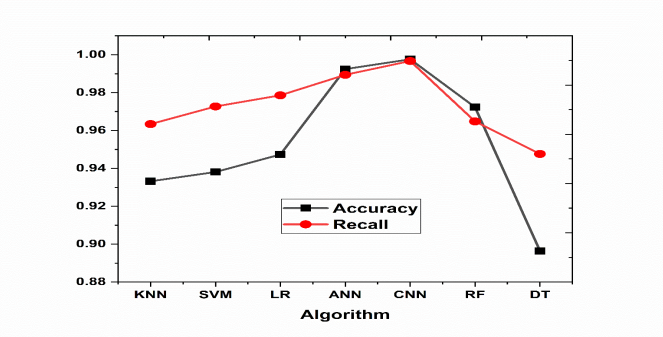

Fig 6. Accuracy and recall values of various algorithms

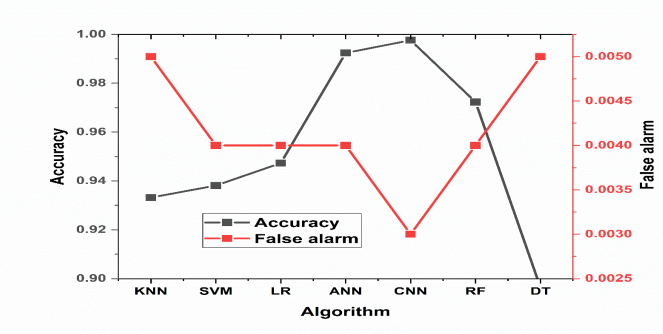

Fig 7. Accuracy and false alarm values of various algorithms

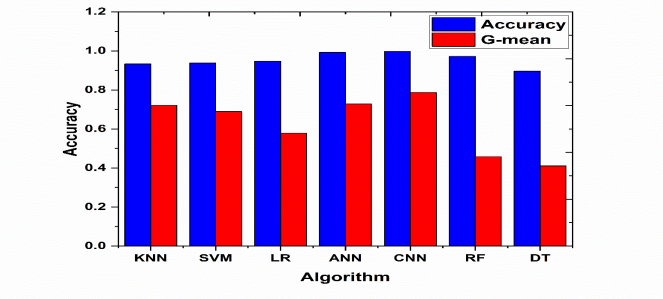

Fig 8. Accuracy and G-mean values of various algorithms

The detection method, where the system will educate itself to be able to tell the difference between normal and aberrant activity is supposed to be of extreme importance. Since we are using anomaly-based intrusion detection approaches, the system must be able to recognise both the known and unknown threats. As a supervised learning approach, anomaly-based detection requires a data set to train its system. For a set of selected machine learning algorithms, we are leveraging by opting for building a defensive system in both the cases of network-based application layer and the host-based network layer. Noting that a satisfactory result is achievable by the methodology propounded by us, it is felt that the results obtained by present experimentation need be compared with previous reports of research carried out elsewhere [8–10]. The following section furnishes the results of comparison.

3.1 Comparison with other Methods

Table 2 show the results of comparison between the proposed model using CNN classifier and those reported by others. It is revealed that our method superior to other methods in respect of accuracy. Similarly, the execution time in our proposed method is far less than values reported till date [9]; moreover, the G-mean is better in our case as compared to the previously reported value [10]. It is therefore apparent the method proposed by us is superior to the existing methods. This tends to authenticate the novelty of our proposition to use CNN classifier and therefore inherits its merit over other techniques advocated by a number of previous researchers.

Table 2. Comparison between the proposed method and the methods suggested by previous workers

R ef.	Technique	D ataset	Outcomes and Performance
[8]	Convolutional Neural Network (CNN)	Bot-IoT	Accuracy 0.9970, precision 0.9960, and recall 0.9990
[9]	Convolutional Neural Network (CNN)	Bot-IoT	Accuracy 91.27%, and elapsed time 64 min 18 sec. in batch size 128
[10]	SMOTE-SLFN$_{(150)}$-LSTM$_{(150,150)}$	IoTID20	Accuracy 0.8620 $\pm$ 0.0260, and G-mean 0.7835 $\pm$ 0.0247
Proposed Method	Convolutional Neural Network (CNN)	KDD	Accuracy 0.9976, execution time 1.30 sec., precision 0.9952, recall 0.9967, and G-mean 0.7865

4 Conclusion

In this paper, various deep learning and machine learning techniques are implanted on the dataset KDD to obtain a desirable solution to the well-known problem of IoT privacy and security threats. Artificial intelligence system of neural network-based intrusion detection and classification is developed in the present investigation to combat with the inherent security threats in the internet of things networks. A ML-D technique is proposed for classification of different types of attacks viz. ACK, SCAN, SYN, UDP, UDP Plain. The performance of the proposed CNN method is compared with earlier work that had employed traditional ML and DL methods. The comparison is made in respect of achieving the level of accuracy, precision, recall value, false alarm, G-mean value and the computational time to execute the same task. It may be inferred from the experiment results that proposed method using CNN is able to outperform other methods and techniques in respect of its performance on insurance of the security and privacy of IoT systems. The authors conclude that the use of CNN for classification and implementation of the suggested protocols make up a novel technique in respect of mitigating the IoT threats and insuring security of devices

Acknowledgement

The authors acknowledge with gratitude the assistance received from the administration of Suresh Gyan Vihar University to conduction of the study and preparation the report for communication.

References

1) Bharati S, Mondal MRH, Podder P, Prasath VBS. Federated learning: Applications, challenges and future directions. *International Journal of Hybrid Intelligent Systems*. 2022;18(1-2):19–35. Available from: https://doi.org/10.3233/HIS-220006.
2) Omolara AE, Alabdulatif A, Abiodun OI, Alawida M, Alabdulatif A, Alshoura WH, et al. The internet of things security: A survey encompassing unexplored areas and new insights. *Computers & Security*. 2022;112:102494. Available from: https://doi.org/10.1016/j.cose.2021.102494.

3) Amjad RK, Muhammad K. Deep Learning for intrusion detection and security of internet of things (IoT): current analysis, challenges, and possible solutions. 2022. Available from: https://doi.org/10.1155/2022/4016073.
4) Abbas G, Mehmood A, Carsten M, Epiphaniou G, Lloret J. Safety, Security and Privacy in Machine Learning Based Internet of Things. *Journal of Sensor and Actuator Networks*. 2022;11(3):38. Available from: https://doi.org/10.3390/jsan11030038.
5) Subrato B, Prajoy P. Machine and deep learning for IoT security and privacy: applications, challenges, and future directions. 2022. Available from: https://doi.org/10.1155/2022/8951961.
6) Ahanger TA, Tariq U, Ibrahim A, Ullah IA, Bouteraa Y, Gebali F. Securing IoT-Empowered Fog Computing Systems: Machine Learning Perspective. *Mathematics*. 2022;10(8):1298. Available from: https://doi.org/10.3390/math10081298.
7) Agarwal S, Gupta MK. Context Aware Image Sentiment Classification using Deep Learning Techniques. *Indian Journal Of Science And Technology*. 2022;15(47):2619–2627. Available from: https://doi.org/10.17485/IJST/v15i47.1907.
8) Banaamah AM, Ahmad I. Intrusion Detection in IoT Using Deep Learning. *Sensors*. 2022;22(21):8417. Available from: https://doi.org/10.3390/s22218417.
9) Susilo B, Sari RF. Intrusion Detection in IoT Networks Using Deep Learning Algorithm. *Information*. 2020;11(5):279. Available from: https://doi.org/10.3390/info11050279.
10) Qaddoura R, Al-Zoubi AM, Faris H, Almomani I. A Multi-Layer Classification Approach for Intrusion Detection in IoT Networks Based on Deep Learning. *Sensors*. 2021;21(9):2987. Available from: https://doi.org/10.3390/s21092987.
11) Dankwa S, Yang L. Securing IoT Devices: A Robust and Efficient Deep Learning with a Mixed Batch Adversarial Generation Process for CAPTCHA Security Verification. *Electronics*. 2021;10(15):1798. Available from: https://doi.org/10.3390/electronics10151798.
12) Janani K, Ramamoorthy S. IoT Security and Privacy Using Deep Learning Model: A Review. *2021 International Conference on Intelligent Technologies (CONIT)*. 2021;p. 1–6. Available from: https://doi.org/10.1109/CONIT51480.2021.9498404.
13) Ganesh B, Markkandan S, Vinotha V, Priyadarshini S, Kaviya V. IoT security using machine learning techniques. 2022. Available from: https://doi.org/10.1007/978-981-19-2538-2_37.
14) Ch SC, Puli S, Santhi MVBT. Machine Learning Based Data Security Model Using Blockchain for Secure Data Transmission in IoT. *2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC)*. 2021;p. 1521–1527. Available from: https://doi:10.1109/ICESC51422.2021.9532659.
15) Ajagbe SA, Awotunde JB, Adesina AO, Achimugu P, Kumar TA. Internet of Medical Things (IoMT): Applications, Challenges, and Prospects in a Data-Driven Technology. *Intelligent Healthcare*. 2022;p. 299–319. Available from: https://doi.org/10.1007/978-981-16-8150-9_14.
16) Shilpa PC, Shereen R, Jacob S, Vinod P. Sentiment Analysis Using Deep Learning. *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*. 2021. Available from: https://doi.org/10.1109/ICICV50876.2021.9388382.
17) Singh C, Imam T, Wibowo S, Grandhi S. A Deep Learning Approach for Sentiment Analysis of COVID-19 Reviews. *Applied Sciences*. 2022;12(8):3709. Available from: https://doi.org/10.3390/app12083709.
18) Khan Y, Su'ud MBM, Alam MM, Ahmad SF, Salim NA, Khan N. Architectural Threats to Security and Privacy: A Challenge for Internet of Things (IoT) Applications. *Electronics*. 2023;12(1):88. Available from: https://doi.org/10.3390/electronics12010088.
19) Bhukya M, Venu M, Ramdas GC, Arun V, Veerender KS, A. Intrusion detection models for IOT networks via deep learning approaches. *Measurement Sensors*. 2023;25. Available from: https://doi.org/10.1016/j.measen.2022.100641.
20) Mohamed AB, Nour M, Hossam H. Introducing deep learning for IoT security in deep learning approaches for security threats in IoT environments. *IEEE*. 2023;p. 1–26. Available from: https://doi.org/10.1002/9781119884170.ch1.
21) Istiaque AK, Tahir M, Hadi HM, Lun LS, Ahad A. Machine Learning for authentication and authorization in IoT: taxonomy, challenges and future research direction. *Sensors*. 2021;21:5122. Available from: https://doi.org/10.3390/s21155122.
22) Jain S, Dwivedi A, Khanna A. Implementation of Machine Learning and Deep Learning Techniques in IoT Security: A Review. *SSRN Electronic Journal*. Available from: https://doi.org/10.2139/ssrn.3832166.
23) Parjanay S, Siddhant J, Shashank G, Vinay C. Role of machine learning and deep learning in securing 5G-driven industrial IoT applications. *Ad Hoc Networks*. 2021;123:102685. Available from: https://doi.org/10.1016/j.adhoc.2021.102685.
24) Mohammed AG, Amr M, Abdulla AA, Xiaojiang D, Ihsan A, Mohsen G. A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Communications Surveys & Tutorial*. 2021. Available from: https://doi.org/10.1109/COMST.2020.2988293.
25) Paul PK. Cyber Physical Systems, Machine Learning & Deep Learning—Emergence as an Academic Program and Field for Developing Digital Society. *Convergence of Deep Learning in Cyber-IoT Systems and Security 2022*. 2022;p. 67–83. Available from: https://doi.org/10.1002/9781119857686.ch3.