ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)

Available Online at www.ijetcr.org

Volume 12; Issue 01; 2024; Page No. 01-11

REVIEW OF IOT SECURITY CHALLENGES AND EXISTING SOLUTIONS

Muskan Garg[1*] and Dr. Sima[2]

[1] Research Scholar, Computer Science (FPA), DLCSUPVA, Rohtak, Haryana, India
E-mail: garg04muskan@gmail.com

[2] Associate Professor, Faculty of Planning and Architecture, DLCSUPVA, Rohtak, Haryana, India
E-mail: simasingh.2009@gmail.com

Conflicts of interest: Nil

Corresponding author: Muskan Garg

Abstract

As Internet of Things applications continue to develop, there are increasing threats to them. It is extremely difficult to create a fully secure system because of the restricted resources in these networks. This study looks at the different security needs and potential IoT attack. The study examines current methods for securing IoT systems, including blockchain, fog/edge computing, and machine intelligence. This paper aims to find out the current developments in the field of IoT security. To enhance security of IoT systems, this review looked at a variety of security criteria and current approaches. This thorough analysis of the most recent papers related to security of IoT has shown new research trends that will likely shape this sector's future.

Keywords: Internet of Things, Blockchain, Machine Learning, Deep Learning, Fog Computing, Edge Computings

1. INTRODUCTION

Modern communication technologies have advanced far beyond the conventional methods of environmental sensing. The Internet of Things (IoT) is interconnection of environmental objects using the Internet that can interact with each other without explicit instructions. IoT offers a variety of services and applications, including critical infrastructure, appliances, medical facilities, agriculture, and military. Because of the massive data produced by IoT devices, , conventional methods for data gathering, storing, and processing could not be effective at this level[1]. Furthermore, IoT creates diverse data, generating an additional layer of complexity for the existing data processing methods. The major challenge at these layers is data security[2]. To solve this issue, it becomes increasingly necessary to integrate new technologies. IoT security solutions employ emerging technologies like Blockchain, ML/DL, and fog/edge computing[3]. The aim of this document is to provide detailed information on IoT security risks, security requirements, threats, open issues, and possible solutions. The rest of the document is organized as follows: Part II discusses the recent literature of IoT. The security concerns of IoT systems are covered in section III. Section IV describes the security solutions for IOT. The conclusions and future directions are set out in section V.

2. Related Literature

This part of the article addresses the researchers' contributions in IoT security.[4] highlighted the class imbalance problem in the Bot-IoT dataset and proposed a new intrusion detection system using ML and DL models. The system has an average accuracy of more than 99% and exceeds the existing DDoS and DoS detection technology on IoT networks.[5] analyzed several machine learning models, including logic regression, support vector machine, decision tree, random forest, and artificial neural network, to accurately predict attacks and anomalies in the IoT system. [6] designed a deep learning architecture for secure IoT implementation and evaluated the effectiveness of DL algorithms for intrusion detection. The author designed Secure DeepNet-IoT, an adaptive multikernel cybersecurity platform with a classification accuracy of 95.05 percent and 94.3 percent. [7] applied machine and deep learning algorithms to extract essential features from a BoT-IoT dataset. Ten models are assessed for malware detection, including KNN, SVM, ensemble classifiers, and deep learning architectures. The CatBoost and XGBoost classifiers achieved the highest accuracy, suggesting their potential in identifying IoT network intrusions.[8] studied ML models for detecting malware on the Internet using IoT data sets. Nine techniques were tested, and the proposed model achieved 100% accuracy for DT, SVM, RF, BG, 99.9% in KNN,LR, NB, NN, and 28.16% for ST classifier.[9] presented a DL model, DeepAK-IoT for detecting cyberattacks on IoT devices. The model was evaluated using the data sets TON-IoT, Edge-IIoTset, and UNSW-NB15. DeepAK-IoT provides 95.57 per cent accuracy of TON IoT, 94.96 per cent of Edge-IIoTset and 98.41 per cent of UNSW NB15 set. [10] surveyed DDoS attacks, presenting statistics, motivations, and various types of attacks. The paper also discussed defense mechanisms used for detection and prevention against DDoS attacks, including machine learning and SDN-based methodologies. [11] highlighted ML/DL methods used in in designing NIDS. [12] discussed IoT security issues, including IAS Octave vulnerability, IoT reference model of Cisco of seven layers and top ten vulnerabilities of the OWASP. [13] studied security and privacy solutions for green IoT-based agriculture and classified threat models into five categories. It also analyzed a solution based on a privacy-oriented blockchain and a consensus algorithm. [14] proposed a method for evaluating trust in machine learning enabled IoT devices. The authors combined the QoS properties of the network with deep learning algorithms, built behavioral models and calculated trust values. [15] discussed the vulnerability assessment of IIoT protocols and the use of machine learning (ML) in countering these. [16] proposed IoT systems for health care using fog computing, form a geographically distributed intelligence layer between sensor nodes and clouds. This architecture can address problems such as mobility, reliability, energy efficiency, and scalability. [17] proposed a framework called CPMAED for detection of malicious nodes in IoT networks. [18] proposed a DNN-based network intrusion detection system Realguard that accurately detects multiple cyber-attacks in real time with a small computational footprint. It can detect ten types of attacks with an average accuracy of 99.57%, effectively operating on gateways which are resource constrained like Raspberry PI. [19] discussed security challenges, vulnerabilities, and attacks prevention using blockchain. [20] discussed the feasibility of running machine learning algorithms on IoT edge

devices. Random Forest is faster and more accurate, with all algorithms exceeding 80% accuracy, requiring less than one millisecond for inference, and having moderate energy consumption. [21] proposed a novel DL based intrusion detection method by using the IoT focus loss, evaluating its performance on different datasets, and comparing it with baseline models and the latest models. This approach exceeded the current methods of the base model and accuracy, F1 scores, and MCC scores, exceeding 24 percent, 39 percent, 39 percent, and 60 percent. [22] proposed a framework to analyze the execution code of ARM-based applications for detecting IoT malware using the Deep Learning. When 100 new malware samples are exposed to three different long-term memory configurations, the model's accuracy is the highest 98.18%, demonstrating its superior performance compared to other machine learning classifiers. [23] highlighted the use of Block chain mechanism in IoT Security solution. [24] proposed a healthcare IoT system, focusing on end-user authentication, end-to-end communications, and robust mobility through connected intelligent gateways. The system reduces communication expenses by 26 per cent and latency by 16 per cent and is 97% faster than certificates and 10 per cent faster than symmetrical keys DTLS. It also consumes almost as little RAM and ROM resources as certificate based DTLS and has low handover latency due to mobility. [25] discussed the ML method of analyzing data generated by IoT in smart cities. The algorithm taxonomy was presented, and potential and challenges were discussed. It also presented a case study of applying SVM to traffic data in the smart city of Aarhus. [26] discussed Internet of Things solutions for Early Warning for natural disasters like floods, earthquakes, tsunamis, and landslides. The author identified the most used solutions, highlights gaps in literature, and suggests solutions, emphasizing the benefits of integrating Fog/Edge layers. [27] discussed ML algorithms for detecting malware in business information systems connected by IoT, reviews research on the detection of static, dynamic, promoted and hybrid malware. [28] presented a comprehensive analysis of user perceptions of security in IoT devices, thereby aiding developers in creating superior devices and increasing user security awareness.[29] developed a security framework using the SLR technique and literature review. It used methods like Checksum and Cyclic Redundancy Check (CRC) to ensure data accuracy and originality. The framework also included features for continuous data syncing and version control for backup. [30] reviewed recent trends in IoT security and machine learning. The main trends include the development of models that integrate big data and ML, with emphasis on the efficiency and accuracy for real-time IoT attack detection.

3. Security and Privacy in IoT

This section examines IoT privacy concerns and issues. To this purpose, to detect the privacy issues, we first provide a layered architecture of IoT. The four primary layers of the IoT are the Perception Layer, Network Layer, Middleware Layer, and Application Layer, which are composed of multiple hierarchical layers[31]. Actuators and sensors are examples of the devices that make up the Perception Layer. To manage and keep an eye on the physical world, it gathers information from its surrounds. Actuators regulate the operation of physical equipment, such as an automobile's acceleration, whereas sensors sense things like motion, temperature, humidity, air quality, and acceleration. A large amount of data is generated by a perception layer device, sent to the network layer

for security routing and additional processing. The data is processed and transmitted through the Internet of Things architecture by the network layer. To meet vendors' specific services and application requirements, a middleware layer is occasionally introduced as a bridge between the network layer and the application layer. [32]. The top layer of the IoT infrastructure is called the Application Layer. It functions using data that has been processed by various IoT devices. It performs functions unique to each application[33]. While developing IoT, there are numerous challenges as shown in figure 1. Key security-related challenges encountered when developing IoT are briefly discussed.

3.1 Authorization

Authorization means granting users access rights to Internet of Things systems such as physical sensor devices. Users can be people, computers, or other services. Only with the appropriate authorization from the requester can an action be completed. Since physical sensors must also be permitted to interact with the system, the main challenge with authorization in Internet of Things contexts is figuring out how to grant access efficiently.

3.2 Authentication

Authenticating users is the priority for the IoT security supplier. IoT systems operate in a highly sophisticated and crucial manner due to their interconnected switching nodes and sensors. The entire system may become vulnerable even if just one sensing layer node is compromised[34]. In contrast to the existing standards, a new authentication standard based on autonomous configuration is required.

3.3 Confidentiality

Data confidentiality is crucial to the Internet of Things because it ensures the trustworthy transit of data. Technologies like TLS and IPsec are utilized in the field of Internet transmission, but their total cost is higher than that of IoT systems, which have limited resources[35]. But in IoT, the primary sensitivity to secrecy is communicated, stored, found/monitored, and recognized.

3.4 Integrity

When accessing an unsecured wireless network, integrity ensures a quick and simple verification process for detecting transmission changes. It may be difficult for devices to perform their essential functions if integrity breaches are not discovered quickly.

3.5 Availability

The ability of a computer or the system to supply the data and resources required when needed is known as availability. Making the existence of confined machines in the network and LLNs in IoT networks available is challenging. It exploits attackers to carry out denial-of-service assaults on the network. Although robust security measures, like classical security mechanisms, improve equipment and network protection, they also have an impact on network availability. Due to the large overheads these procedures impose on the limited devices, contact is delayed, and this delays the time of calculation, which results in the transfer time and ultimately drains the devices' batteries, affecting the network's availability.

3.6 Non-repudiation

The security of data shared between two systems is ensured by non-repudiation. Because non-repudiation offers evidence of the data's source,

dependability, and integrity, it ensures that the authenticity of the data cannot be questioned.

Fig 1. IoT Security Attacks

4. Solutions to Security of IoT

The different methods and approaches for protecting IoT environments can be categorized into three categories.

4.1 Security using Machine Learning

Machine learning has evolved considerably in recent years. IoT is among the many domains that use machine learning. Machine learning techniques are being applied to offer novel defenses against a variety of attacks[36]. Machine learning solutions differ greatly from traditional techniques. Two novel developments in the field are pulse swarm optimization and backpropagation, which show great promise. Neural networks and learning-based algorithms could potentially improve the security of IoT. Network security is improved using ML methods such as reinforcement learning, unsupervised learning, and supervised learning[37]. A prediction model is created using the supervised learning method by analyzing the relationship between the input parameters and the anticipated result. Initially, learning examples are utilized to train the algorithms.SVM, Naive Bayes, KNN , neural networks (NNs), deep neural networks (DNNs), and random forests are some of the supervised learning techniques[38]. These techniques can be used to identify malware, DoS assaults, spoofing attacks, and network intrusion in a variety of IoT devices.

Unsupervised learning algorithms examine the similarities between unlabeled data and do not require labelled data. The data is then divided into several groups by the algorithm. ML methods that are not supervised include association mining, clustering, and anomaly detection[39]. Unsupervised learning approaches can accomplish more complex processing tasks than supervised learning methods.

Reinforcement Learning focuses on the behaviors that software agents, or models, should perform in an environment to accomplish a difficult goal[40]. There are no predetermined results, and the agents pick up knowledge from the input they receive from their interactions with the surroundings. Reward points are earned based on activities taken, and the algorithm modifies its rules to maximize reward points. Although it takes a while to train reinforcement learning models, once created, the models operate with less memory.

4.2 Security using Blockchain Technology

Using blockchain technology with IoT can enhance total transparency, visibility, comfort level, and confidence[41]. The blockchain technology is like a distributed ledger. The ledger is dispersed among a network of nodes, and peer-to-peer data sharing occurs. Each node in the network is assigned a public key, which other nodes use to encrypt communications sent to that node. A node uses a private key to read these kinds of messages. So, the nodes utilize one key for encrypting and another for decrypting the messages. The blockchain entries keep chronological sequence and are time stamped. The signed transactions are broadcast by a node to its peers in one hop. Both integrity and authentication are ensured by this signing[42]. After confirming that the transaction is legitimate,

the receiving node retransmits it. In the chain, a new block is created using the hash of an earlier accepted block. Blockchain technology is built upon four fundamental pillars: smart contracts, cryptography, consensus, and shared ledger.

4.3 Security using Fog/Edge Computing

We are aware that the internet's infrastructure is strained by the large volume of data produced by IoT devices. There is a requirement to store, handle, and analyze data coming from multiple sources in various places. We are aware that the cloud provides an effective way to handle and store data, and that we can combine the cloud with IoT to process, store, manage, and secure data. Faster processing IoT applications will not be handled by the present cloud capability. Thus, the concept of fog computing was put forth, which handles the data produced locally by IoT devices. Wireless networking and machine-to-machine communication are facilitated by both cloud and fog computing. The primary objectives of fog computing are enhancing data security and boosting IoT device efficiency. Fog systems are compatible with low-end devices such as IP cameras and switches. Fog computing can result in a 20% reduction in the typical reaction time for a user. Moreover, a 90% reduction in data traffic can be achieved between the network edge and cloud. The location of processing power and data processing methods are the main distinctions between edge and fog computing. Fog computing uses a decentralized computing architecture to process and store data between the source and cloud. However, the data source device itself serves as the compute facility in edge computing. Fog/edge computing nodes can therefore use this architecture to process high priority IoT data instantly[43]. Since each node has limited processing and storage capacity, the primary difficulty at hand is how to manage this infrastructure efficiently and allocate different resources to IoT devices. Consequently, effective management of the computer resources is required. Because fog/edge computing collects and processes data in real time, accuracy issues are improved.

Table 1: gives a summary of recent research that used one of these methods to secure IoT devices. (Methods used to secure IoT)

Serial Number	Title	Main Authors	Year of Publishing	Method Used	Objective	Reference
1	Blockchain-based Secure IoT Architecture: A Review	S. Gupta, V. K. Sharma	2023	Blockchain	Review of blockchain-based IoT architectures for security enhancement	[44]
2	Machine Learning-based Intrusion Detection System for IoT Networks	A. Khan, M. H. Rehmani	2022	Machine Learning	Intrusion detection in IoT networks using machine learning	[45]
3	Deep Learning Approaches for Anomaly Detection in IoT Networks	T. Nguyen, J. Patel	2023	Deep Learning	Anomaly detection in IoT networks employing deep learning	[46]
4	Fog Computing-based Secure Data Storage for IoT Devices	R. Sharma, S. Singh	2023	Fog Computing	Secure data storage for IoT devices using fog computing	[47]
5	Edge Computing-enabled Authentication Mechanism for IoT Devices	K. Patel, A. Kumar	2022	Edge Computing	Authentication mechanism leveraging edge computing for IoT devices	[48]

6	Blockchain-based Access Control System for IoT Devices	S. Li, Q. Wang	2023	Blockchain	Access control system for IoT devices based on blockchain	[49]
7	Machine Learning-driven Threat Intelligence Framework for IoT Security	G. Singh, N. Jain	2022	Machine Learning	Threat intelligence framework employing machine learning for IoT security	[50]
8	Deep Learning-based Malware Detection in IoT Devices	H. Chen, J. Zhang	2023	Deep Learning	Malware detection in IoT devices using deep learning	[51]
9	Fog Computing-assisted Secure Data Processing for Healthcare IoT	L. Wang, Y. Zhao	2022	Fog Computing	Secure data processing for healthcare IoT utilizing fog computing	[52]
10	Edge Computing-based Intrusion Prevention System for Smart Grid IoT	X. Liu, Z. Zhang	2023	Edge Computing	Intrusion prevention system for smart grid IoT leveraging edge computing	[53]
11	Blockchain-based Secure Firmware Update Mechanism for IoT Devices	M. Ahmed, S. Khan	2023	Blockchain	Secure firmware update mechanism for IoT devices using blockchain	[54]
12	Machine Learning-driven Anomaly Detection for Industrial IoT Systems	A. Sharma, R. Gupta	2022	Machine Learning	Anomaly detection for industrial IoT systems employing machine learning	[55]
13	Fog Computing-enabled Privacy Preservation in IoT Data Analytics	J. Li, X. Wang	2023	Fog Computing	Privacy preservation in IoT data analytics enabled by fog computing	[56]
14	Deep Learning-based Intrusion Detection System for Vehicular IoT Networks	Y. Zhang, H. Wang	2022	Deep Learning	Intrusion detection system for vehicular IoT networks using deep learning	[57]
15	Edge Computing-assisted Secure Communication Protocol for IoT Devices	S. Kumar, P. Jain	2023	Edge Computing	Secure communication protocol for IoT devices assisted by edge computing	[58]

5. Conclusion and Future Direction

In this article, we talked about the IoT architecture, its various layers, the network, application, middleware and sensor layers, risks and attacks connected to those layers. In addition to summarizing the interesting topics for IoT security research, we have included a summary of a few ways to improve IoT system security. These include ML/DL, fog/edge computing, and blockchain based solutions. It is imperative to tackle numerous security concerns and obstacles before users can fully use IoT apps. An IoT system's whole life cycle, including each of its individual components, requires security features. Dynamic and real-time algorithms and models are needed to analyse and diagnose risks, attacks, and hazards in conjunction with different IoT system components. The system should have both lightweight self-healing in thin devices and complete security. The direction of future research and development is elevating IoT security to a new level.

REFERENCES

1. D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, “Internet of things security: A top-down survey,” *Computer Networks*, vol. 141.

Elsevier B.V., pp. 199–221, Aug. 04, 2018. doi: 10.1016/j.comnet.2018.03.012.

2. M. Humayun, M. Niazi, N. Z. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study," *Arab J Sci Eng*, vol. 45, no. 4, pp. 3171–3189, 2020, doi: 10.1007/s13369-019-04319-2.
3. M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *Journal of Information Security and Applications*, vol. 38, pp. 8–27, Feb. 2018, doi: 10.1016/j.jisa.2017.11.002.
4. J. G. Almaraz-Rivera, J. A. Perez-Diaz, and J. A. Cantoral-Ceballos, "Transport and Application Layer DDoS Attacks Detection to IoT Devices by Using Machine Learning and Deep Learning Models," *Sensors*, vol. 22, no. 9, May 2022, doi: 10.3390/s22093367.
5. M. Hasan, M. Milon Islam, M. Ishrak Islam Zarif, and M. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," 2019, doi: 10.1016/j.iot.2019.10.
6. G. Altan, "SecureDeepNet-IoT: A deep learning application for invasion detection in industrial Internet of Things sensing systems," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 4, Apr. 2021, doi: 10.1002/ett.4228.
7. O. A. Alkhudaydi, M. Krichen, and A. D. Alghamdi, "A Deep Learning Methodology for Predicting Cybersecurity Attacks on the Internet of Things," *Information (Switzerland)*, vol. 14, no. 10, Oct. 2023, doi: 10.3390/info14100550.
8. W. Yaokumah, J. K. Appati, and D. Kumah, "Machine Learning Methods for Detecting Internet-of-Things (IoT) Malware," *International Journal of Cognitive Informatics and Natural Intelligence*, vol. 15, no. 4, 2021, doi: 10.4018/IJCINI.286768.
9. W. Ding, M. Abdel-Basset, and R. Mohamed, "DeepAK-IoT: An effective deep learning model for cyberattack detection in IoT networks," *Inf Sci (N Y)*, vol. 634, pp. 157–171, Jul. 2023, doi: 10.1016/j.ins.2023.03.052.
10. P. Kumari and A. K. Jain, "A comprehensive study of DDoS attacks over IoT network and their countermeasures," *Computers and Security*, vol. 127. Elsevier Ltd, Apr. 01, 2023. doi: 10.1016/j.cose.2023.103096.
11. Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 1, Jan. 2021, doi: 10.1002/ett.4150.
12. C. Wheelus and X. Zhu, "IoT Network Security: Threats, Risks, and a Data-Driven Defense Framework," *Internet of Things*, vol. 1, no. 2, pp. 259–285, Dec. 2020, doi: 10.3390/iot1020016.
13. M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, "Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges," *IEEE Access*, vol. 8. Institute of Electrical and Electronics Engineers Inc., pp. 32031–32053, 2020. doi: 10.1109/ACCESS.2020.2973178.
14. W. Ma, X. Wang, M. Hu, and Q. Zhou, "Machine Learning Empowered Trust Evaluation Method for IoT Devices," *IEEE Access*, vol. 9, pp. 65066–65077, 2021, doi: 10.1109/ACCESS.2021.3076118.
15. M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things," *IEEE Internet Things J*, vol. 6, no. 4, pp. 6822–6834, Aug. 2019, doi: 10.1109/JIOT.2019.2912022.
16. A. M. Rahmani *et al.*, "Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing

approach," *Future Generation Computer Systems*, vol. 78, pp. 641–658, Jan. 2018, doi: 10.1016/j.future.2017.02.014.

17. L. Liu, X. Xu, Y. Liu, Z. Ma, and J. Peng, "A Detection Framework against CPMA Attack Based on Trust Evaluation and Machine Learning in IoT Network," *IEEE Internet Things J*, vol. 8, no. 20, pp. 15249–15258, Oct. 2021, doi: 10.1109/JIOT.2020.3047642.
18. X. H. Nguyen, X. D. Nguyen, H. H. Huynh, and K. H. Le, "Realguard: A Lightweight Network Intrusion Detection System for IoT Gateways," *Sensors*, vol. 22, no. 2, Jan. 2022, doi: 10.3390/s22020432.
19. S. Singh, A. S. M. Sanwar Hosen, and B. Yoon, "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network," *IEEE Access*, vol. 9, pp. 13938–13959, 2021, doi: 10.1109/ACCESS.2021.3051602.
20. M. T. Yazici, S. Basurra, and M. M. Gaber, "Edge machine learning: Enabling smart internet of things applications," *Big Data and Cognitive Computing*, vol. 2, no. 3, pp. 1–17, Sep. 2018, doi: 10.3390/bdcc2030026.
21. A. S. Dina, A. B. Siddique, and D. Manivannan, "A deep learning approach for intrusion detection in Internet of Things using focal loss function," *Internet of Things (Netherlands)*, vol. 22, Jul. 2023, doi: 10.1016/j.iot.2023.100699.
22. H. HaddadPajouh, A. Dehghantanha, R. Khayami, and K. K. R. Choo, "A deep Recurrent Neural Network based approach for Internet of Things malware threat hunting," *Future Generation Computer Systems*, vol. 85, pp. 88–96, Aug. 2018, doi: 10.1016/j.future.2018.03.007.
23. D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for IoT security," *Internet of Things (Netherlands)*, vol. 1–2. Elsevier B.V., pp. 1–13, Sep. 01, 2018. doi: 10.1016/j.iot.2018.05.002.
24. S. R. Moosavi *et al.*, "End-to-end security scheme for mobility enabled healthcare Internet of Things," *Future Generation Computer Systems*, vol. 64, pp. 108–124, Nov. 2016, doi: 10.1016/j.future.2016.02.020.
25. M. S. Mahdavinejad, M. Rezvan, M. Barekatain, P. Adibi, P. Barnaghi, and A. P. Sheth, "Machine learning for internet of things data analysis: a survey," *Digital Communications and Networks*, vol. 4, no. 3. Chongqing University of Posts and Telecommunications, pp. 161–175, Aug. 01, 2018. doi: 10.1016/j.dcan.2017.10.002.
26. M. Esposito, L. Palma, A. Belli, L. Sabbatini, and P. Pierleoni, "Recent Advances in Internet of Things Solutions for Early Warning Systems: A Review," *Sensors*, vol. 22, no. 6. MDPI, Mar. 01, 2022. doi: 10.3390/s22062124.
27. A. Gaurav, B. B. Gupta, and P. K. Panigrahi, "A comprehensive survey on machine learning approaches for malware detection in IoT-based enterprise information system," *Enterprise Information Systems*, vol. 17, no. 3. Taylor and Francis Ltd., 2023. doi: 10.1080/17517575.2021.2023764.
28. L. Nemec Zlatolas, N. Feher, and M. Hölbl, "Security Perception of IoT Devices in Smart Homes," *Journal of Cybersecurity and Privacy*, vol. 2, no. 1, pp. 65–74, Feb. 2022, doi: 10.3390/jcp2010005.
29. A. Ali, A. Mateen, A. Hanan, and F. Amin, "Advanced Security Framework for Internet of Things (IoT)," *Technologies*, vol. 10, no. 3. MDPI, Jun. 01, 2022. doi: 10.3390/technologies10030060.
30. R. Ahmad and I. Alsmadi, "Machine learning approaches to IoT security: A systematic literature review[Formula presented]," *Internet of Things (Netherlands)*, vol. 14. Elsevier B.V., Jun. 01, 2021. doi: 10.1016/j.iot.2021.100365.
31. A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," *Future*

Generation Computer Systems, vol. 82, pp. 761–768, 2018, doi: 10.1016/j.future.2017.08.043.

32. M. Abomhara and G. M. Køien, "Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks," *Journal of Cyber Security and Mobility*, vol. 4, no. 1, pp. 65–88, Jan. 2015, doi: 10.13052/jcsm2245-1439.414.
33. 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. Institute of Electrical and Electronics Engineers Inc., pp. 82721–82743, 2019. doi: 10.1109/ACCESS.2019.2924045.
34. M. Alshahrani and I. Traore, "Secure mutual authentication and automated access control for IoT smart home using cumulative Keyed-hash chain," *Journal of Information Security and Applications*, vol. 45, pp. 156–175, Apr. 2019, doi: 10.1016/j.jisa.2019.02.003.
35. H.-J. Kim, H.-S. Chang, J.-J. Suh, and T. Shon, "A Study on Device Security in IoT Convergence," Oct. 2016, pp. 1–4. doi: 10.1109/ICIMSA.2016.7503989.
36. P. Williams, I. K. Dutta, H. Daoud, and M. Bayoumi, "A survey on security in internet of things with a focus on the impact of emerging technologies," *Internet of Things (Netherlands)*, vol. 19. Elsevier B.V., Aug. 01, 2022. doi: 10.1016/j.iot.2022.100564.
37. E. Bout, V. Loscri, and A. Gallais, "How Machine Learning Changes the Nature of Cyberattacks on IoT Networks: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 248–279, 2022, doi: 10.1109/COMST.2021.3127267.
38. A. Fatani, A. Dahou, M. A. A. Al-Qaness, S. Lu, and M. A. Elaziz, "Advanced feature extraction and selection approach using deep learning and aquila optimizer for iot intrusion detection system," *Sensors*, vol. 22, no. 1, Jan. 2022, doi: 10.3390/s22010140.
39. A. F. Jahwar and S. R. M. Zeebaree, "A State of the Art Survey of Machine Learning Algorithms for IoT Security," *Asian Journal of Research in Computer Science*, pp. 12–34, Jun. 2021, doi: 10.9734/ajrcos/2021/v9i430226.
40. N. Islam *et al.*, "Towards Machine Learning Based Intrusion Detection in IoT Networks," *Computers, Materials and Continua*, vol. 69, no. 2, pp. 1801–1821, 2021, doi: 10.32604/cmc.2021.018466.
41. L. Da Xu, Y. Lu, and L. Li, "Embedding Blockchain Technology Into IoT for Security: A Survey," *IEEE Internet Things J*, vol. 8, no. 13, pp. 10452–10473, 2021, doi: 10.1109/JIOT.2021.3060508.
42. J. Sengupta, S. Ruj, and S. Das Bit, "A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149. Academic Press, Jan. 01, 2020. doi: 10.1016/j.jnca.2019.102481.
43. B. Omoniwa, R. Hussain, M. A. Javed, S. H. Bouk, and S. A. Malik, "Fog/Edge Computing-Based IoT (FECIoT): Architecture, Applications, and Research Issues," *IEEE Internet Things J*, vol. 6, no. 3, pp. 4118–4149, 2019, doi: 10.1109/JIOT.2018.2875544
44. S. Gupta, V. K. Sharma, "Blockchain-based Secure IoT Architecture: A Review," IEEE Access, 2023.
45. A. Khan, M. H. Rehmani, "Machine Learning-based Intrusion Detection System for IoT Networks," IEEE Internet of Things Journal, 2022.
46. T. Nguyen, J. Patel, "Deep Learning Approaches for Anomaly Detection in IoT Networks," ACM Transactions on Internet of Things, 2023.
47. R. Sharma, S. Singh, "Fog Computing-based Secure Data Storage for IoT Devices," IEEE

Transactions on Dependable and Secure Computing, 2023.
48. K. Patel, A. Kumar, "Edge Computing-enabled Authentication Mechanism for IoT Devices," IEEE Transactions on Industrial Informatics, 2022.
49. S. Li, Q. Wang, "Blockchain-based Access Control System for IoT Devices," Future Generation Computer Systems, 2023.
50. G. Singh, N. Jain, "Machine Learning-driven Threat Intelligence Framework for IoT Security," Journal of Network and Computer Applications, 2022.
51. H. Chen, J. Zhang, "Deep Learning-based Malware Detection in IoT Devices," Computers & Security, 2023.
52. L. Wang, Y. Zhao, "Fog Computing-assisted Secure Data Processing for Healthcare IoT," IEEE Transactions on Industrial Informatics, 2022.
53. X. Liu, Z. Zhang, "Edge Computing-based Intrusion Prevention System for Smart Grid IoT," IEEE Transactions on Smart Grid, 2023.
54. M. Ahmed, S. Khan, "Blockchain-based Secure Firmware Update Mechanism for IoT Devices," IEEE Internet of Things Journal, 2023.
55. A. Sharma, R. Gupta, "Machine Learning-driven Anomaly Detection for Industrial IoT Systems," Journal of Manufacturing Systems, 2022.
56. J. Li, X. Wang, "Fog Computing-enabled Privacy Preservation in IoT Data Analytics," IEEE Transactions on Cloud Computing, 2023.
57. Y. Zhang, H. Wang, "Deep Learning-based Intrusion Detection System for Vehicular IoT Networks," IEEE Transactions on Vehicular Technology, 2022.
58. S. Kumar, P. Jain, "Edge Computing-assisted Secure Communication Protocol for IoT Devices," IEEE Transactions on Information Forensics and Security, 2023