INTERNATIONAL JOURNAL OF RESEARCH CULTURE SOCIETY
Monthly Peer-Reviewed, Refereed, Indexed Journal
Volume - 8, Issue - 11, November - 2024

ISSN(O): 2456-6683
[Impact Factor: 9.241]

IJRCS

DOIs:10.2017/IJRCS/202411001 --:-- Research Paper / Article / Review

Machine Learning - Taxonomy, Challenges, and Future Research Directions for Authentication and Authorization in the Internet of Things

Ms. Varkha K. Jewani (Pragati V. Thawani) [1] , Dr. Prafulla E Ajmire[2]

Dr. Mohammad Atique Mohammad Junaid[3], Dr. Zeba Atique Shaikh[4]

[1]*Research Scholar, Computer Science Dept., Sant Gadge Baba Amravati University, Amravati, India*
vkjewani@gmail.com
[2]*Supervisior, Computer Science Dept., Sant Gadge Baba Amravati University, Amravati, India*
peajmire@gmail.com
[3]*Professor & Head, Department of Computer Science, Faculty of Engineering & Technology, Sant Gadge Baba Amravati University, India. EMAIL - mohd.atique@gmail.com*
[4]*Research Scholar, Computer Science and Engineering Dept., Sant Gadge Baba Amravati University, Amravati, India*
zeba.shaikh2207@gmail.com

Abstract— *one of the main obstacles to the Internet of Things' (IoT) broad acceptance, despite continuous efforts to promote its adoption, is security. Securing Internet of Things (IoT) networks, including water supply or electricity grids, has become a top national and international responsibility. To tackle the security issue associated with the Internet of Things, a number of studies utilizing blockchain, AI, and edge/fog computing are now underway. The CIA triad's authentication and permission are essential components for defending the network against hostile actors. However, because of the size of IoT networks and the resource-constrained nature of devices, current authorization and authentication techniques are insufficient to handle security. There is a lot of interest in applying machine learning techniques to help with the authentication and authorization process for IoT to overcome obstacles caused by various limits of IoT networks. This paper reviews current developments in IoT network authentication and authorization methods. Author offers a taxonomy of IoT authentication and authorization systems based on the review, with an emphasis on machine learning-based schemes. An extensive examination of the authentication and authorization (AA) security risks and difficulties for Internet of Things is given, utilizing the taxonomy that has been offered. In addition, several standards for achieving a high level of AA resilience in IoT deployments are assessed to improve IoT security. Finally, a thorough examination of outstanding problems, difficulties, and potential research avenues is provided to enable secure IoT nodes.*

Keywords: Internet of Things, IoT, Security, Authentication, Authorization, Machine Learning.

1. INTRODUCTION :

By the end of 2025, over 30 billion devices are expected to be connected to the Internet [1]. The potential that IoT has to enhance corporate operations and spur growth is the cause of this increase. The Internet of Things (IoT) is a network of interconnected physical objects that may be uniquely identified by intelligent objects or devices (like sensors) that are connected to the Internet in a variety of environments and could produce events [2, 3]. Thus, to facilitate data exchange across nodes, security measures such as key management, data protection, secure sessions on communication establishments, dependable hardware/software patches, monitoring, and auditing must be implemented on IoT nodes. IoT security is directly impacted by data exchange amongst IoT nodes, which is mostly dependent on the reliability of the data and the quality of service provided. For instance, millions of Internet of Things devices infected with the Mirai malware were the source of a distributed denial of service (DDoS) attack. Using a straightforward web application, many Internet of Things (IoT) devices, including smart home and closed-circuit television systems, were compromised by malware and deployed against the servers [4]. The initial lines of defense in Internet of Things environments are authentication and authorization (AA), which limit activities and actions [5]. By imposing user limitations and exposing vital resources to unauthorized parties, AA seeks to avoid breaches. Authentication, along with defense mechanisms against outside intrusions like man-in-the-middle attacks [6] and eavesdropping assaults [7, 8], is typically tailored to address various risks at specific network conditions. Malicious behavior, however, is erratic and cannot be addressed prior to every attack. To combat both external and internal dangers, AA provides security services. By continuously analyzing the connectivity patterns of nodes after effective initial authentication, machine learning (ML)-based AA is a promising tool to counter these threats. It allows security schemes to learn how to identify and counteract new and existing complex attacks efficiently, allowing any behavioral shifts from valid to suspicious to be observed. It is not practical

to directly apply ML algorithms on IoT devices due to resource constraints. Consequently, it is anticipated that effective ML-based AA with feature reduction strategies will reduce resource consumption while maximizing data availability, accuracy, and efficiency [9].

1.1 Current Issues and Motivation

A few securities need to be met to facilitate the widespread use of IoT [10, 11]. IoT security researchers must devote a great deal of attention to authentication and authorization since they are essential security features. Currently, many Internet of Things implementations use centralized client-server architecture and connect to the cloud using the online. Cloud servers that identify, authenticate, and connect all devices accommodate large amounts of processing and storage. Interaction amongst Internet of Things devices even if they are nearby, they must pass through the cloud. One such model is vulnerable to coordinated attacks, delays, and outages that could impact the operation of the whole system. The limited resources of Internet of Things devices make the issue worse. Because they were not created for devices with limited resources, the existing best security practices cannot be used to secure the Internet of Things environment, leaving billions of devices vulnerable to attack. For certain IoT features (such as clustering, protocols, applications, data aggregation, services, architectures, resource allocation, and security for the time being), traditional methodologies are effective. AA systems that manage distributed access from many IoT nodes in a secure and efficient manner will be required soon. IoT has become an important component in many deployments, including smart parking, home, and industry systems, energy utilization management, traffic control, and remote health care services. Customers and service providers demand the privacy of their actions, and personal information in all such implementations. To win over users' trust, IoT needs to ensure complete security and privacy of its users. There is a dearth of research on ML-based IoT security that concentrates on authentication and authorization, even though ML and IoT access management systems are currently important fields of study [12].

1.2. Authentication and Authorization in IoT

Two essential elements of online device and consumer protection are authorization and authentication. This makes these elements necessary for the deployment of IoT. because, at its most basic, the Internet of Things is just a network of connected gadgets—from basic sensors to sophisticated mobile devices and cars—that exchange data. The device identification process known as authentication verifies the legitimacy of the device client ID and ensures that it is unique to that device. A node (sensor node or user) that has been granted authorization can access resources like reading or writing data, executing programs, and manipulating actuators. Revocation or denial of access is also covered by authorization, particularly in the case of someone or something malevolent. Moreover, authorization offers a way to associate a particular device (or subject membership group of devices) with services.

There are two different kinds of authorization and authentication procedures: one for users and one for devices. The authentication and authorization of devices is the main topic of this review study. A great illustration of this is a sensor. Device identity and authorization level are established through the AA procedures prior to the initiation of the communication session and the sensory data exchange.

2. LITERATURE REVIEW

IoT security-related topics have been the subject of several academic studies. For instance, writers in [13] provided an overview of IoT threat mitigation techniques using "autonomic security." These tactics were divided into three categories by the writers: self-healing, self-protecting, and a hybrid of self-defence and self-repair. They provided three descriptions of the use against various threats. Layers: analysis, processing, communication, and perception (Cloud). Similarly, Ref. [14] examined the protocols in place to manage Internet access and IoT confidentiality. Future directions, possibilities, and difficulties in IoT security were offered by the work. It did not, however, look at IoT authentication and authorization techniques in a methodical manner. Issues with security and confidentiality are looked at in [15, 16]. There is a discussion on IoT device limitations and related security solutions. Additionally, a categorization of Internet of Things attacks, and access control methods is provided. It does not, however, address IoT AA with nodes' dynamic behavior. The writers of [17] took a comprehensive approach to IoT by considering device architecture, security, and privacy. They offered difficulties for Internet of Things and edge computing applications. The authors of [18] discussed the significance of ML-driven techniques for Internet of Things security and privacy. In a different study, Ref. [19] investigated the efficacy of machine learning (ML)-driven strategies to detect intrusions in Internet of Things (IoT) networks by utilizing these techniques in intrusion detection systems, either through traffic classification or anomalies. Similarly, the authors [20] talked about the comprehensive study of privacy and security across the levels (physical, network, and application). Additionally, the authors outline the drawbacks of the existing ML-driven techniques and algorithms for Internet of Things security.

Table 1 recapitulates the research contributions related to the authentication and authorization found in the literature.

References	Authors Contribution(s)
Yang et al. [16]	Discussing IoT attacks, examining IoT access control systems and architectures, analyzing security challenges in various IoT layers.
Lin et al. [17]	A summary of the issues with security and privacy, as well as the difficulties with fog/edge computing and Internet of Things applications.
Xiao et al. [18]	Addressing the significance of ML-driven techniques for IoT privacy and security by demonstrating how ML-

	driven security solutions are put into practice for IoT networks.
El-hajj et al. [15]	authentication domain. It offers an overview of the many different authentication techniques that have been put forth in the literature.
Preeti et al. [19]	This study investigated the feasibility of machine learning (ML)-driven plans to detect intrusions in Internet of Things networks by utilizing these techniques in intrusion detection systems, either through anomalies or traffic categorization.
Hussain et al. [20]	Talking about a thorough examination of privacy and security across the network, application, and physical layers.

3. Machine Learning for IoT Security

This section offers a succinct summary of some machine learning algorithms and how they are applied in the Internet of Things.

3.1 Supervised Learning- In IoT networks, supervised learning algorithms are used for spectrum detection, channel estimation, adaptive filtration, and position determination. They work with labelled datasets. Regression and classification are the two distinct process types that are included in this group. Among the most often used classification methods are decision trees, random forests, naive Bayes, and support vector machines (SVM). Polynomial and logistic regression are two often used regression techniques. These algorithms, which forecast output based on the learnt model for every new observation, are also referred to as "instance-based" algorithms. For IoT security, supervised learning algorithms including SVM, DT, and naïve Bayes (NB) have been extensively utilized. For example, SVMs contain non-linear constraints for a solution model. However, SVM is ineffective for large data sets. Compared to SVM, random forest methods are easier to use and can adjust to a large dataset.
It provides a higher level of accuracy and cuts down on prediction time [21]. Training takes longer than SVM and NB, though. Processing large amounts of feature-rich data and using a lot of memory are requirements for logistic regression and neighboring methods. Supervised learning techniques have been applied to IoT networks in the communication layer and cloud to identify intrusions and DDoS attacks.

3.2 Unsupervised Learning – The unsupervised learning algorithms employ heuristics to identify patterns in the input data by analyzing unlabeled data. Unsupervised algorithms find anomalies, trends, and cluster classes. Classification algorithms are used in unsupervised learning to categorize the data. Unsupervised techniques in IoT can be applied without any prior knowledge of the intended result. K-means and hierarchical clustering are two common clustering techniques that are based on unsupervised machine learning algorithms. The most common method of clustering is K-means clustering, which is based on a straightforward algorithm that creates clusters based on patterns found in the data points (e.g., normal or abnormal traffic). Same-size clusters are produced because of the cluster/edge groups forming around the centroids. However, defining the number of clusters during the clusters' creation is necessary, and this isn't always possible with accuracy and efficiency [22]. Unsupervised learning techniques, such K-means, are typically employed in the communication layer to identify anomalies and Sybil attacks.

3.3 Reinforcement Learning - Reinforcement learning (RL) techniques discover the best combination of behaviors to maximize reward by experimenting with different actions in each context. This reward system helps to solve several IoT security problems [23]. To choose the best course of action in a particular condition, RL interacts with the environment and learns from experience without requiring any prior knowledge of the surroundings. While RL techniques are straightforward, it takes a while to find the best course of action. The primary concerns in dynamic Internet of Things network environments are this sluggish convergence and an ideal state transition function or policy. Unlike conventional methods like linear aggregation, reinforcement machine learning can adjust and respond to changes over time. A key component of creating an autonomous communications system that can effectively protect Internet of Things devices without interference from the outside world and is sophisticated enough to foresee any failures is illustrated by RL. By learning from the cloud or any other high-computational edge device's environment, reinforcement learning techniques (such as Q-learning) can be employed for IoT device authentication, jamming detection, and malware attack detection without the need for a previous training dataset [24, 25].

4. Taxonomy of ML-Based AA for IoT

The suggested classification for AA in IoT is shown in this section. The suggested taxonomy is based on an analysis of numerous research studies that considered a number of factors when creating AA schemes for Internet of Things security. The research on AA can be grouped using the following classes based on the examination of the body of available literature.

1. AA-based IoT Security Requirements
2. Attacks and Risks for AA in IoT
3. Techniques used for AA
4. Characteristics of the AA schemes

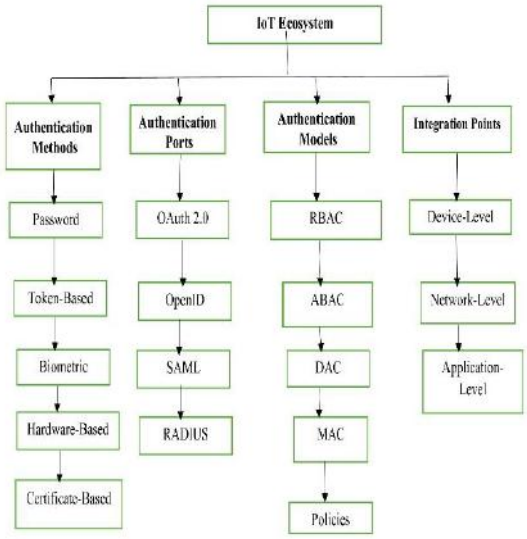

Fig. 1-Taxonomy of ML-based AA for IoT

4.1 AA-Based IoT Security Requirements- There are many different criteria for securing IoT networks because of the heterogeneity and restricted nature of IoT devices. The following are the IoT security prerequisites that must be met for any AA systems:

- **Light weightiness**: The primary need for AA schemes in the Internet of Things is that they be small enough to function adequately for multiple IoT nodes under all energy conditions [26–28].
- **Privacy Profiling and Tracking:** One vulnerability that might lead to privacy profiling and tracking is the combination of an identity with a particular person [29]. Thus, prohibiting IoT operation is one of the main issues, and the security system must oversee safeguarding the privacy of the customers.
- **Robustness and Resilience**: The IoT AA system needs to be robust and resilient to attacks because of the increasing number of attack vectors, IoT node failures, and agility. Additionally, security networks should be able to identify flaws and fix them right away by taking the appropriate action.
- **Heterogeneity**: Networks and nodes inside the Internet of Things are diverse. Because of the properties of the end device, heterogeneity is a fundamental necessity for the AA scheme. Heterogeneity in AA systems will address problems with a variety of device kinds.
- **High Availability**: Despite risks occurring within the Internet of Things network, the high availability of the AA Scheme verifies that all network services are fully available feasible [30].
- **High Accuracy:** To access any IoT node and the network as a whole, a high degree of accuracy level of any AA scheme is necessary [31]. A high degree of precision in the authorization and authentication process will guarantee the system's overall high level of security.
- **High Reliability:** A crucial prerequisite for all authorization and authentication protocols is high reliability. The success rate of the method is what matters. It verifies that, for the duration indicated, every function within the IoT network is functioning properly.

4.2 Attacks and Risks for AA in IoT

For the purpose of protecting networks and devices in the Internet of Things (IoT), Access Authentication (AA) is essential. But when it comes to authentication methods, the Internet of Things environment poses several hazards and obstacles. The following are some typical AA attacks and dangers in Internet of Things environments:[32]

- **Phishing attacks –**
  Credential theft: Attackers may deceive administrators or users into divulging their authentication credentials.
  Key Extraction: Via physical access or reverse engineering, attackers can obtain the keys from devices that use hardcoded or poorly protected credentials.
- **Attacks in Replay**
  Replay of Authentication Data: To obtain unauthorized access, attackers may intercept authentication tokens or credentials and replay them. If session tokens are not unique or tokens are not time-sensitive, this becomes very problematic.
- **Attacks by a Man-in-the-Middle (MitM)**
  Intercepting and Modifying Authentication Data: Cybercriminals can listen in on and modify the authentication information that is transferred between devices or between a device and a server.
  Session Hijacking: If appropriate encryption and validation are not implemented, attackers may be able to take control of an ongoing session.
- **Attacks with a denial of service (DoS)**
  Overloading the authentication server or device with too many requests can be the result of an attack and cause the service to become unavailable.

4.3 Techniques used for AA

In the context of the Internet of Things (IoT), access authentication (AA) refers to a number of strategies and procedures that make sure that only authorized users and devices are able to access the network and its resources. In IoT contexts, the following methods of authentication are frequently employed:[33]

Password-Related Verification

Description: To authenticate, users or devices need to provide their login and password.

Difficulties: It can be challenging to manage passwords for multiple devices, and passwords may be weak or compromised.

Top Techniques: Employ policies for passwords, create strong, complicated passwords, and think about combining them with additional authentication techniques (such multi-factor authentication).

O Authentication: An open standard for token-based authorization and authentication is called OAuth (Open

Authorization). OAuth makes it possible to grant access tokens to outside apps without disclosing user credentials.
Benefits: Often utilized for web and mobile apps, it permits secure assigned access.
Versions: OAuth 2.0 (often used), OAuth 1.0a.
OpenID Connect is an authentication layer that is based on OAuth 2.0 and offers a standardized method for user authentication and identity retrieval.
Benefits: Offers single sign-on (SSO) and user authentication. ID tokens and user data endpoints are the components.
Kerberos Overview: Kerberos is a network authentication protocol that enables nodes to safely identify themselves over an insecure network by using tickets.
Benefits: Mutual authentication is offered, guaranteeing server and user authentication.
Ticket Granting Ticket (TGT), Service Tickets, and Key Distribution Center (KDC) are the components.

4.4 Characteristics of the AA schemes

In the context of the Internet of Things (IoT) or any other system, access authentication (AA) schemes must have a few essential features to guarantee that they are efficient, safe, and appropriate for the intended use. The following are the main traits of AA schemes:[34]

- **Confidentiality**: Provides protection against unauthorized access to authentication data, including tokens, keys, and credentials.
  Application: Encrypt data before sending it and while storing it. Use safe storage procedures and keep private information hidden.
- **Integrity:** Ensures that unapproved parties cannot change or tamper with authentication data. Application: To guarantee that the data is not changed during transmission or storage, use digital signatures and cryptographic hash algorithms.
- **Authenticity**: Assures that people or devices are who they say they are by confirming their identification. Use robust authentication techniques, such digital certificates, biometric verification, and multi-factor authentication (MFA), in your implementation.
- **Non-Repudiation**: Assures that the device or user cannot retract their participation in the actions taken or their involvement once authentication has been completed.
  Implementation: To generate an audit trail of authentication events, employ digital signatures and logging systems.
- **Scalability:** The authentication system's capacity to accommodate a growing number of users or devices without seeing a decrease in performance.
  Implementation: Create scalable authentication structures that handle large-scale deployments by using cloud-based or distributed systems.

5. Open Issues, Challenges, and Future Directions

IoT is thought to be: (a) highly complex, with frequent and quick changes to the security requirements of network entities; and (b) highly heterogeneous, with a wide range of network entity types and characteristics. Therefore, before ML-based AA is integrated into IoT to increase security, several concerns must be resolved. An AA process uses a wide range of encryption techniques, including hash keys, XOR-based encryption, Elliptic-curve cryptography (ECC), using a smart card, and biometric technology. Any newly created AA scheme should aim to be small and protect IoT nodes from assaults by considering the little amount of space and low processing power factor seen in IoT devices. [35].

- **Resource Constraint and Robustness of Authentication Protocols**: The end nodes with the fewest resources are the sensors (low battery capacity, limited processing resources).
  The protocols must be simple and balance resource use with security.
  Low computation costs should also be considered in the design of IoT authentication systems, particularly in resource-constrained and IoT framework environments. This emphasizes the requirement for lightweight encryption methods and protocols to be implemented in authentication systems. Robustness against potential attacks such as Sybil, node capture, interpret, password identification, message breaches, brute forces, broker, protection, collision, and text selection is a need for the authentication methods.
  - **Authorization for Every Service**: User identities are required to gain access to many services, however certain identities are exclusive to a particular service. As a result, based on the many services that want to be able to access and use identity data, a scheme needs to offer a way to gain access to the device. As a result, sharing user information between system services is either prohibited or requires adherence to each service's authorization guidelines.
  - **Sharing Data to reduce on Overhead**: In devices with limited resources, especially, communication is greatly impacted by the overhead of authentication procedures. Communication partners should exchange fewer communications with each other. Because IoT devices have limited capacity, the message should be as quiet as possible.
  - **Anonymity:** Because of the considerable data exchange involved with IoT, anonymity is a major problem. An attacker might target the Internet of Things (IoT) network to get information about IoT nodes, which could divulge vital data, such as medical records. As an alternative, a hacker can locate a person or item and damage the gadgets or their characteristics, particularly in a mobile network. Future research can concentrate on data anonymization and create an open Internet of Things security procedure.[36].

6. Conclusion :

IoT is spreading quickly across a variety of industries. Given the recent attacks on the IoT network, which demonstrate how vulnerable IoT networks are, this raises grave worries about the security of IoT devices. IoT networks have the potential to greatly endanger end users by increasing the vulnerabilities in the current IoT network if they are not

properly secured. Based on a thorough examination of IoT networks' risks related to authorization and authentication, as well as how new and old approaches evolve and get better, the flaws can be reduced. This analysis offered a thorough analysis and suggested a thorough taxonomy of AA in Internet of Things networks. We examined many facets of AA using broad and ML-driven approaches based on the taxonomy to examine how AA can enhance the IoT ecosystem. Security and pinpoint possible areas for further study. IoT architecture considering AA methods are also covered, with an emphasis on different types of threats and assaults in every IoT layer. The For ML-based IoT applications, requirements and current difficulties have also been examined. However, the researchers have not considered basic performance parameters like the delay and the location for IoT node authentication in the majority of ML-based IoT AA schemes. Moreover, the literature contains relatively few ML-driven permission techniques. Therefore, to increase the security of the Internet of Things, it is imperative to look into ML-driven AA schemes while taking standard and ML performance measures into account. These metrics include the perception, communication, data processing, analysis, and application layers. In addition, architectural strategies like hybrid approaches, which go beyond centralized or solely distributed systems, can be employed in conjunction with machine learning for IoT authentication.

REFERENCES

1. Statista. Internet of Things—Active Connections Worldwide 2015–2025; Statista Research Department: Hamburg, Germany, 2021.
2. Li, X.; Lu, R.; Liang, X.; Shen, X.; Chen, J.; Lin, X. Smart community: An internet of things application. IEEE Commun. Mag. 2011, 49, 68–75. [CrossRef]
3. Ahad, A.; Tahir, M.; Sheikh, M.A.; Ahmed, K.I.; Mughees, A.; Numani, A. Technologies trend towards 5g network for smart healthcare using iot: A review. Sensors 2020, 20, 4047. [CrossRef]
4. Kolias, C.; Kambourakis, G.; Stavrou, A.; Voas, J. DDoS in the IoT: Mirai and other botnets. Computer 2017, 50, 80–84. [CrossRef]
5. Putra, G.D.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R. Trust management in decentralized iot access control system. In Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2–6 May 2020; pp. 1–9.
6. Kang, J.J.; Fahd, K.; Venkatraman, S.; Trujillo-Rasua, R.; Haskell-Dowland, P. Hybrid Routing for Man-in-the-Middle (MITM) Attack Detection in IoT Networks. In Proceedings of the 2019 29th International Telecommunication Networks and Applications Conference (ITNAC), Auckland, New Zealand, 27–29 November 2019. [CrossRef]
7. Qijun Gu, Peng Liu, "Denial of Service Attacks", Handbook of Hajiheidari, S.; Wakil, K.; Badri, M.; Navimipour, N.J. Intrusion detection systems in the Internet of things: A comprehensive investigation. Comput. Netw. 2019, 160, 165–191. [CrossRef]
8. Shu, Z.; Wan, J.; Li, D.; Lin, J.; Vasilakos, A.V.; Imran, M. Security in Software-Defined Networking: Threats and Countermeasures. Mob. Netw. Appl. 2016, 21, 764–776. [CrossRef]
9. Jayasinghe, U.; Lee, G.M.; Um, T.W.; Shi, Q. Machine Learning Based Trust Computational Model for IoT Services. IEEE Trans. Sustain. Comput. 2018, 4, 39–52. [CrossRef]
10. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Commun. Surv. Tutor. 2015, 17, 2347–2376. [CrossRef]
11. Airehrour, D.; Gutierrez, J.; Ray, S.K. Secure routing for internet of things: A survey. J. Netw. Comput. Appl. 2016, 66, 198–213. [CrossRef]
12. Ali, I.; Sabir, S.; Ullah, Z. Internet of Things Security, Device Authentication and Access Control: A Review. Int. J. Comput. Sci. Inf. Secur. 2019, 14, 456–466.
13. Ashraf, Q.M.; Habaebi, M.H. Autonomic schemes for threat mitigation in Internet of Things. J. Netw. Comput. Appl. 2015, 49, 112–127. [CrossRef]
14. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy and trust in Internet of things: The road ahead. Comput. Netw. 2015, 76, 146–164. [CrossRef]
15. El-Hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A survey of internet of things (IoT) authentication schemes. Sensors 2019, 19, 1141. [CrossRef]
16. Yang, Y.; Wu, L.; Yin, G.; Li, L.; Zhao, H. A Survey on Security and Privacy Issues in Internet-of-Things. IEEE Internet Things J. 2017, 4, 1250–1258. [CrossRef]
17. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. IEEE Internet Things J. 2017, 4, 1125–1142. [CrossRef]
18. Xiao, L.; Wan, X.; Lu, X.; Zhang, Y.; Wu, D. IoT Security Techniques Based on Machine Learning. arXiv 2018, arXiv:1801.06275.
19. Mishra, P.; Varadharajan, V.; Tupakula, U.; Pilli, E.S. A detailed investigation and analysis of using machine learning techniques for intrusion detection. IEEE Commun. Surv. Tutor. 2019, 21, 686–728. [CrossRef]
20. Hussain, F.; Hussain, R.; Hassan, S.A.; Hossain, E. Machine Learning in IoT Security: Current Solutions and Future Challenges. IEEE Commun. Surv. Tutor. 2020, 22, 1686–1721. [CrossRef]
21. Hasan, M.; Islam, M.M.; Zarif, M.I.I.; Hashem, M. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. Internet Things 2019, 7, 100059. [CrossRef]
22. Sun,P.; Li, J.; Alam Bhuiyan, M.Z.; Wang, L.; Li, B. Modeling and clustering attacker activities in IoT through machine learning techniques. Inf. Sci. 2018, 479, 456–471. [CrossRef]
23. Park, T.; Abuzainab, N.; Saad, W. Learning How to Communicate in the Internet of Things: Finite Resources and Heterogeneity. IEEE Access 2016, 4, 7063–7073. [CrossRef]

24. Xiao, L.; Li, Y.; Huang, X.; Du, X. Cloud-based malware detection game for mobile devices with offloading. IEEE Trans. Mob. Comput. 2017, 16, 2742–2750. [CrossRef]
25. Xiao, L.; Xie, C.; Chen, T.; Dai, H.; Poor, H.V. A Mobile offloading game against smart attacks. IEEE Access 2016, 4, 2281–2291. [CrossRef]
26. Tahir, M.; Sardaraz, M.; Muhammad, S.; Khan, M.S. A Lightweight Authentication and Authorization Framework for Blockchain Enabled IoT Network in Health-Informatics. Sustainability 2020, 12, 6960. [CrossRef]
27. Lee, D.H.; Lee, I.Y. A lightweight authentication and key agreement schemes for IoT environments. Sensors 2020, 20, 5350. [CrossRef]
28. Lara, E.; Aguilar, L.; Sanchez, M.A.; García, J.A. Lightweight authentication protocol for M2M communications of resource constrained devices in industrial internet of things. Sensors 2020, 20, 501. [CrossRef]
29. Nespoli, P.; Zago, M.; Celdrán, A.H.; Pérez, M.G.; Mármol, F.G.; Clemente, F.J. PALOT: Profiling and authenticating users leveraging internet of things. Sensors 2019, 19, 2832. [CrossRef] [PubMed]
30. Yang, H.; Kim, Y. Design and Implementation of High-Availability Architecture for IoT-Cloud Services. Sensors 2019, 19, 3276. [CrossRef] [PubMed]
31. Jayasinghe, U.; Otebolaku, A.; Um, T.W.; Lee, G.M. Data centric trust evaluation and prediction framework for IOT. In Proceedings of the 2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K), Nanjing, China, 27–29 November 2017; pp. 1–7. [CrossRef]
32. Fraile, F.; Tagawa, T.; Poler, R.; Ortiz, A. Trustworthy Industrial IoT Gateways for Interoperability Platforms and Ecosystems. IEEE Internet Things J. 2018, 5, 4506–4514. [CrossRef]
33. Ferreira, C.M.S.; Garrocho, C.T.B.; Oliveira, R.A.R.; Silva, J.S.; Cavalcanti, C.F.M.d.C. IoT registration and authentication in smart city applications with blockchain. Sensors 2021, 21, 1323. [CrossRef]
34. Banks, A.; Briggs, E.; Borgendale, K.; Gupta, R. MQTT Version 5.0; Standard, O. A. S. I. S: 2019. Available online: https: //docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html (accessed on 20 July 2020)
35. Elmouaatamid, O.; Lahmer, M.; Belkasmi, M. Group authentication with fault tolerance for internet of things. In International Symposium on Ubiquitous Networking; Springer: Cham, Switzerland, 2017; Volume 10542 LNCS, pp. 299–307. [CrossRef].
36. Varkha Jewani, Prafulla Ajmire, Geeta Brijwani, A Security Framework for IoT using Machine Learning Technique, Design Engineering ISSN: 0011-9342 | Year 2021Issue: 8 | Pages: 15892-15906[15892].