International Journal of Safety and Security Engineering
Vol. 12, No. 2, April, 2022, pp. 209-216
Journal homepage: http://iieta.org/journals/ijsse

Study and Analysis of Various Authentication and Authorization for IoT Devices: A Challenging Overview

Pallavi Sunil Bangare[1,2*], Kishor P. Patil[1]

[1] Department of E&TC, Sinhgad Academy of Engineering, Savitribai Phule Pune University, Pune 411048, India
[2] Department of Information Technology, Sinhgad Academy of Engineering, Savitribai Phule Pune University, Pune 411048, India

Corresponding Author Email: psbangare.sae@sinhgad.edu

https://doi.org/10.18280/ijsse.120209

Received: 1 February 2022
Accepted: 28 March 2022

Keywords:
authentication, authorization, internet of things, security, network

ABSTRACT

Nowadays, Internet of Things (IoT) is being achieved significant improvement in the scientific community. Both industry and academia are concentrated on the concepts of improving security, maintainability and utility through the improvement and standardization of optimal practices. There are various existing approaches are arisen in the security of IoT, ranging from cryptography to network security for identifying management. Thus, this paper focused on the security due to its impacts of limiting factors to adoption of wider IoT. This paper discusses the survey of various existing approaches suitable for IoT environment in the domain of authentication and authorization. Hence, this survey analyzes various techniques corresponding to authentication and authorization for IoT devices. This study is to utilize 25 research papers concentrated on various techniques and the review of researches technique-wise is to be provided. Finally, the survey will encourage the analysis based on the publication year, research methodology, performance metrics, and achievement of the research techniques toward authentication and authorization for IoT devices, as well as the journals. Finally, the research gaps and difficulties with the methodologies will be highlighted. Furthermore, the motive for establishing an effective approach for authentication and authorisation in IoT device techniques will be disclosed.

1. INTRODUCTION

The Internet of Things is an intelligent methodology, which interlinks all the elements, involves sensors, cellular phones and other home appliances. In this model, the information is broadcasted among people and elements exist in the internet. Nowadays, numerous IoT applications are assists the users through communication among smart phones. These devices are employed to utilize, access and process the relevant information gathered from the sensors. From this feature, the Smartphone is primarily considered for the common device, which is progressively augmenting the performance. This plays a major establishing role for accessing and controlling several devices in the IoT environment, like cellular phone, smart city, smart grid and smart health. Due to the commercial improvement of IoT devices, IoT has become the necessary need for the routine life of people. The wireless sensor network (WSN) has become a major element of IoT, which is responsible to collect and deliver the substantial phenomenon as well as information through the numerous quantities of resource constrained and heterogeneous sensors. Hence, the incorporation of WSN and 5G network provides a successful deployment of IoT devices. Due to the incorporation of WSN and 5G network, multiple sensors and the smart devices are introduced for the private lives of every people. This model enhanced the connectivity, but the security attack arises in the model cannot be resolved. To protect the IoT devices from the attackers or unregistered persons, the effective authorization and authentication model is to established in the IoT environment [1].

Security is the major functions in all the networks due to the attackers. Since, the attackers are penetrating into the network for getting the valuable information stored in the network. The internet-based healthcare model holds the relevant information of the patients, which are more susceptible to privacy anxiety [2]. In the IoT-based healthcare paradigm, privacy and security are important concerns in most devices, and information is broadcasted wirelessly among such devices. Because humans are directly involved in healthcare applications, wireless transmission of such information implies that strong and secure communication among actuators, sensors, caregivers, and patients is necessary. The exploitation or privacy concerns may limit the people for employing IoT-based healthcare applications [3]. Traditional privacy and preserving mechanism involve existing cryptographic approaches, secure set of rules and security assurance cannot be used again for resource constraints, security-based requirements and system model of IoT-based healthcare models [4]. To resolve the security issues, the powerful security model is established for both short and long communication range. The security of network is enhanced by subjecting multiple security solutions in the network. One is based on the effectiveness of security algorithm, which is based on the power, bandwidth and memory. The less amount of using these resources is to make the algorithm as infeasible. The clinical-based sensor nodes may lose or crashed due to the

minute size. These limitations can be resolved through the powerful authentication and authorization approaches [5].

The fundamental goal of this method is to examine the various mechanisms used in IoT-based authentication and authorisation approaches. The security techniques are divided into authentication methods, authorization methods, and combinations of both methods based on the application area used in security approaches. This survey is organised based on the programme used, technique classification, publication year, and performance measure. The review articles' weaknesses are extensively discussed in the research gaps and problems section. Furthermore, the better performance parameter, known as execution time, is discussed in the analysis section. As a result, the section on research gaps stimulated enthusiasm for future extensions of security enhancing measures. This survey paper is organized in the following order: Section 2 explains the review of various techniques involved in the authentication and authorization methods, and section 3 includes the research gaps and issues of these models. Section 4 demonstrates the investigation of security enhancement model of IoT approaches based on methods, utilized tool set, performance metrics and year of publication, and the conclusion of this survey is provided in section 5.

2. LITERATURE SURVEY

This section described the various methods employed for the authentication and authorization in IoT devices. The security of IoT devices can be achieved by authorization and authentication approaches. Figure 1 depicts the categorization of security approaches in IoT. The challenges of security enhancement approaches were motivated the researchers for doing the research in this domain.

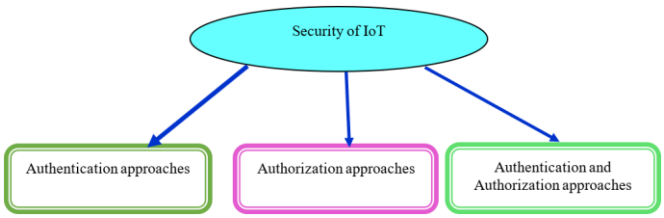

Figure 1. Categorization of security approaches in IoT

2.1 Categorization of IoT-based security approaches

The review of various techniques utilized for security enhancement of IoT are based on authentication approaches, authorization approaches, and the combination of both of the approaches, which are described in the subsection.

2.1.1 Authentication approaches

This section describes the various authentication mechanisms used for IoT security augmentation. The approach created by Azad et al. [6] has the main characteristic of providing an auto-enforcing authentication mechanism for securing the network against unregistered users. In this scenario, the authentication approach relied on a low entropy password, but not in the Public-Key Infrastructure (PKI) or an authorised third party. The following is the operating principle: In a Password-Authenticated Key Exchange (PAKE) system, two or more parties (a client and a server or two clients) use a password to identify themselves to each other. The parties create a cryptographic session key by exchanging a series of messages. The unauthorised party (one who controls the communication channel but does not know the password) could not provide successful authentication and could not guess the password using this strategy. Azad et al approach's is based on the Password Authenticated Key Exchange through Juggling protocol (or J-PAKE). The J-PAKE protocol allows two parties to communicate in a secure and authenticated manner utilising a low-entropy shared password without the use of a Public-Key Infrastructure (PKI). The J-PAKE protocol allows two parties to communicate in a secure and authenticated manner utilising a low-entropy shared password without the use of a Public-Key Infrastructure (PKI). To verify that parties follow the protocol parameters, the J-PAKE protocol incorporates Zero Knowledge Proofs. This method proved to be incredibly efficient against the network's many sorts of security attacks. Although the processing overhead of this strategy was little in this example, the method's computational complexity was substantial. The work that is lacking is that of a true SIP server and client. So, while this may be the study's weakest link, the author has recommended for it in the future.

Azrour et al. [7] developed the improved authentication model for enhancing the security in IoT devices. This model was developed to resist the various kinds of external attacks. This security model contains the various phases, namely sensor addition, registration of user phase, login as well as authentication phase, and the password modification phase. Finally, the analysis of security was verified through the mutual authentication scheme. Although, this method was very effective against various kinds of attacks, but the computational cost of this method was high.

Mandal et al. [8] developed the certificate-free signcryption approach for the IoT environment. This method was employed for the access control purpose of user in order to improve the security. This method was achieved the low computation cost and low communication cost. This method was comprised of several phases, like initialization, enrollment, registration, login and access control, inclusion of smart device phase, and user revocation phase. Finally, the security was validated through the security analysis model, named biometric update phase. Although, this method was reduced the computational cost, but this method was failed to process with real world applications.

Deebak [9] developed the lightweight authentication and key management approach for assisting the regular mutual user verification model, which suggests the secure transmission among the communication devices. This method was restricted the excess utilization of evaluation resources. This authentication approach was subjected to the less processing operations, like hash function, hash dependent authentication scheme, and the Ex-OR operation. The authentication scheme was enhanced by generating the key token among the peer estimation devices. This method was also monitored the energy consumption among the established devices. However, this method did not provide the better security, due to the poor resource usage.

Guo et al. [10] developed the trust dependent master slave authentication model for enhancing the security of IoT devices. This method was designed by combining the distribution authentication model along with master slave model. The trust behavior of authentication model was enhanced through reputation-based Byzantine fault acceptance model. Although, this method was improved the efficiency and credibility of

authentication model, but this method was achieved high computational overhead.

Almadhoun et al. [11] developed the blockchain-based authentication model for the security enhancement of IoT devices. This method was employed for recognizing the user to admit IoT devices. Here, the fog nodes were employed for suggesting the scalability of the system through IoT devices from the burden computational task. This authentication approach was composed of admin, end-user, fog nodes, IoT devices and cloud. Although, this method was employed for establishing the user and IoT devices, but still this method was failed to process with real Ethereum network.

Shah and Venkatesan [12] designed the multi-key-based authentication approach using secure vaults. In this model, the secret key was communicated among IoT server and device, named secure vault, which was gathered from similar sized various smaller keys. The primary portion of secure vault was established among IoT device as well as server and secure vault key. This method was consumed less memory, and the computational power consumed by this method was low. However, this method was susceptible to distinct types of attacks.

Gope and Sikdar [13] designed the privacy dependent and lightweight authentication approach for IoT devices. In this model, a new authentication factor was established, named externally unclonable function. This method was not only focused on the security, but the computational efficiency of the system was also enhanced. This security model was composed of two phases, named setup phase and authentication phase. The authentication phase includes the request, server response, server authentication and device authentication. Moreover, the security of this model was analyzed through the privacy model. However, this method was failed to analyze with password guessing attack.

Walshe et al. [14] developed the noninteractive zero-knowledge (NIZKP) authentication protocol, which was formed by integrating the certain factors in sensors and communication IoT. This method was resisted against the certain external attacks. This method was established the message exchange protocol along with security authentication mechanism. Although, the execution time of this method was low, but failed to process with hash functions. Sciancalepore et al. [15] developed the elliptic curve-based authentication mechanism in IoT devices for improving the computation complexity of network model. This method was formed by incorporating the key management protocol with Elliptic curve authentication approach. Although, this method was robust against the various replay attacks, but the method failed to process with other kinds of attacks.

2.1.2 Authorization approaches

The various authorization approaches employed for the security enhancement of IoT is explained in this section. Ghosh et al. [16] developed the authorization mechanism, termed as SoftAuthZ for the security enhancement of IoT. This mechanism was formed by the incorporation of such soft security models, like confidence, belief and so on. This method was employed for assisting the decision of authorization models. This method was incorporated the various IoT-based environmental attributes, like environmental context, device nature, trust levels and variability. The confidence score achieved by this method was employed for making the authorization decisions. This method was achieved the maximum rate of authorization and improved the validation of efficiency. However, the simulation time of this method was high.

Cirani et al. [17] developed the open authorization models for improving the security analysis of IoT. This method was highly configurable and flexible. The processing operation was performed on the IoT-OAuth architecture. This architecture was permitted the access tokens, authorization requests and communication protocols. This architecture was employed in various communication scenarios, like network broker, Gateway, end-to-end and hybrid gateway communication. This method was reduced the energy consumption of this model. The computational time and storage overhead of this model was low. This method was failed to process with real world applications.

Siris et al. [18] developed the decentralized-based approach for the IoT-security enhancement. This method was introduced the two policies for establishing this approach. The first policy was utilized the information of server, such as time and cost. The second policy was operated based on first server. This method was achieved delay, execution cost and information reduction, which was required to be transmitted through the IoT devices. However, this method did not produce the better result with multiple ledgers.

Chifor et al. [19] developed the authorization scheme for the security enhancement of IoT. This method was a lightweight identity scheme for identifying the digital process in IoT devices. The processing of this scheme was relied on the authentication of federated cloud. This method was evaluated from the extension of authentication-based transmitted message. The security of this scheme was enhanced through keep-alive protocol. The security scheme was validated through the topology of Kaa IoT-based network. Although, this method was solved the security issues happens in the network, but this method was failed to process with other kinds of IoT distributors.

Grande and Beltrán et al. [20] developed the delegation-based authorization approach for enhancing the privacy of IoT devices. This method was relied on the cryptographic scheme, which was utilized extensively and familiar protocols, like OAuth and constrained protocol. The processing of this method was based on the three set of rules, like auto-enrolment of constrained devices, authorized access and resource deployment. This protocol was evaluated through real world applications. Although, this method was achieved the effective power utilization and latency, but this method did not achieve the fault tolerance.

Zemmoudj et al. [21] developed the context-aware authorization model for enhancing the security of IoT devices. This method was especially developed for preserving the records of patient exchanged and communicated through the IoT devices using context-aware security and context aware protocol. To achieve this, two kinds of protocols were developed, such as Pseudonym service and delegation protocol. The Pseudonym service was employed to protect the record of patients, and the delegation protocol was relied on the context and trust-based. This protocol was employed to produce the rules with the trust values. Although, the efficiency of this protocol was high, but the public-key certificate was not processed.

2.1.3 Authentication and authorization approaches

The various authentication and authorization approaches employed for the security enhancement of IoT is explained in this section. Shin and Kwon [1] developed the hybrid security

approach using the combination of WSN and 5G for IoT. This architecture model was composed of the combination of Elliptic curve cryptography (ECC)-based privacy preserving model and key agreement scheme in IoT. The security analysis was performed against the certain external attacks. Although, this protocol was more effective and secure, but this method was failed to process with real world applications.

Hernandez-Ramos et al. [22] developed the Architectural Reference Model (ARM) for enhancing the security of IoT devices. This approach was evaluated for assisting the smart objects while processing. The ARM-based security model contains key management, authorization and authentication, which was performed based on the reputation as well as trust. The context manager was introduced to manage all the operations performed in the IoT network. The entire security processing performed in the scenario was based on the decision-making rules. However, this method did not attain the convincible security improvement.

Sebastian et al. [23] developed the security enhancement of IoT in noisy environments. This architecture was composed of channel setup, credential exchange and token revocation. This method was preserved the information from unauthorized person. The communication was established among the client and authorization server. The resource server acts as an intermediate among client and authorization server. The resource server was provided the file in the form of token file as well as credential file. Although, this method was very feasible, the network connectivity of this method was low.

Ali et al. [24] developed the xDBAuth method for improving the security of IoT devices. The xDBAuth method was developed by the incorporation of block chain model and authentication approaches for IoT devices. This method was formed by the incorporation of local and global contracts, which was performed the delegation and access control model. In addition, the developed method was protected the privacy of external user through permitting the authentication of IoT services. After performing the authentication, the authorization model was established based on the validation phase of block chain. Although, this method was achieved the less computational overhead and high throughput, but the computational cost of this model was low.

Lohachab [25] developed the ECC-based security enhancement approach for IoT devices. This model was composed of seven phases, like initialization, setup, registration, access policy, authentication and data exchange, credential update and revoke phase for executing the operations. Each of the phases exist in the architecture was performed various operations. The analysis of security was verified through informal and formal analysis. Although, this method was achieved the maximum transmission efficiency, but this method did not produce the better result with real world applications.

Wetzels et al. [26] developed the hybrid security scheme for preserving the security of IoT. This method was allowed to integrate present and custom Application Programming Interface (API) with the absence of restarting services. The data aggregation model was composed of internal and external services, which contains multiple API. The communication was established among user and user tokens. The end points in this model were terminated to request and authentication models. The endpoints in this model contains API-based authentication and callbacks, logout, login and sign-up. This method was necessitating the extensive processing overhead.

Moosavi et al. [5] developed the smart gateways for preserving the security of IoT. This method was relied on the certificate-based handshake protocol based on the IP security solution. This method was diminished the impacts of Denial-of-Service (DoS) attack owing to the distributed nature of architecture. Although, this method reduced the communication overhead as well as communication latency, but failed to produce the better result all time due to the impact of varying environment.

Tahir et al. [27] developed the block chain-based security enhancement approach for both authorization and authentication of IoT in health informatics. The block chain-based model was established for the elimination of unauthorized or third party, data sharing improvement, immutability, cost of overhead and security enhancement. This method was formed the random numbers in the authentication process, which was linked through the joint conditional probability. This method was established among IoT devices for the acquisition of information. Although, this method was achieved the better communication cost and computational overhead, but this method did not achieve the better result with real world applications.

Pajooh and Rashid [28] developed the optimization model for the privacy preserving purpose of IoT devices. This model was partitioned the network into multiple number of clusters through evolutionary algorithms. The evolutionary algorithm was formed by combining the Genetic Algorithm (GA) as well as Particle Swarm Optimization (PSO). This approach was performed through the assistance of cluster head. Although, this method was achieved the augmented security and credibility, but the peer-to-peer nature of this model was low. Gulati et al. [29, 30] have also given IOT and Wireless Networking review. Bangare et al. [31] have used the IOT for their work of data transfer using “LiFi”. Bangare et al. [32-35] have proposed the machine learning and IoT work for various domains. Joseph et al. [36] worked for the real time systems and Bangare et al. [37] have shown the collateral extensions in IoT security. Bangare et al. [38] Fog computing-based security for IoT systems. Pande et. al. [39] have presented a detailed survey of latest neural network termed as Capsule Network (CapsNet) which finds its application in several domains including IoT. Pande et. al. [40, 41] have presented an approach for extracting control points which can be used for secured routing in IoT enabled devices.

3. RESEARCH GAPS IDENTIFIED

The research gaps and issues achieved during the analysis of security enhancement using authentication and authorization approaches in IoT are given below.

The research gap of authentication model is as follows:

The auto-enforcing authentication approach did not process well with real server and clients. Thus, the challenge lies on developing a prototype for establishing the actual server as well as clients [6]. The security of blockchain model was low [8], thus the challenge lies on exploring the blockchain model for achieving the properties, like transparency and immutability [8]. The security enhancement model did not achieve the real-world applications for investigating the functional attributes, like computation and communication cost [9]. The Ethereum network was failed to connect with real world Ethereum network for establishing the network with client [11].

The research gap of authorization model is as follows:

The SoftAuthZ security model was failed to collect the user centric information. Thus, the challenge lies on implementing the multi user model for collecting the user centric information as well as validation based on detection of anomalous events by Ghosh et al. [16]. Cirani et al. [17] shows that the performance of oauth-based authorization service (OAS) model was poor in IoT environment. Thus, the challenge lies on implementing the procedure on both simulation and actual test beds for evaluating the performance of constrained environment. The research gap of authentication and authorization model was listed in this section. The security of ECC model did not effective all time due to the varying environment by Shin and Kwon [1]. Hernandez-Ramos et al. [22], this method was failed to achieve the trade-off among security features. The dynamic nature of ECC model was very poor, which was affected the performance of model [25].

4. ANALYSIS AND DISCUSSION

This section described the analysis and discussion of various security methods in IoT using authentication and authorization approaches. The various methods employed for the security of IoT devices are analyzed through categorization of methods, implementation tools, publication year and employed metrics.

4.1 Analysis based on security methods

The various analysis methods employed for the security of IoT devices are discussed in this section. The security analysis based on authentication and authorization approaches are discussed in Figure 2. From Figure 2, it is realized that 40% of research papers were employed the authentication approaches for the security of IoT, and 24% of research papers were utilized the authorization approaches for the security of IoT. Similarly, the authentication and authorization approaches were employed for the security of IoT is 28% and 8% of the research papers were utilized the other techniques for the security of IoT. From the analysis, most of the research papers were employed authentication approach for improving the security of IoT.

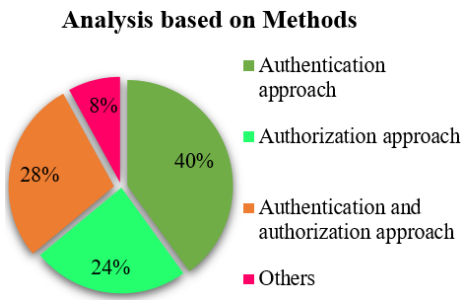

Figure 2. Analysis based on methods

4.2 Analysis using publication year

This section described the analysis of publication year based on the authentication and authorization approaches for which the 25 papers were surveyed. The survey based on the publication year is expressed in Table 1. Among the 25 research papers, most of the research papers regarding authentication and authorization approaches were published in the year of 2019.

4.3 Analysis using employed software

This section described the implementation tools adapted by the existing authentication and authorization approaches in IoT devices. The analysis of various implementation tools for the authentication and authorization approaches are depicted in Figure 3. The utilized tools for the implementation tools were AVISPA, cooja, Java, python, NS3, ACPT and Scyther. From Figure 3, it is clearly known that, JAVA is the most widely employed software for the authentication and authorization approaches.

4.4 Analysis using performance metrics based on number of papers published

This section described the survey of various evaluation metrics based on the number of published papers among the 25 research papers utilized for the authentication and authorization approaches in IoT. The analysis of various evaluation metrics for the security enhancement in IoT are depicted in Figure 4. The evaluation metrics achieved through the security analysis of IoT approaches are computation cost, communication cost, authorization rate, confidence score, energy consumption, memory usage, execution time, delay, throughput and latency. From the analysis, execution time is the most widely employed parameter for the security analysis of IoT.

Table 1. Analysis based on publication year

Number of papers	Publication year
3	2015
1	2016
3	2017
5	2018
7	2019
5	2020
1	2021

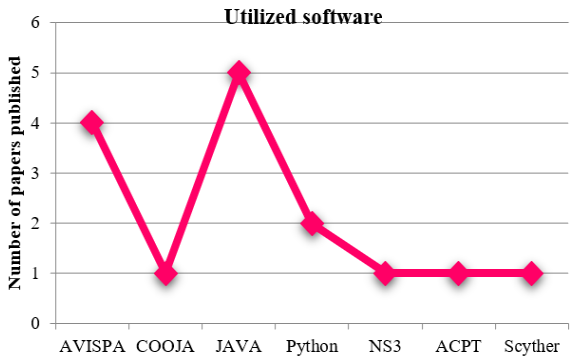

Figure 3. Analysis based on employed software

4.5 Analysis of metrics based on research papers

This section described the performance metrics utilized for the security analysis of IoT based on research papers are given in Table 2. The performance metrics employed for the research papers were computation cost, communication cost, authorization rate, confidence score, energy consumption, memory usage, execution time, delay, throughput and latency. From these evaluation parameters, it is clearly declared that the execution time was the enormously utilized metrics for the performance evaluation of various methods.

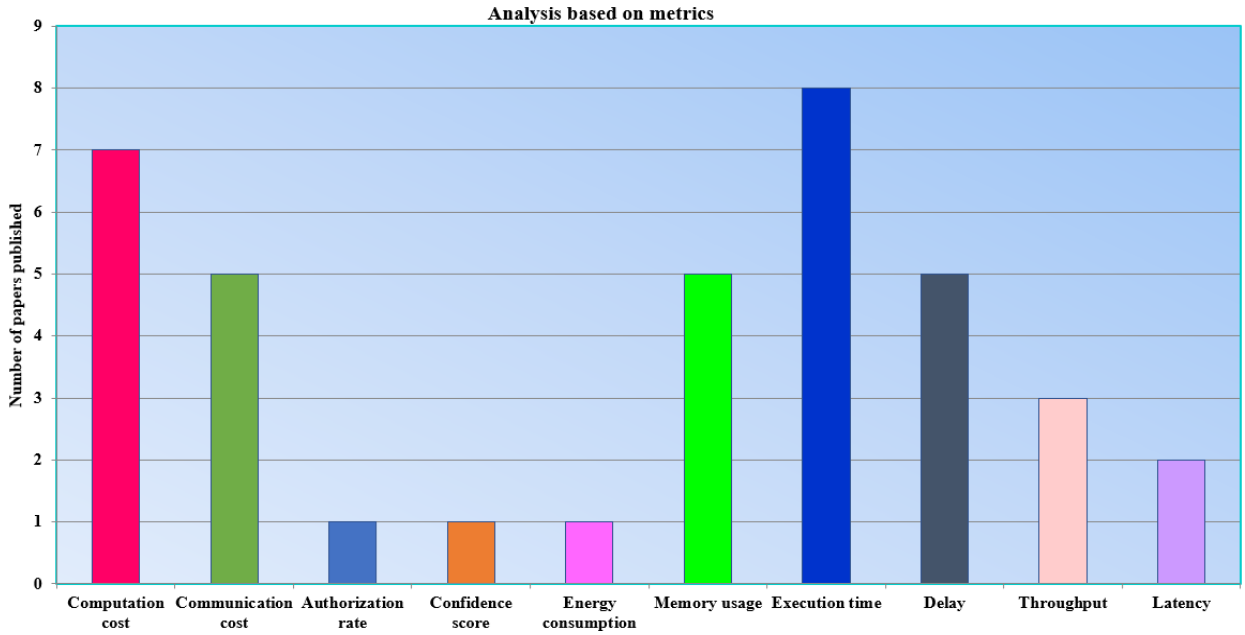

Figure 4. Analysis based on simulation metrics

4.6 Performance analysis based on performance metrics

This section depicts the analysis of performance metrics values in terms of execution time are discussed below.

Table 2. Analysis of metrics

Metrics	Published papers
Computation cost	[1, 7-9, 18, 24, 25]
Communication cost	[1, 5, 8, 9, 18]
Authorization rate	[16]
Confidence score	[16]
Energy consumption	[12]
Memory usage	[12, 17, 20, 22, 23]
Execution time	[9, 12, 13, 15, 21, 24, 25, 27]
Delay	[5, 9, 10, 18, 20]
Throughput	[9, 10, 27]
Latency	[5, 20]

Table 3. Analysis using execution time

Execution time	Range (in millisecond)
[24]	0.04
[25]	0.765
[9]	6.434
[27]	70
[12]	2.5
[13]	1.23
[15]	800
[21]	1320

The analysis using performance metrics is expressed in this section using Table 3. Moreover, Table 3 shows the investigation using execution time by covering various range of time in milliseconds. From the below table, it is recognized that, the research paper [24] assumed less execution time in milliseconds, and research paper [21] has assumed maximum execution time in milliseconds.

5. CONCLUSION

This paper includes an overview of several security-based authentication and authorisation approaches. This survey is organised by gathering 25 research articles from various publications found in Google scholar, and the papers obtained are classified based on authentication, authorization, and a mix of both techniques. Each of these systems used various strategies to improve IoT security, such as cryptographic-based approaches, block chain-based models, certificate-based models, delegation protocols, and so on. The research articles included in this study were compiled from a variety of internet sources, including Google Scholar, IEEE, Springer, and others.

The gathered research articles are surveyed, and gaps and concerns addressed by specific current research publications are presented. Furthermore, this study offers future work for IoT security analysis in terms of identifying various research gaps and challenges. Following that, the analysis and discussion of this survey are offered based on approach classification, implementation tools, publication year, and assessment metrics. The study clearly shows that authentication procedures were widely used in the majority of research articles. Aside from these, execution time was the most often employed performance parameter in the majority of the security enhancement and analysis methods in IoT research articles. Similarly, the majority of security enhancement techniques were published in 2019, and the majority of research publications used Java as a platform.

Although the certificate-free signcryption solution for the IoT environment had a cheap computational cost, it did not perform well in real-world applications. The lightweight authentication and key management solution aided the traditional mutual user verification paradigm, but it had low security. The trust-dependent master-slave authentication approach used to improve the security of IoT devices had a significant computational burden. Blockchain-based models are vulnerable to several forms of assaults. The privacy-sensitive and lightweight authentication strategy for IoT devices was unable to withstand a password guessing attack. Other attacks were similarly rejected by the noninteractive zero-knowledge (NIZKP) authentication mechanism. SoftAuthZ has a high authorisation for IoT security enhancement, but the simulation time is also high. The open authorization frameworks for increasing IoT security analyses

failed to deal with real-world applications. With many ledgers, the decentralised approach to IoT security enhancement did not yield a superior outcome. The delegation-based authorisation solution for improving IoT device privacy has low latency but poor fault tolerance. The context-aware authorization approach has a high efficiency for improving the security of IoT devices, but the public-key certificate was not processed. The Architectural Reference Model (ARM) for improving the security of IoT devices could not achieve the desired level of protection. the improvement of IoT security in noisy areas with limited network connectivity. The xDBAuth approach for increasing IoT device security had a cheap computing cost and a high throughput. With real-world implementations, the ECC-based security improvement technique for IoT devices did not deliver a better outcome. Because of the influence of various environments, smart gateways for protecting IoT security failed to offer better results all of the time. The block chain-based security improvement technique for both IoT authorization and authentication in health informatics has not yielded promising results in real-world applications. The calculation cost, communication cost, authorization rate, confidence score, energy consumption, memory use, execution time, delay, throughput, and latency are the assessment metrics obtained via the security analysis of IoT techniques. The future work is the authentication and authorization methods which have low computing cost, high security, good tolerance and high throughput.

REFERENCES

[1] Shin, S., Kwon, T. (2020). A privacy-preserving authentication, authorization, and key agreement scheme for wireless sensor networks in 5G-integrated Internet of Things. IEEE Access, 8: 67555-67571. https://doi.org/10.1109/ACCESS.2020.2985719

[2] Shahzad, M., Singh, M.P. (2017). Continuous authentication and authorization for the internet of things. IEEE Internet Computing, 21(2): 86-90. https://doi.org/10.1109/MIC.2017.33

[3] Trnka, M., Cerny, T., Stickney, N. (2018). Survey of Authentication and Authorization for the Internet of Things. Security and Communication Networks, 2018: 4351603. https://doi.org/10.1155/2018/4351603

[4] Fang, H., Qi, A., Wang, X. (2020). Fast authentication and progressive authorization in large-scale IoT: How to leverage ai for security enhancement. IEEE Network, 34(3): 24-29. https://doi.org/10.1109/MNET.011.1900276

[5] Moosavi, S.R., Gia, T.N., Rahmani, A.M., Nigussie, E., Virtanen, S., Isoaho, J., Tenhunen, H. (2015). SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. Procedia Computer Science, 52: 452-459. https://doi.org/10.1016/j.procs.2015.05.013

[6] Azad, M.A., Bag, S., Perera, C., Barhamgi, M., Hao, F. (2019). Authentic caller: Self-enforcing authentication in a next-generation network. IEEE Transactions on Industrial Informatics, 16(5): 3606-3615. https://doi.org/10.1109/TII.2019.2941724

[7] Azrour, M., Mabrouki, J., Guezzaz, A., Farhaoui, Y. (2021). New enhanced authentication protocol for internet of things. Big Data Mining and Analytics, 4(1): 1-9. https://doi.org/10.26599/BDMA.2020.9020010

[8] Mandal, S., Bera, B., Sutrala, A.K., Das, A.K., Choo, K. K.R., Park, Y. (2020). Certificateless-signcryption-based three-factor user access control scheme for IoT environment. IEEE Internet of Things Journal, 7(4): 3184-3197. https://doi.org/10.1109/JIOT.2020.2966242

[9] Deebak, B.D. (2020). Lightweight authentication and key management in mobile-sink for smart IoT-assisted systems. Sustainable Cities and Society, 63: 102416. https://doi.org/10.1016/j.scs.2020.102416

[10] Guo, S., Wang, F., Zhang, N., Qi, F., Qiu, X. (2020). Master-slave chain based trusted cross-domain authentication mechanism in IoT. Journal of Network and Computer Applications, 172: 102812. https://doi.org/10.1016/j.jnca.2020.102812

[11] Almadhoun, R., Kadadha, M., Alhemeiri, M., Alshehhi, M., Salah, K. (2018). A user authentication scheme of IoT devices using blockchain-enabled fog nodes. In 2018 IEEE/ACS 15th international conference on computer systems and applications (AICCSA), Aqaba, Jordan, pp. 1-8. https://doi.org/10.1109/AICCSA.2018.8612856

[12] Shah, T., Venkatesan, S. (2018). Authentication of IoT device and IoT server using secure vaults. In 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), York, NY, USA, pp. 819-824. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00117

[13] Gope, P., Sikdar, B. (2018). Lightweight and privacy-preserving two-factor authentication scheme for IoT devices. IEEE Internet of Things Journal, 6(1): 580-589. https://doi.org/10.1109/JIOT.2018.2846299

[14] Walshe, M., Epiphaniou, G., Al-Khateeb, H., Hammoudeh, M., Katos, V., Dehghantanha, A. (2019). Non-interactive zero knowledge proofs for the authentication of IoT devices in reduced connectivity environments. Ad Hoc Networks, 95: 101988. https://doi.org/10.1016/j.adhoc.2019.101988

[15] Sciancalepore, S., Piro, G., Boggia, G., Bianchi, G. (2016). Public key authentication and key agreement in IoT devices with minimal airtime consumption. IEEE Embedded Systems Letters, 9(1): 1-4. https://doi.org/10.1109/LES.2016.2630729

[16] Ghosh, N., Chandra, S., Sachidananda, V., Elovici, Y. (2019). SoftAuthZ: A context-aware, behavior-based authorization framework for home IoT. IEEE Internet of Things Journal, 6(6): 10773-10785. https://doi.org/10.1109/JIOT.2019.2941767

[17] Cirani, S., Picone, M., Gonizzi, P., Veltri, L., Ferrari, G. (2014). IoT-OAS: An OAuth-based authorization service architecture for secure services in IoT scenarios. IEEE Sensors Journal, 15(2): 1224-1234. https://doi.org/10.1109/JSEN.2014.2361406

[18] Siris, V.A., Dimopoulos, D., Fotiou, N., Voulgaris, S., Polyzos, G.C. (2020). Decentralized authorization in constrained IoT environments exploiting interledger mechanisms. Computer Communications, 152: 243-251. https://doi.org/10.1016/j.comcom.2020.01.030

[19] Chifor, B.C., Bica, I., Patriciu, V.V., Pop, F. (2018). A security authorization scheme for smart home Internet of Things devices. Future Generation Computer Systems, 86: 740-749.

https://doi.org/10.1016/j.future.2017.05.048
[20] Grande, E., Beltrán, M. (2020). Edge-centric delegation of authorization for constrained devices in the Internet of Things. Computer Communications, 160: 464-474. https://doi.org/10.1016/j.comcom.2020.06.029
[21] Zemmoudj, S., Bermad, N., Omar, M. (2019). Context-aware pseudonymization and authorization model for IoT-based smart hospitals. Journal of Ambient Intelligence and Humanized Computing, 10(11): 4473-4490. https://doi.org/10.1007/s12652-018-1129-0
[22] Hernandez-Ramos, J.L., Pawlowski, M.P., Jara, A.J., Skarmeta, A.F., Ladid, L. (2015). Toward a lightweight authentication and authorization framework for smart objects. IEEE Journal on Selected Areas in Communications, 33(4): 690-702. https://doi.org/10.1109/JSAC.2015.2393436
[23] Echeverria, S., Lewis, G.A., Klinedinst, D., Seitz, L. (2019). Authentication and authorization for IoT devices in disadvantaged environments. In 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, pp. 368-373. https://doi.org/10.1109/WF-IoT.2019.8767192
[24] Ali, G., Ahmad, N., Cao, Y., Khan, S., Cruickshank, H., Qazi, E.A., Ali, A. (2020). xDBAuth: Blockchain based cross domain authentication and authorization framework for Internet of Things. IEEE Access, 8: 58800-58816. https://doi.org/10.1109/ACCESS.2020.2982542
[25] Lohachab, A. (2019). ECC based inter-device authentication and authorization scheme using MQTT for IoT networks. Journal of Information Security and Applications, 46: 1-12. https://doi.org/10.1016/j.jisa.2019.02.005
[26] Wetzels, M., Ayoola, I., Bogers, S., Peters, P., Chen, W., Feijs, L. (2018). Consume: A privacy-preserving authorisation and authentication service for connecting with health and wellbeing APIs. Pervasive and Mobile Computing, 43: 20-26. https://doi.org/10.1016/j.pmcj.2017.11.002
[27] Tahir, M., Sardaraz, M., Muhammad, S., Saud Khan, M. (2020). A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics. Sustainability, 12(17): 6960. https://doi.org/10.3390/su12176960
[28] Rashid, M.A., Pajooh, H.H. (2019). A security framework for IoT authentication and authorization based on blockchain technology. In 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, pp. 264-271. https://doi.org/10.1109/TrustCom/BigDataSE.2019.00043
[29] Gulati, K., Boddu, R.S. K., Kapila, D., Bangare, S.L., Chandnani, N., Saravanan, G. (2021). A review paper on wireless sensor network techniques in Internet of Things (IoT), 51: 161-165. https://doi.org/10.1016/j.matpr.2021.05.067
[30] Gulati, K., Sriram, V.P., Sharma, M., Robin, S.E., Bangare, S.L. (2021). Use for graphical user tools in data analytics and machine learning application. Turkish Journal of Physiotherapy and Rehabilitation; 32(3): 3540-3546.
[31] Bangare, S.L., Srivastava, A., Siddiqui, S., Kumar, A., Bhagat, P. (2020). File sharing application using lifi. Mukt Shabd Journal Ugc Care List Group - I Journal, 9(6): 5179-5187.
[32] Bangare, S.L., Pradeepini, G., Patil, S.T. (2018). Regenerative pixel mode and tumour locus algorithm development for brain tumour analysis: A new computational technique for precise medical imaging. International Journal of Biomedical Engineering and Technology, 27(1-2): 76-85. https://dx.doi.org/10.1504/IJBET.2018.093087
[33] Bangare, S.L., Pradeepini, G., Patil, S.T. (2017). Neuroendoscopy adapter module development for better brain tumor image visualization. International Journal of Electrical and Computer Engineering, 7(6): 3643-3654.
[34] Bangare, S.L. (2022). Classification of optimal brain tissue using dynamic region growing and fuzzy min-max neural network in brain magnetic resonance images. Neuroscience Informatics, 2(3): 100019. https://doi.org/10.1016/j.neuri.2021.100019
[35] Bangare, S.L., Bangare, P.S., Patil, K.P. (2021). Internet of Things with Green Computing. Turkish Journal of Physiotherapy and Rehabilitation, 32(3): 12494-12497.
[36] Joseph, L.L., Shrivastava, P., Kaushik, A., Bangare, S.L., Naveen, A., Raj, K.B., Gulati, K. (2021). Methods to identify facial detection in deep learning through the use of real-time training datasets management. EFFLATOUNIA-Multidisciplinary Journal, 5(2): 1298-1311.
[37] Bangare, S.L., Athawale, S., Giri, V. (2021). Collateral extension in provocation of security in IoT. International Journal of Future Generation Communication and Networking, 14(1): 3703-3716.
[38] Bangare, M.L., Bangare, P.M., Apare, R.S., Bangare, S.L. (2021). Fog computing based security of IoT application. Design Engineering, (7): 7542-7549.
[39] Pande, S.D., Chetty, M.S.R. (2018). Analysis of capsule network (Capsnet) architectures and applications. Journal of Advanced Research in Dynamical and Control Systems, 10(10): 2765-2771.
[40] Pande, S.D., Chetty, M.S.R. (2019). Position invariant spline curve based image retrieval using control points. International Journal of Intelligent Engineering Systems, 12(4): 177-191. https://doi.org/10.22266/ijies2019.0831.17
[41] Pande, S.D., Patil, U.A., Chinchore, R., Chetty, M.S.R. (2019). Precise approach for modified 2 stage algorithm to find control points of cubic Bezier curve. In 2019 5th International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, India, pp. 1-8. https://doi.org/10.1109/ICCUBEA47591.2019.9128550