SPAST Open Access Research

Authentication schemes for Post Cloud Computing-enabled IoT Models: A Systematic Review

Upendra Verma[1], Dr. Divya Midhunchakkaravarthy[2], Dr. Pawan Kumar Chaurasia[3]
[1]Post Doc Researcher, Lincoln University College, Malaysia; [2]Director, Centre of Postgraduate Studies, Lincoln University College, [3]Associate Professor, Babasaheb Bhimrao Ambedkar Central University, Lucknow. drupendra.pdf@lincoln.edu.my

Abstract

In recent years, the post-cloud computing model has become one of the most significant technological advancement because of its capability to process a wide range of delay-sensitive IoT applications. Post-cloud commuting model provides several services closer to the IoT devices called Post-cloud computing-enabled IoT model. The IoT devices have limited computational resources in delay-sensitive IoT applications. Thus, security solutions must be lightweight and response-intensive. The authentication plays a crucial role in post-cloud computing model. This work provides a comprehensive review of authentication schemes for post-cloud computing model, analyzing their limitations, strengths and application domain. The objective of this review is to provide direction to researchers and scholars in the development of authentication schemes, particularly for post-cloud computing models including edge computing, fog computing, and dew computing.

Keywords: Post-cloud computing model; Authentication schemes; Delay-sensitive IoT applications; Dew computing; Fog computing; Edge computing.

Introduction

Today, applications for the Internet of Things (IoT) may be found in a number of industries and sectors, including smart city, healthcare, smart grid, smart transportation, industrial automation, etc. [1-4]. A new computing models like fog computing [5], edge computing [6], and dew computing [7] have been introduced in order to meet the real-time demands of particular applications. Users have started benefiting from the on-demand availability of computing resources for data storage and processing power through cloud computing. Fog computing uses nodes that are less distant from IoT devices and higher computational capabilities in contrast to IoT devices. With contrast to centralized cloud, data is processed more quickly with fog computing. Another paradigm is edge computing, which enables primarily IoT and mobile computing by distributing compute and data storage to the closest place. Edge computing restricts the issue of bandwidth and communication latency by reducing distant communications. Fog computing allows for task sharing, whereas edge computing places processing at the edge device. All computing paradigm should require internet connection to continue the operations. However, the services won't be available if the Internet connection is lost. In these circumstances, dew computing has emerged to offer the connectivity with the devices. Dew computing can serve as a bridging technology between cloud and IoT devices. The computational services can be accessed with dew computing even without an internet connection. Figure 1 illustrates the architecture of post-cloud computing-enabled IoT model. In this model, the post-cloud computing models provide services to the delay sensitive IoT applications. The requirement for constant internet access is the major restriction of cloud and fog computing. Dew computing sets itself apart by offering extremely little dependency on the internet, close proximity to the end user, reduced latency, and higher speed. In dew computing, for instance, you can have a browser page open and being used without having access to the internet (cloud), with data accessible from an on-site computer. Dew computing is not a replacement for cloud computing; rather, it provides a complementary service. Data centres and servers can be viewed as a form of cloud computing. Fog computing may act as a small cloud, router, gateway etc. Edge computing considered as a one way hope from the devices. The on-site computers (in the absence of internet connectivity) that offer services to IoT devices are represented by dew computing.

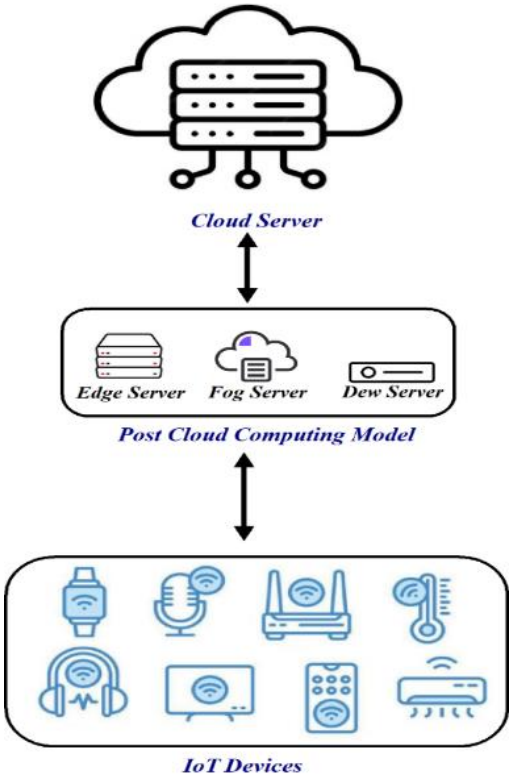

Figure 1. Architecture of IoT-enabled Post Cloud Computing Model

Dew computing can be used in a variety of ways to enhance the present paradigms for computing [10]. Figure 2 illustrates the hierarchal organization of dew, edge, fog and cloud computing paradigm.

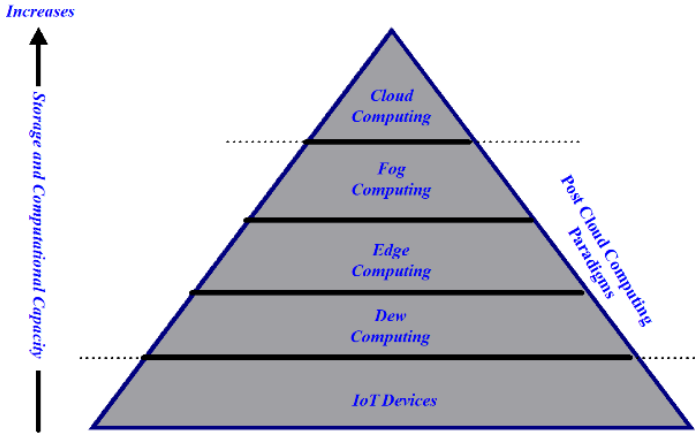

Figure 2. Hierarchical Arrangement of Post Cloud Comptuing Paradigms

Figure 2 shows that the processing is done at various levels in the hierarchy. The computational capacity and storage of post-cloud computing paradigms are decreased from top to bottom. The fog and edge computing paradigms are functioning well, when the internet connection is always available. When the internet is down, dew computing contributes by storing data locally for later processing. The attack surface will continue to expand as post-cloud computing brings services closer to IoT devices without requiring human intervention. Therefore, the robust security mechanism requires to dealt with the modern cryptographic threats. The most common security areas in post-cloud computing paradigms are illustrated in the Figure 3.

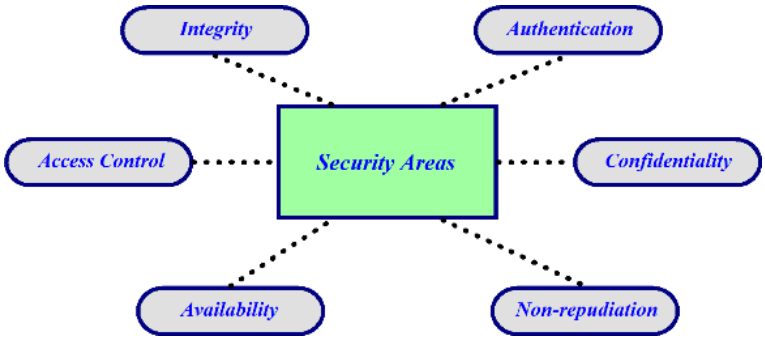

Figure 3. Security areas in Post-cloud computing enabled IoT application

The authentication is the supreme requirement out of the all core security areas [8]. The post-cloud computing paradigms are resource-constrained, and the IoT devices are closer to the computing paradigms. Therefore, the authentication mechanisms used in cloud computing cannot be used for the post-cloud computing model due to its resource-constrained networks. We therefore require a protocol that enables the formation of trustworthy sessions without relying on cloud server. An efficient authentication scheme is required for secure communication between post-cloud computing models and IoT devices. Table 1 shows the comparison between cloud computing and post-cloud computing models with respect to several parameters.

Table 1. Comparison between Dew computing and other computing paradigm

Parameters	***Post-cloud computing model***			***Cloud Computing***
	Dew Computing	***Edge Computing***	***Fog Computing***	
Network bandwidth	*Very low*	*Low*	*Low*	*High*
Communication latency	*Very low*	*Low*	*Low*	*High*
Energy consumption	*Very low*	*Low*	*Low*	*High*
Location cognizance	*Supported*	*Supported*	*Supported*	*Unsupported*
Real time processing	*Yes*	*Yes*	*Yes*	*No*
Motivated for IoT	*Yes*	*Yes*	*Yes*	*Yes*
Dependency on Internet connection	*No*	*Yes*	*Yes*	*Yes*

The rest of the paper is structured as follows:
Section 2 describes the background including challenges of IoT-Cloud model, features of post-cloud computing model and research motivation. The comparative analysis of authentication schemes for post-cloud computing-enabled IoT devices has presented in Section 3. The discussion of proposed

work is presented in Section 4. Lastly, Section 5 presents our conclusions.

2. Background

2.1 Challenges of Cloud enabled IoT paradigm

Cloud computing is a highly prospective technology that relies on virtualisation and distributed computing [9]. The cloud deployment approach enables the storage and retrieval of files to a distant server. The IoT-Cloud computing concept is a combination of cloud computing with IoT that offers a range of services to individuals such as smart healthcare, smart city and smart home. The IoT-Cloud paradigm uses cloud computing as an interface to access the services from the internet of things [10]. The Figure 4 depicts the IoT-Cloud computing paradigm.

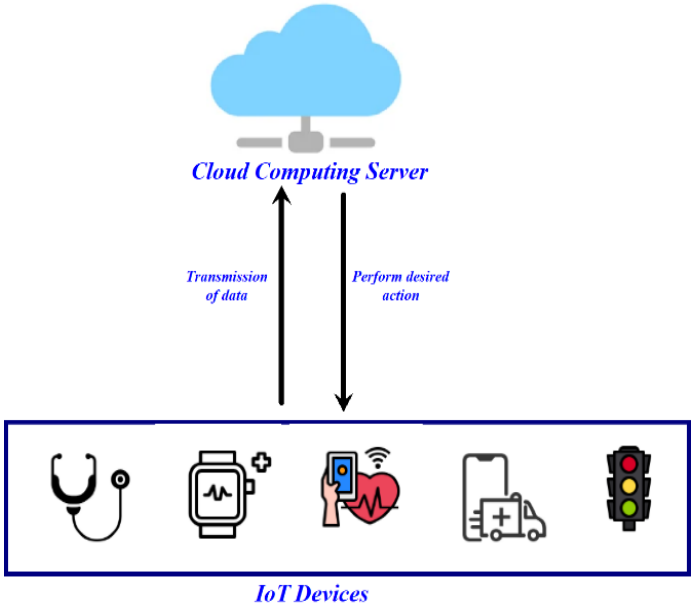

Figure 4. IoT-Cloud computing model

In IoT-cloud paradigm, the cost of transmission, network congestion, data processing, and end-to-end latency are all more affected by the physical distance between an IoT device and a cloud server. The IoT-Cloud paradigm has numerous critical issues for delay-sensitive IoT applications. Therefore, the ability of the IoT-Cloud paradigm is inadequate to control the necessities of delay-sensitive IoT applications [11].

2.2 Research Motivation

The IoT devices and post-cloud computing servers are resource-constrained, therefore they consumed minimal computational overhead as compared to resource-rich network entities. Due to resource constrained nature of server & device, heavyweight cryptographic solutions cannot feasible. Several authentication protocols have presented employing symmetric key cryptosystem, because in comparison to asymmetric key cryptosystem, symmetric key cryptosystem is computationally less expensive. The distribution of secret key or key management is a significant challenges of symmetric key cryptosystem. Asymmetric key cryptosystem solves the issue of symmetric key cryptosystems through the use of two keys i.e. public and private key. Many asymmetric key cryptosystems like Diffie-Hellman (DH) key agreement, Digital signature scheme (DSA), ECC, Rivest-Shamir-Adleman (RSA) etc. have been proposed to solve the problem of key distribution. RSA and ECC are most widely used asymmetric cryptosystem for authentication and key management [12-13].

Post-cloud computing paradigms are the resource constrained model as compared to cloud computing model. Therefore, lightweight cryptographic primitives such as ECC performs much better than RSA due to less bandwidth consumption & minimal energy, faster computational capability and smaller key size [14]. The mutual authentication and key agreement scheme in post-cloud computing enabled IoT devices has attract very miniature attention so far. Therefore, an ECC can also be adopted in dew-enabled IoT systems. In this article, ECC-based key agreement and authentication is propounded for IoT devices to securely access the amenities of dew server without access to internet. The designed protocol reduces the cryptographic attacks when IoT device connects to the dew server.

3. Literature Review

This section presented few of the recent authentication schemes for post-cloud computing enabled IoT networks. The comparative analysis of various authentication schemes is based on the certain criterias such as application domain and applied post-cloud computing model. The outcome of this comparative analysis gives the strengths and limitations of various authentication schemes in post-cloud computing-enabled IoT models. The comparative analysis of authentication schemes for post-cloud computing model is summarized in Table 2. The subsequent abbreviations are used in the Table 2.

+: Offers the security features/ resilience to cryptographic attacks

-: Does not offer the security features/vulnerable to cryptographic attacks

Model: Post-cloud computing model

AD: Application domain

Table 2. Comparative analysis of authentication schemes

Authentication schemes	***AD***	***Model***	***Strengths (+)***	***Limitations (-)***
Chen et al. [15], 2021	Smart Grid Networks	Edge computing	+Key agreement +User Anonymity +Replay attack	-GW spoofing attack -Password guessing attack -MITM attack
Braeken et al. [16], 2022	IoT Networks	Dew computing	+Replay attack +Impersonation attack +MITM attack +Password guessing attack	-Anonymity -Perfect forward secrecy -Session-key secrecy attack
Verma et al. [17], 2020	IoT networks	Fog computing	+Brute force attack +MITM attack +Replay attack	-Computation overhead -Communication overhead -Password guessing attack
Shahidinejad et al., [18], 2021	IoT-Cloud networks	Edge computing	+MITM attack +Eavesdropping +Disclosure attack +Anonymity	-Formal verification of protocol -Storage overhead -Computation overhead
Zhang et al. [19], 2020	Vehicular networks	Edge computing	+Mutual authentication +Replaying resistance	-User anonymity -Energy computation
Wazid et al. [20], 2019	Internet of Vehicles	Fog computing	+User anonymity +MITM attack +Impersonation attack +Replay attack	-Disclosure attack
Wu et al. [21], 2021	Vehicular ad hoc networks	Fog computing	+MITM attack +Untraceability +Replay attack	-Smart card loss attack
Ma et al. [22], 2022	IoT networks	Dew computing	+Anonymity +Location privacy +Replay attack +DoS attack	-Shared Key agreement -Malicious TTP
Abbas et al. [23], 2019	IoT-enabled applications	Fog computing	+Anonymity +Mutual authentication	-Higher computational cost
Ibrahim [24], 2016	Fog computing applications	Edge and Fog computing	+MITM attack +Replay attack +Forward secrecy	-User anonymity -Impersonation attack
Amor et al. [25], 2017	Fog computing applications	Edge and Fog computing	+Replay attack +User anonymity +MITM attack	-Fog server impersonation attack -Known key security -Forward secrecy
Jia et al. [26], 2019	Health care applications	Fog computing	+User anonymity +Replay attack +Impersonation attack +MITM attack	-Service aware authentication -Cloud offline authentication
Guo et al. [27], 2020	Fog computing applications	Fog computing	+Offline dictionary attack +Stolen verifier attack	-Anonymity -Untraceability -Forward secrecy
Wei et al. [28], 2021	VANET	Fog computing	+Offline dictionary attack	-Untraceability -Forward secrecy
				-Stolen verifier attack -Known session key attack -Anonymity -MITM attack
Chen et al. [29], 2021	Fog computing applications	Fog computing	+Offline dictionary attack +Stolen verifier attack	-Untraceability -Forward secrecy -Anonymity -MITM attack
Wazid et al. [30], 2019	Fog computing applications	Fog computing	+Offline dictionary attack	-Untraceability -Stolen verifier attack -Known session key attack -Anonymity -Forward secrecy
Liu et al. [31], 2024	Smart Grid Networks	Fog computing	+Replay attack +User anonymity +MITM attack +Session key attack	-Impersonation attack
Jin et al. [32], 2020	IoT networks	Edge computing	+Mutual authentication +Replay attack +User anonymity	-Impersonation attack -Internal threat exploitation
Rakeei et al. [33], 2022	Mobile applications	Edge computing	+Insider attack +PUF functionality	-MITM attack -Anonymity -Replay attack -DoS attack
Li et al. [34], 2020	Mobile application	Edge computing	+Insider attack +PUF functionality	-Anonymity -Replay attack -DoS attack -MITM attack
Braeken [35], 2022	IoT networks	Dew computing	+Perfect forward secrecy +Anonymity +Replay attack +Insider attack +Stolen device attack	-Common shared key

4. Discussion

This paper outlines the literature review of authentication schemes in the field of post-cloud computing model in the various fields such as VANET, IoT, smart grid, healthcare etc. The study of various authentication schemes helps researchers to identify the future research directions for developing a new authentication scheme in the domain of post-cloud computing model. The outcome of proposed work has been summarized below:

i. The lightweight cryptographic primitives such as ECC and hash function should be considered while implementing a new authentication scheme for post-cloud computing enabled IoT networks.

ii. The developed authentication schemes should be resilience to cryptographic attacks.

iii. The robustness of authentication scheme is validated by formal security verification tools such as AVISPA, Scyther etc.

iv. The informal security analysis should be taken into account while developing a new authentication schemes for post-cloud computing models.

v. The authentication schemes in post-cloud computing model should be efficient in terms of communication and storage overhead.

vi. The authentication schemes should preserve the privacy and anonymity in post-cloud computing model.

vii. The performance analysis in terms of computational complexity should be considered while developing the new authentication scheme in post-cloud computing enabled IoT networks.

5. Conclusions

This work provides a comprehensive and structured review of authentication schemes in post-cloud computing model. This paper examines the analysis of various authentication schemes for fog, edge, and dew computing in terms of strengths and limitations. This study provides the evolving security issues in post-cloud computing model and the challenges of the cloud computing model for delay-sensitive applications have been presented. The work shows the importance of post-cloud computing paradigms for delay sensitive IoT application. The discussion section of this research study is a step forward and helps the academician & researchers for the identification of research gaps in the field of authentication for post-cloud computing models.

References

1. Kim, Tai-hoon, Carlos Ramos, and Sabah Mohammed. "Smart city and IoT." Future Generation Computer Systems 76 (2017): 159-162.
2. Ghasempour, Alireza. "Internet of things in smart grid: Architecture, applications, services, key technologies, and challenges." Inventions 4.1 (2019): 22
3. Saarika, P. S., K. Sandhya, and T. Sudha. "Smart transportation system using IoT." 2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon). IEEE, 2017.
4. Farooq, Muhammad Shoaib, et al. "A survey on the role of industrial IOT in manufacturing for implementation of smart industry." Sensors 23.21 (2023): 8958.
5. Sabireen, H., and V. J. I. E. Neelanarayanan. "A review on fog computing: Architecture, fog with IoT, algorithms and research challenges." Ict Express 7.2 (2021): 162-176.
6. Yu, Wei, et al. "A survey on the edge computing for the Internet of Things." IEEE access 6 (2017): 6900-6919
7. Gushev, Marjan. "Dew computing architecture for cyber-physical systems and IoT." Internet of things 11 (2020): 100186
8. El-Hajj, Mohammed, et al. "A survey of internet of things (IoT) authentication schemes." Sensors 19.5 (2019): 1141.
9. Shukur, Hanan, et al. "Cloud computing virtualization of resources allocation for distributed systems." Journal of Applied Science and Technology Trends 1.2 (2020): 98-105
10. Babu, Shaik Masthan, A. Jaya Lakshmi, and B. Thirumala Rao. "A study on cloud based Internet of Things: CloudIoT." 2015 global conference on communication technologies (GCCT). IEEE, 2015
11. Avan, Amin, Akramul Azim, and Qusay H. Mahmoud. "A state-of-the-art review of task scheduling for edge computing: A delay-sensitive application perspective." Electronics 12.12 (2023): 2599
12. Yassein, Muneer Bani, et al. "Comprehensive study of symmetric key and asymmetric key encryption algorithms." 2017 international conference on engineering and technology (ICET). IEEE, 2017
13. Mahto, Dindayal, and Dilip Kumar Yadav. "RSA and ECC: A comparative analysis." International journal of applied engineering research 12.19 (2017): 9053-9061.
14. Suárez-Albela, Manuel, et al. "A practical performance comparison of ECC and RSA for resource-constrained IoT devices." 2018 Global Internet of Things Summit (GIoTS). IEEE, 2018
15. Chen, Chien-Ming, et al. "Lightweight authentication protocol in edge-based smart grid environment." EURASIP Journal on Wireless Communications and Networking 2021 (2021): 1-18.
16. Braeken, S., Obaidat, M.S., Mishra, D., Mishra, A., Rao, Y.S.: Efficient design of an authenticated key agreement protocol for dew-assisted IoT systems. The Journal of Supercomputing pp. 1–19 (2022).
17. Verma, Upendra, and Diwakar Bhardwaj. "Design of lightweight authentication protocol for fog enabled internet of things-a centralized authentication framework." Int. J. Commun. Netw. Inf. Secur 12 (2020): 162-167.
18. Shahidinejad, A., Ghobaei-Arani, M., Souri, A., Shojafar, M., & Kumari, S. (2021). Light-edge: Alightweight authentication protocol for IoT devices in an edge-cloud environment. IEEE consumer electronics magazine, 11(2), 57-63.
19. Zhang, J., Zhong, H., Cui, J., Tian, M., Xu, Y., & Liu, L. (2020). Edge computing-based privacy-preserving authentication framework and protocol for 5G-enabled vehicular networks. IEEE Transactions on Vehicular Technology, 69(7), 7940-7954.
20. M. Wazid, P. Bagga, A.K. Das, S. Shetty, J.J. Rodrigues, Y.H. Park, AKM-IoV: authenticated key management protocol in fog computing-based Internet of vehicles deployment, IEEE Int. Things J. 6 (5) (2019) 8804–8817.
21. T.-Y. Wu, Z. Lee, L. Yang, J.-N. Luo, and R. Tso, "Provably secure authentication key exchange scheme using fog nodes in vehicular ad hoc networks," 7e Journal of Supercomputing, vol. 77, no. 7, pp. 6992–7020, 2021.
22. Ma Y, Ma Y, Cheng Q. Cryptanalysis and enhancement of an authenticated key agreement protocol for dew-assisted IoT systems. Secur Commun Netw. 2022; 2022:1-11
23. Abbas N, Asim M, Tariq N, Baker T, Abbas S. A mechanism for securing IoT-enabled applications at the fog layer. J Sens Actuator Netw. 2019;8(1):16.
24. Ibrahim MH. Octopus: an edge-fog mutual authentication scheme. IJ Network Security 2016;18(6):1089–101
25. Amor AB, Abid M, Meddeb A. A privacy-preserving authentication scheme in an edge-fog environment. In: 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA). IEEE; 2017. p. 1225–31.
26. Jia X, He D, Kumar N, Choo K-KR. Authenticated key agreement scheme for fog-driven iot healthcare system. Wireless Networks 2019;25(8):4737–50.
27. Y. Guo, Z. Zhang, Y. Guo, Fog-centric authenticated key agreement scheme without trusted parties, IEEE Syst. J. 15 (4) (2020) 5057–5066.
28. L. Wei, J. Cui, H. Zhong, I. Bolodurina, L. Liu, A lightweight and conditional privacy-preserving authenticated key agreement scheme with multi-TA model for fog-based VANETs, IEEE Trans. Dependable Secure Comput. (2021).
29. C.-M. Chen, Y. Huang, K.-H. Wang, S. Kumari, M.-E. Wu, A secure authenticated and key exchange scheme for fog computing, Enterpr. Inf. Syst. 15 (9) (2021) 1200–1215.
30. M. Wazid, A.K. Das, N. Kumar, A.V. Vasilakos, Design of secure key management and user authentication scheme for fog computing services, Future Gener. Comput. Syst. 91 (2019) 475–492.
31. Liu J, Wang H, Bao J, Sun R, Du X, Guizani M. RPMDA: robust and privacy-enhanced multidimensional data aggregation scheme for fog-assisted smart grids. IEEE Internet Things J 2024. https://doi.org/10.1109/JIOT.2024.3352558.
32. Jin W, Xu R, You T, Hong Y-G, Kim D. Secure edge computing management based on independent microservices providers for gateway-centric IOT Networks. IEEE Access 2020; 8:187975 – 90.

33. M. Rakeei, F. Moazami, An efficient and provably secure authenticated key agreement scheme for mobile edge computing, Wirel. Netw. 28 (7) (2022) 2983–2999.
34. Li, Yuting, et al. "A secure anonymous identity-based scheme in new authentication architecture for mobile edge computing." IEEE Systems Journal 15.1 (2020): 935-946.
35. Braeken, An. "Authenticated key agreement protocols for dew-assisted IoT systems." The Journal of Supercomputing 78.10 (2022): 12093-12113.