Fog computing security and privacy issues, open challenges, and blockchain solution: An overview

Yehia Ibrahim Alzoubi, Ahmad Al-Ahmad, Ashraf Jaradat
Management Information Systems Department, College of Business Administration,
American University of the Middle East, Kuwait

Article Info

Article history:

Received Mar 27, 2020
Revised May 5, 2021
Accepted May 18, 2021

Keywords:

Application
Benefit
Fog computing
IoT
Security

ABSTRACT

Due to the expansion growth of the IoT devices, Fog computing was proposed to enhance the low latency IoT applications and meet the distribution nature of these devices. However, Fog computing was criticized for several privacy and security vulnerabilities. This paper aims to identify and discuss the security challenges for Fog computing. It also discusses blockchain technology as a complementary mechanism associated with Fog computing to mitigate the impact of these issues. The findings of this paper reveal that blockchain can meet the privacy and security requirements of fog computing; however, there are several limitations of blockchain that should be further investigated in the context of Fog computing.

Corresponding Author:

Ahmad Al-Ahmad
Management Information Systems Department College of Business Administration
American University of the Middle East, Kuwait
Email: ahmad.alahmad@aum.edu.kw

1. INTRODUCTION

IoT is a technology that is used in the interconnectivity of several types of physical devices with embedded software such as PDAs, smartphones, smart vehicles, smart meters, and sensors. On the other hand, Cloud computing is a technology that provides on-demand computing resources [1]. IoT devices depend on the Cloud to improve flexibility, system stability, fault tolerance, cost-effective, innovative business models, and better communications [2], [3]. Due to the expansion growth of the number of IoT devices [4], the Cloud has to deal with a massive amount of data that include confidential and sensitive data. Therefore, it requires security mechanisms to protect confidentiality, privacy, data integrity and to eliminate security threats. Likewise, Cloud computing architecture when used with IoT devices may suffer from a critical challenge related to delay-sensitive applications such as online games and emergency services which might be ruined when unexpected delays occur. Consequently, fog computing (FC) has been proposed to overcome these drawbacks of Cloud computing traditional drawbacks [5], [6].

FC is "an end-to-end horizontal architecture that distributes computing, storage, control, and networking functions closer to users along the Cloud-to-thing continuum" [7]. FC can help to address several security concerns related to Cloud and IoT generated data security. FC facilitates the on-site data storage and analysis of time-sensitive heterogeneous data by reducing the amount of confidential data stored and transmitted to the Cloud. Moreover, FC can help to mitigate latency issues, unavailability of location awareness, mobility support, and bandwidth obstacles [8], [9]. Approximately, 45% of IoT-generated data will use FC that can be installed within the close range of IoT sensors and devices for local processing and data storage [10], [11].

Despite the above-mentioned benefits, FC compromises several issues. These issues due to the distributed and homogeneous nature of FC, its extension of the Cloud which inherits several issues from the

Cloud, and its proximity to IoT devices [12]. The most challenging issues that have been reported in the literature were privacy and security issues. Fortunately, many studies have recently reported that security and privacy issues in FC can be mitigated by adopting the blockchain (BC) technology [13]-[16]. BC has originally used in Bitcoin; however, recently many applications have adopted BC to enhance privacy and security online transactions [17]. Accordingly, this research is conducted to improve the general understanding of the FC security challenges for future digital infrastructure and how BC can mitigate the effect of these challenges. Hence, this paper aims to answer the following research questions:

RQ1 : What are the security and privacy issues that face FC?

RQ2 : How BC can mitigate the impact of FC security and privacy issues?

The main contributions of this study are: i) identify and analyze the security challenges along with their existing solutions and respective limitations, ii) study the complementary relationship between BC and FC by exploring BC-based solutions to cater a Fog-enabled IoT's privacy and security concerns. The rest of this paper is organized as follows. Section 2 presents the background of FC. Section 3 discusses the state-of-the-art privacy and security challenges due to the use of FC. Section 4 discusses how BC can mitigate the open challenges of security and privacy in FC. Section 5 concludes this paper.

2. FOG COMPUTING BACKGROUND

Figure 1 provides a holistic view of the FC-IoT architecture. In this architecture, each IoT device can be connected to one Fog node through wired or wireless access media such as ZigBee and WiFi. Fog nodes communicate with each other through wireless or wired media as well. Virtualization technologies such as software-defined network and network functions virtualization are used to achieve network virtualization and traffic engineering [6], [18]. In this architecture, three layers can be identified; IoT device layer (i.e., end-user's devices such as smartphone, smartwatches, and so on), Fog layer (i.e., routers, switches, computers, and so on), and Cloud layer (i.e., the central storage and control devices and systems) [19]-[21].

A typical BC and smart contract implementation also illustrated in Figure 1. The data sent from IoT devices to the Fog node for data aggregation and further analysis [22]. Fog nodes enforce predefined security policies to manage connected IoT devices and services and also play an intermediate role of interaction between the Cloud and the public BC which enable indexing of authentication for data query [23]. The diagram explains real-time indexing, BC enabled authentication and secure data transfer. The data transferred is encrypted using an encryption algorithm such as AES and RSA which provides a short key establishment time and protects against network attacks [23]. In short, BC enables an indexing authentication approach that represents a scalable, decentralized, and protected data sharing in FC.

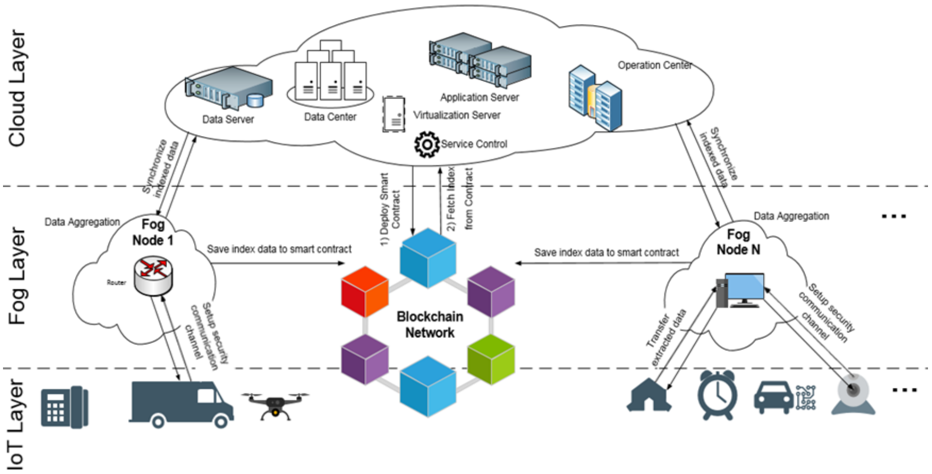

Figure 1. BC-fog architecture

3. SECURITY AND PRIVACY ISSUES OF FOG COMPUTING

Due to the nature of the FC of distribution, heterogeneity, closeness to IoT devices, and extension of Cloud computing many security and privacy issues were reported in the literature. This makes FC vulnerable to many attacks such as Man-in-the-Middle, Denial-of-Service, Rogue Fog Node, and Sybil attacks [24]. Some of these challenges have been provided some solutions as shown in Table 1.

Table 1. Summary of recommended solutions for some of security and privacy issues of FC

Issue	Recommendation
Access control	Several solutions were provided in the literature such as attribute-based encryption (ABE) access control [25], fine-grained access control [26], policy-driven management framework [27], leakage-resilient functional encryption schemes, device management, and key management [28], [29].
Packet Forwarding	It should be ensured that the features of the sent packet are maintained to guarantee the privacy of the packet sent between two Fog nodes or between Fog and IoT devices. End-to-end connectivity requires the cooperation of other nodes to enable message delivery and privacy-preserving packet forwarding should be used [28].
Virtualization	A lack of security countermeasures may result in enabling VM to manipulate the services of the Fog or taking control of the underlying operating system and hardware. Several solutions have been proposed such as implementing isolation policies, network abstraction, VM monitoring, multi-factor authentication, installation of detection systems at host and network, user-based permissions model, and hardening the hypervisor [25], [30], [31].
Fault Tolerance	Attackers may take control over or disable Fog nodes or the entire structure, due to misconfigurations, out-of-date software, weaknesses, and other faults. Therefore, participating in various policies and mechanisms as well as the deployment of a proactive fault-tolerance method is vital [25], [32].
Data Management	Data identification, aggregation, search, analysis, sharing, and distribution represent another issue for FC. Several mechanisms were proposed to ensure data integrity such as Trusted Platform Module (TPM), homomorphic encryption, one-way entrance permutation, key distribution, searchable, symmetric, and asymmetric encryption, data encryption schema used for single keyword search, and key-aggregate encryptions [6], [28], [33].
Light-weight Protocol Design	Lightweight protocols should support real-time service performance by reducing the communication between the IoT devices and Fog nodes. Various lightweight cryptographic schemes and techniques were anticipated to address this issue including elliptic curve cryptosystem [28], has functions, masking techniques, and stream chippers for secure end-to-end communication [6].
Malicious Fog Node	In order to avoid this issue, it was suggested to deploy fake node detection systems and trust-based routing mechanisms [6], creating and deleting virtual machine instances in a dynamic way complicates the process of maintaining a blacklist of rogue nodes [34].

The security and privacy solutions of FC proposed by literature oversimplified the real ecosystem nature of FC assuming FC as a single Cloud provider. FC compromises numerous cooperating service providers, services, and infrastructures related to diverse trust domains [35]. Therefore, state-of-the-art solutions are essential to encounter the security and privacy requirements for the FC. These solutions should ease the collaboration between different components in this complex environment. Table 2 summarizes the open questions and research challenges in this context.

Table 2. Open research challenges of security and privacy issues of FC

Issue	Open Research Challenges
Authentication	Since FC offers different services to a huge number of IoT devices, authentication should be applied at different levels during communication between Fog nodes and IoT devices [25]. In spite of the new authentication techniques that have been proposed such as identity, Decoy, anonymous, and cooperative, single-domain, cross-domain, and handover authentication [28], authentication represents one of the major worries in FC [4].
Detection Systems	Although several detection systems were proposed such as signature-based and neural network-based, fuzzy logic, lightweight countermeasure utilizing bloom filters, and distributed detection systems [23]-[25], there is a vital need for new systems that can integrate the different detection components which are distributed in the Fog network [24].
Trust Management	Trust, in FC, must be enabled by the Fog nodes. Moreover, Fog nodes that are delegated with data and processing requests by the IoT devices are mandatory to create consistent communications with the Fog nodes. This two-way challenge makes the creation of the trust a challenging task, despite several trust models that have been proposed such as trusted execution environment (TEE), region-based trust-aware (RBTA), and trusted distributed platform over the edge devices [25], [28].
Join/Leave Node	There is a vital need to create an authentication structure whenever an IoT device leaves one Fog node and join another or when a Fog node leaves the Fog layer. This structure should be of low complexity. Moreover, the system should be able to identify the misbehaved IoT device [24], [36].
Forensics	There is a big number of log records FC. This hardens the acquirement of the log data from Fog nodes [37]. Some proposed solutions were by keeping tracking of changes in data location among regions using mobility service (MS) and location register database (LRD) [25]. However, Fog forensics are questioned to some boundaries like the need for international regulation and application-level logging [38]. Furthermore, more resources and computational processing power to store trusted evidence in a distributed ecosystem with multiple trust domains [21].
Privacy Preservation	Comparing to Cloud computing, FC is more vulnerable than Cloud computing in terms of privacy risks (i.e., data, identity, location, and usage privacy). The vulnerability is observed due to the closeness of Fog nodes to the customer, which allows gathering more sensitive information from them and computing the customer data is outsourced to the Fog node, which might collect data from IoT services and relate them to the real identities of the clients [39]. Several solutions have been suggested in the literature to preserve the privacy of data in Fog environment like masking technique or lightweight encryption algorithms, Home-Area Network (HAN), identity obstruction techniques, differential and homomorphic techniques, identity-based and attribute-based encryptions, and proxy re-encryption [1], [40].

Several recommendations were provided in the literature to enhance security and privacy in the Fog environment [14], [17], [26], [38], [41]-[49]. i) Deliver the elementary services of access control, authentication, and authorization of all components involved in the Fog environment in order to establish secure communication channels, ii) Monitor the status of infrastructure using situational awareness mechanisms, iii) FC should provide privacy for both IoT devices and the service providers as these providers are part of the FC, iv) FC must provide digital evidence management (Forensics), v) BC technology can provide a high privacy and security for FC since it permits transparent and provable evidence, increases trust, and enhances data sharing decisions. Recently, many authors argued that BC can overcome many of the above privacy and security challenges. Their findings will be included in the following discussion.

4. BLOCKCHAIN SOLUTION

This section discusses how BC may help to mitigate the open research challenges of security and privacy issues of FC. Initially, BC technology originated in 2008 from a paper by Nakamoto [50] on bitcoin. BC is a chain of blocks that store a committed transaction by using a public ledger. It has emerged as a disruptive force, general-purpose technology for industries to support information exchange and transactions that require authentication and trust [51]. BC offers a decentralized shared database with transparent and immutable transaction records. It enables peer-to-peer transfer of digital assets without any intermediaries [6].

Some key characteristics, such as decentralization, persistency, anonymity, and auditability, are associated with BC technology [52]. BC persistency feature assures the ability to measure trust and offers producers and consumers the ability to prove their data are authentic. BC anonymity can help to prevent the producer's and consumer's identity [24]. BC decentralization nature of synchronized online registries can detect and prevent malicious actions [24]. Furthermore, BC compromises several core technologies, such as digital signatures, cryptographic hash, and distributed consensus algorithms that can significantly enhance security and privacy concerns [51].

Smart contracts in BC is an effective rules to authenticate the IoT devices which protect data privacy [51]. Furthermore, they are useful in detecting and preventing malicious actions. Providing unique guide and symmetric key pair to each IoT device connected to the BC network is another motivation to implement BC technology as it simplifies the utilization of security protocols [23]. BC provides secure communication among IoT devices and enables the verification of the device’s identity and ensures verified cryptography of the transactions [53].

Due to the above features, BC can be a useful technology to cater to the above-mentioned security and privacy issues in FC-IoT systems. It is in an easy, efficient, trustworthy, and secured manner [54]. BC ensures security, authentication, and integrity of transmitted data by IoT devices to be cryptographically proofed and assigned by the authentic sender. BC provides secure tracking of IoT device transactions easier [55].

As FC possesses a distributed computing environment, BC technology can offer good grounds for FC-enabled IoT systems to build and manage decentralized trust and security solutions [24]. BC can detect and isolate the malfunctioning node to protect the whole system from any security breach [6]. This provides self-healing capability to the Fog-enabled IoT systems. The security system equipped with BC-based security satisfies most of the requirements of Fog-enabled IoT systems by enhancing independent operation between all the connected nodes [55]. Table 3 (in appendix) summarizes how BC can enhance security and privacy in FC based on the latest literature.

5. CONCLUSION AND FUTURE DIRECTIONS

IoT devices are vulnerable to different security attacks due to the lack in hardware and software security designs. This paper discusses potential security and privacy challenges observed from Fog-enabled IoT literatures. It also discussed BC as an emerging security and privacy solution for Fog-enabled IoT domain. This paper, provides an overview of the open challenges of FC security and privacy issues. It also provides an overview of how BC can mitigate most of these challenges. The BC characteristics such as decentralization can provide a mechanism that enhance security, authentication, and integrity of data sent by IoT devices. It also ensures anonymity of the IoT devices.

Despite the above-mentioned characteristics and benefits of BC if used in FC, not all Fog applications are supported by all BC consensus mechanisms. For instance, proof of work (PoW) cannot be hosted on Fog devices as it demands enormous resources such as power and computing to execute transactions. Moreover, bitcoin BC poses response time latency in transaction validation process which make it not the best choice for real-time applications. In addition, due to the tremendous rate of growth in the number of IoT devices, BC in FC may face an issue in scalability. Therefore, more research is yet to be accompanied in this era. The findings of this paper guide academics and industries to investigate new answers to the open questions of the FC security and privacy issues.

APPENDIX

Table 3. Open research challenges of security and privacy issues of FC

Domain	BC Advantages
Security	Reduce security threats: BC can be used to create secured virtual zones that help in mitigating the effect and protecting the system against several threat attacks, such as cache poisoning, ARP spoofing, and denial of service attacks [56]. Well-structured: BC is based on a clear well-defined structure that takes into consideration all security aspects such as authentication, authorization, and data protection [57]. Enhance security: BC encrypt the data exchanged within the architecture, which in return enhances the security of the system [58]. Enhance IoT security: BC enrich the security in the IoT devices by overcoming the limitation of the devices when applying security policies [59]. Prevent from a single point of failure: Being decentralized made the BC architecture not having such a weak point as a single point of failure [56].
Preservation	Enhance Data integrity: BC protects efficiently the data from unintended and incomplete changes due to the solid trust verification process for any transaction types [60]. Protect users and device identity: BC protects the identity of the IoT devices by supporting anonymous communication methods [60] Enhance independency: BC reduce the need to have a third-party to verify entities or processes which minimizes the sharing of data with external bodies [58]. Enhance confidentiality: BC architecture enable the user to control his data in term of locations to save the entities to participate in the trust verification process [61]. Enhance authentication: BC uses immune verification and validation processes that make identity theft extremely difficult if not impossible [62].
Performance	Enhance performance: BC uses Software-Defined Networks (SDN), which may enhance certain functions in the applied architecture, such as authentication and logging [59]. Reduce delay: Distribution of processes in the BC will reduce the delay in delivering the required response from the system [63]. Reduce Overhead: Distribution of processes in the BC will reduce the overhead that were on a single machine [64].
Scalability	Scalability: BC doesn't have any restriction on the type of devices nor the process scenario. For instance, BC can be implemented using any IoT device, any Fog node structure, and any decentralized process [63].
Flexibility	Improve Flexibility: BC has different implementation models that go beyond the classical implementation. This will help BC in meeting various needs and requirements. For instance, security requirements can be fulfilled by using centralized and decentralized components in the architecture, for example, the use of a centralized ledger, instead of a centralized ledger, while using a distributed trust can help to solve satisfies certain security requests [53].
Efficiency	Enhance geographical data use: BC uses the geographical data to prove and verify the process and devices while keeping the geographical data protected [64]. Support concurrency: BC enables multiple processes to be executed at the same time, which in return will enhance the efficiency, power usage and reduce the resources needed [65].
Energy saving	Save energy: BC enhances the power usage efficiency as it distributes the tasks and reduces the overhead on the IoT devices [59].
Auditability	Enhance auditability: BC processes are transparent and logged in all the participants of the architecture [6].

REFERENCES

[1] P. Prakash, K. Darshaun, P. Yaazhlene, M. V. Ganesh, and B. Vasudha, "Fog Computing: Issues, Challenges and Future Directions," *International Journal of Electrical and Computer Engineering (IJECE),* vol. 7, no. 6, pp. 3669-3673, 2017, doi: 10.11591/ijece.v7i6.pp3669-3673.

[2] A. Yassine, S. Singh, M. S. Hossain, and G. Muhammad, "IoT big data analytics for smart homes with fog and cloud computing," *Future Generation Computer Systems,* vol. 91, pp. 563-573, 2019, doi: 10.1016/j.future.2018.08.040.

[3] R. Iqbal, T. A. Butt, M. Afzaal, and K. Salah, "Trust management in social Internet of vehicles: Factors, challenges, blockchain, and fog solutions," *International Journal of Distributed Sensor Networks*, vol. 15, no. 1, 2018, doi: 10.1177/1550147719825820.

[4] Y. I. Alzoubi, A. Al-Ahmad, A. Jaradat, and V. H. Osmanaj, "Fog Computing Architecture, Benefits, Security, and Privacy, for the Internet of Thing Applications: An Overview," *Journal of Theoretical and Applied Information Technology*, vol. 99, no. 2, pp. 436-451, 2021, doi: 10.1002/spy2.145.

[5] Z. Ashi, M. Al-Fawa'reh, and M. Al-Fayoumi, "Fog Computing: Security Challenges and Countermeasures," *International Journal of Computer Applications,* vol. 175, no. 15, pp. 30-36, 2020, doi: 10.5120/ijca2020920648.

[6] N. Tariq *et al.*, "The security of big data in fog-enabled IoT applications including blockchain: A survey," *Sensors*, vol. 19, no. 8, 2019, Art. no. 1788, doi: 10.3390/s19081788.

[7] M. Chiang, S. Ha, I. Chih-Lin, F. Risso, and T. Zhang, "Clarifying fog computing and networking: 10 questions and answers," *IEEE Communications Magazine,* vol. 55, no. 4, pp. 18-20, 2017, doi: 10.1109/MCOM.2017.7901470.

[8] C. Rupa, R. Patan, F. Al-Turjman, and L. Mostarda, "Enhancing the Access Privacy of IDaaS System Using SAML Protocol in Fog Computing," *IEEE Access,* vol. 8, pp. 168793-168801, 2020, doi: 10.1109/ACCESS.2020.3022957.

[9] P. Hu, H. Ning, T. Qiu, H. Song, Y. Wang, and X. Yao, "Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things," I*EEE Internet of Things Journal,* vol. 4, no. 5, pp. 1143-1155, 2017, doi: 10.1109/JIOT.2017.2659783.

[10] X. Shen, L. Zhu, C. Xu, K. Sharif, and R. Lu, "A privacy-preserving data aggregation scheme for dynamic groups in fog computing," *Information Sciences*, vol. 514, pp. 118-130, 2020, doi: 10.1016/j.ins.2019.12.007.

[11] R. Neware and U. Shrawankar, "Fog Computing Architecture, Applications and Security Issues," *International Journal of Fog Computing (IJFC),* vol. 3, no. 1, pp. 75-105, 2020, doi: 10.20944/preprints201903.0145.v1.

[12] Z. Chen, H. Cui, E. Wu, Y. Li, and Y. Xi, "Secure Distributed Data Management for Fog Computing in Large-Scale IoT Application: A Blockchain-Based Solution," *IEEE International Conference on Communications Workshops (ICC Workshops),* 2020, pp. 1-6, doi: 10.1109/ICCWorkshops49005.2020.9145381.

[13] H. Elazhary, "Internet of Things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: Disambiguation and research directions," *Journal of network and computer applications, v*ol. 128, pp. 105-140, 2019, doi: 10.1016/j.jnca.2018.10.021.

[14] S. Nadeem, M. Rizwan, F. Ahmad, and J. Manzoor, "Securing cognitive radio vehicular ad hoc network with fog node based distributed blockchain cloud architecture," *International Journal of Advanced Computer Science and Application*s, vol. 10, no. 1, pp. 288-295, 2019, doi: 10.14569/IJACSA.2019.0100138.

[15] A. S. Al-Ahmad, S. A. Aljunid, and N. K. Ismail, "Mobile cloud computing applications penetration testing model design," *International Journal of Information and Computer Security,* vol. 13, no. 2, pp. 210-226, 2020, doi: 10.1504/IJICS.2020.108849.

[16] A. S. Al-Ahmad and H. Kahtan, "Cloud Computing Review: Features And Issues," *2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, 2018, pp. 1-5, doi: 10.1109/ICSCEE.2018.8538387.

[17] B. K. Mohanta, D. Jena, S. S. Panda, and S. Sobhanayak, "Blockchain technology: A survey on applications and security privacy challenges," *Internet of Things*, vol. 8, 2019, Art. no. 100107, doi: 10.1016/j.iot.2019.100107.

[18] P. Habibi, M. Farhoudi, S. Kazemian, S. Khorsandi, and A. Leon-Garcia, "Fog Computing: A Comprehensive Architectural Survey," *IEEE Access*, vol. 8, pp. 69105-69133, 2020, doi: 10.1109/ACCESS.2020.2983253.

[19] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, "A comprehensive survey on fog computing: State-of-the-art and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 416-464, 2017, doi: 10.1109/COMST.2017.2771153.

[20] F. Haouari, R. Faraj, and J. M. AlJa'am, "Fog Computing Potentials, Applications, and Challenges," *2018 International Conference on Computer and Applications (ICCA)*, 2018, pp. 399-406, doi: 10.1109/COMAPP.2018.8460182.

[21] Y. I. Alzoubi, V. H. Osmanaj, A. Jaradat, and A. Al-Ahmad, "Fog computing security andprivacy for the Internet of Thing applications: State-of-the-art," *Security and Privacy*, vol. 4, no. 2, pp. 1-26, 2020, Art. no. e145, doi: 10.1002/spy2.145.

[22] A. A.-N. Patwary, A. Fu, S. K. Battula, R. K. Naha, S. Garg, and A. Mahanti, "FogAuthChain: A secure location-based authentication scheme in fog computing environments using Blockchain," *Computer Communications,* vol. 162, pp. 212-224, 2020, doi: 10.1016/j.comcom.2020.08.021.

[23] P. Singh, A. Nayyar, A. Kaur, and U. Ghosh, "Blockchain and Fog Based Architecture for Internet of Everything in Smart Cities," *Future Internet,* vol. 12, no 4, 2020, Art. no. 61, doi: /10.3390/fi12040061.

[24] N. S. Khan and M. A. Chishti, "Security Challenges in Fog and IoT, Blockchain Technology and Cell Tree Solutions: A Review," *Scalable Computing: Practice and Experience*, vol. 21, no. 3, pp. 515-542, 2020, DOI:10.12694/scpe.v21i3.1782

[25] R. Roman *et al.*, "A survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, pp. 680-698, 2018, doi: 10.1016/j.future.2016.11.009.

[26] A. Muthanna *et al.,* "Secure and reliable IoT networks using fog computing with software-defined networking and blockchain," *Journal of Sensor and Actuator Networks,* vol. 8, no. 1, 2019, Art. no. 15, doi: /10.3390/jsan8010015.

[27] R. Guo, C. Zhuang, H. Shi, Y. Zhang, and D. Zheng, "A lightweight verifiable outsourced decryption of attribute-based encryption scheme for blockchain-enabled wireless body area network in fog computing," *International Journal of Distributed Sensor Networks,* vol. 16, 2020, doi: 10.1177/1550147720906796.

[28] J. Ni, K. Zhang, X. Lin, and X. S. Shen, "Securing fog computing for internet of things applications: Challenges and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 601-628, 2017, doi: 10.1109/COMST.2017.2762345.

[29] A. Yousefpour *et al.,* "All one needs to know about fog computing and related edge computing paradigms: A complete survey," *Journal of Systems Architecture*, vol. 98, pp. 289-330, 2019, doi: 10.1016/j.sysarc.2019.02.009.

[30] B. Z. Abbasi and M. A. Shah, "Fog computing: Security issues, solutions and robust practices*," 2017 23rd International Conference on Automation and Computing (ICAC),* 2017, pp. 1-6, doi: 10.23919/IConAC.2017.8082079.

[31] S. Khan, S. Parkinson, and Y. Qin, "Fog computing security: a review of current applications and security solutions," *Journal of Cloud Computing*, vol. 6, 2017, Art. no. 90, doi: 10.1186/s13677-017-0090-3.

[32] R. K. Naha *et al.,* "Fog Computing: Survey of trends, architectures, requirements, and research directions," *IEEE access,* vol. 6, pp. 47980-48009, 2018, doi: 10.1109/ACCESS.2018.2866491.

[33] Y. Guan, J. Shao, G. Wei, and M. Xie, "Data security and privacy in fog computing," *IEEE Network*, vol. 32, pp. 106-111, 2018, doi: 10.1109/MNET.2018.1700250.

[34] H. Tian, F. Nan, C.-C. Chang, Y. Huang, J. Lu, and Y. Du, "Privacy-preserving public auditing for secure data storage in fog-to-cloud computing," *Journal of Network and Computer Applications*, vol. 127, pp. 59-69, 2019, doi: 10.1016/j.jnca.2018.12.004.

[35] M. Mukherjee, M. A. Ferrag, L. Maglaras, A. Derhab, and M. Aazam, "Security and privacy issues and solutions for fog," *Fog and Fogonomics: Challenges and Practices of Fog Computing, Communication, Networking, Strategy, and Economics*, pp. 353-374, 2020.

[36] A. K. Alhwaitat, S. Manaseer, and M. Alsyyed, "A survey of digital forensic methods under advanced persistent threat in fog computing environment," *Journal of Theoretical and Applied Information Technology*, vol. 97, no. 18, pp. 4934-4954, 2019.

[37] Y. Wang, T. Uehara, and R. Sasaki, "Fog computing: Issues and challenges in security and forensics," *2015 IEEE 39th Annual Computer Software and Applications Conference,* 2015, pp. 53-59, doi: 10.1109/COMPSAC.2015.173.

[38] M. Mukherjee *et al*., "Security and privacy in fog computing: Challenges," *IEEE Access*, vol. 5, pp. 19293-19304, 2017, doi: 10.1109/ACCESS.2017.2749422.

[39] N. Abubaker, L. Dervishi, and E. Ayday, "Privacy-preserving fog computing paradigm," *2017 IEEE Conference on Communications and Network Security (CNS),* 2017, pp. 502-509, doi: 10.1109/CNS.2017.8228709.

[40] S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: A survey," *International conference on wireless algorithms, systems, and applications,* 2015, pp. 685-695, doi: 10.1007/978-3-319-21837-3_67.

[41] R. Rios, R. Roman, J. A. Onieva, and J. Lopez, "From SMOG to Fog: a security perspective," *2017 Second International Conference on Fog and Mobile Edge Computing (FMEC),* 2017, pp. 56-61, doi: 10.1109/FMEC.2017.7946408.

[42] S. Tuli, R. Mahmud, S. Tuli, and R. Buyya, "Fogbus: A blockchain-based lightweight framework for edge and fog computing," *Journal of Systems and Software*, vol. 154, pp. 22-36, 2019, doi: 10.1016/j.jss.2019.04.050.

[43] S.-H. Jang, J. Guejong, J. Jeong, and B. Sangmin, "Fog computing architecture based blockchain for industrial IoT," *International Conference on Computational Science*, vol. 11538, 2019, pp. 593-606.

[44] H. L. Cech, M. Großmann, and U. R. Krieger, "A fog computing architecture to share sensor data by means of blockchain functionality," *2019 IEEE International Conference on Fog Computing (ICFC),* 2019, pp. 31-40, doi: 10.1109/ICFC.2019.00013.

[45] K. Lei, M. Du, J. Huang, and T. Jin, "Groupchain: Towards a Scalable Public Blockchain in Fog Computing of IoT Services Computing," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 252-262, 2020, doi: 10.1109/TSC.2019.2949801.

[46] X. Huang, D. Ye, R. Yu, and L. Shu, "Securing parked vehicle assisted fog computing with blockchain and optimal smart contract design," *IEEE/CAA Journal of Automatica Sinica,* vol. 7, no. 2, pp. 426-441, 2020, doi: 10.1109/JAS.2020.1003039.

[47] N. Islam, Y. Faheem, I. U. Din, M. Talha, M. Guizani, and M. Khalil, "A blockchain-based fog computing framework for activity recognition as an application to e-Healthcare services," *Future Generation Computer Systems,* vol. 100, pp. 569-578, 2019, doi: 10.1016/j.future.2019.05.059.

[48] J. Yang, Z. Lu, and J. Wu, "Smart-toy-edge-computing-oriented data exchange based on blockchain," *Journal of Systems Architecture,* vol. 87, pp. 36-48, 2018, doi: 10.1016/j.sysarc.2018.05.001.

[49] A. Bonadio, F. Chiti, R. Fantacci, and V. Vespri, "An integrated framework for blockchain inspired fog communications and computing in internet of vehicles," *Journal of Ambient Intelligence and Humanized Computing,* vol. 11, pp. 755-762, 2020.

[50] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[51] O. Ali, A. Jaradat, AtikKulaki, and A. Abuhalimeh, "A comparative study: Blockchain technology utilization benefits, challenges and functionalities," *IEEE Access,* vol. 9, pp. 12730-12749, 2021, doi: 10.1109/ACCESS.2021.3050241.

[52] H. Baniata and A. Kertesz, "A Survey on Blockchain-Fog Integration Approaches," *IEEE Access*, vol. 8, pp. 102657-102668, 2020, doi: 10.1109/ACCESS.2020.2999213.

[53] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, "Blockchain for the IoT and industrial IoT: A review," *Internet of Things*, vol. 10, 2020, Art. no. 100081, doi: 10.1016/j.iot.2019.100081.

[54] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the internet of things: Research issues and challenges," *IEEE Internet of Things Journal,* vol. 6, no. 2, pp. 2188-2204, 2018, doi: 10.1109/JIOT.2018.2882794.

[55] T. Alam, "Design a blockchain-based middleware layer in the Internet of Things Architecture," *JOIV: International Journal on Informatics Visualization*, vol. 4, no. 1, pp. 28-31, 2020, doi: 10.30630/joiv.4.1.334.

[56] J. Sengupta, S. Ruj, and S. D. Bit, "A Comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *Journal of Network and Computer Applications,* vol. 149, 2020, Art. no. 102481, doi: 10.1016/j.jnca.2019.102481.

[57] S. El Kafhali, C. Chahir, M. Hanini, and K. Salah, "Architecture to manage Internet of Things data using blockchain and fog computing," *Proceedings of the 4th International Conference on Big Data and Internet of Things,* 2019, pp. 1-8, Art. no. 32, doi: 10.1145/3372938.3372970.

[58] Y. Ma, Y. Sun, Y. Lei, N. Qin, and J. Lu, "A survey of blockchain technology on security, privacy, and trust in crowdsourcing services," *World Wide Web,* vol. 23, no. 2, pp. 393-419, 2020, doi: 10.1007/s11280-019-00735-4.

[59] S. Misra, P. K. Deb, N. Pathak, and A. Mukherjee, "Blockchain-Enabled SDN for Securing Fog-Based Resource-Constrained IoT," *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS),* 2020, pp. 490-495, doi: 10.1109/INFOCOMWKSHPS50562.2020.9162706.

[60] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "Blockchain leveraged decentralized IoT eHealth framework," *Internet of Things,* vol. 9, 2020, Art. no. 100159, doi: 10.1016/j.iot.2020.100159.

[61] Q. Kong, L. Su, and M. Ma, "Achieving Privacy-Preserving and Verifiable Data Sharing in Vehicular Fog With Blockchain," *IEEE Transactions on Intelligent Transportation Systems,* 2020, pp. 1-10, doi: 10.1109/TITS.2020.2983466.

[62] O. Mounnan, A. El Mouatasim, O. Manad, T. Hidar, A. Abou El Kalam, and N. Idboufker, "Privacy-Aware and Authentication based on Blockchain with Fault Tolerance for IoT enabled Fog Computing," *Fifth International*

Conference on Fog and Mobile Edge Computing (FMEC), 2020, pp. 347-352, doi: 10.1109/FMEC49853.2020.9144845.

[63] L. Yang, M. Li, H. Zhang, H. Ji, M. Xiao, and X. Li, "Distributed Resource Management for Blockchain in Fog-enabled IoT Networks," *IEEE Internet of Things Journal,* vol. 8, no. 4, pp. 2330-2341, 2020, doi: 10.1109/JIOT.2020.3028071.

[64] N. C. Luong, Y. Jiao, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "A Machine-Learning-Based Auction for Resource Trading in Fog Computing," *IEEE Communications Magazine*, vol. 58, no. 3, pp. 82-88, 2020, doi: 10.1109/MCOM.001.1900136.

[65] M. Savi *et al.,* "A blockchain-based brokerage platform for fog computing resource federation," *23rd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, 2020, pp. 147-149, doi: 10.1109/ICIN48450.2020.9059337.