Engineering and Technology Journal e-ISSN: 2456-3358

Volume 11 Issue 02 February-2026, Page No.-8821-8826

DOI: 10.47191/etj/v11i02.04, I.F. – 8.482

© 2026, ETJ

Edge Computing-Assisted Internet of Things: A Blockchain-Based Approach to Security and Privacy Concerns

Dr. Priyanka

Assistant Professor, Ch. Bansilal University, Bhiwani, Haryana

ABSTRACT: The Internet of Things (IoT) is a cutting-edge paradigm that has become a part of our everyday lives and has the potential to offer enormous applications. Millions of smart devices are installed within intricate networks to provide vibrant features like communications, monitoring, and control of vital infrastructures. The state-of-the-art centralized cloud computing paradigm was further burdened by the rapid proliferation of IoT devices and the massive data traffic generated at the network edge because of the scarce resources and bandwidth. To be more precise, we begin by giving a general review of EC-assisted IoT, including definitions, uses, architecture, benefits, and difficulties. Secondly, we describe privacy and security in the context of IoT with EC assistance. After that, we go into great detail on the main categories of threats in EC-assisted IoT and offer potential fixes and defenses in addition to the relevant research initiatives. Next, we further categorize a few security and privacy concerns that have been covered in the literature according to security services as well as security goals and roles. In the end, we discussed Blockchain for Edge-of-things and its solutions that help to provide security and privacy in Edge-computing-assisted Internet of Things. The integration of edge computing with the Internet of Things (IoT) has made possible the Edge-of-Things (EoT), one of the many application domains where blockchain is gaining traction as a viable technology. There is also an exploration of BEoT's ability to provide security services, such as trust management, attack detection, data privacy preservation, and access authentication. In conclusion, some unresolved issues and prospective avenues for investigation concerning the secure EC-assisted Internet of Things paradigm are also covered in detail.

KEYWORDS: Blockchain, Cryptocurrency, Secure Transactions, Distributed Ledger, Digital Signatures, Smart Contracts, Cryptography, Decentralization.

1. INTRODUCTION

The term "Internet of Things" (IoT) describes a group of objects, including smart devices, sensors, actuators, or anything else having electronics incorporated in it, that are connected to the Internet to transmit, store, and receive data pertinent to a certain service or application [1], [2]. The rapid advancement of information technology makes it possible for IoT to facilitate and accelerate the introduction of fresh, creative services and applications. Additionally, IoT smart devices are constantly being updated with more complicated and powerful sensing, computation, and processing power capabilities, enabling their deployment in a variety of challenging contexts. Common IoT services and applications used in several important areas are depicted in the Figure. (1). By 2020, there will be more than 200 billion connectable IoT smart devices and sensors, including wearable technology, smart home appliances, smartphones, tablets, and more, with 30 billion of them having an Internet connection,

Figure 1: Applications of IoT. (a) smart buildings, (b) smart vehicles, (c) energy management, (d) health monitoring, (e) food supply chain, (f) construction management, (g) environmental monitoring, (h) production management, and (I) wearable devices.

according to a report from the International Data Corporation (IDC) [3], [4]. According to a Cisco Global Cloud Index (GCI) assessment, by 2020, sensors and other devices will generate and gather an enormous amount of data from the environment, surpassing 500 Zettabytes (ZB) [5].

2. PURPOSE OF THE STUDY

- **Research Gaps**

  Issues, including latency, inefficient bandwidth utilization, and security flaws, plague current Internet of Things (IoT) infrastructures, which primarily rely on centralized cloud computing. Cloud computing struggles to match the real-time processing and privacy requirements of modern IoT systems, while offering substantial computational and storage capabilities. Additionally, few comprehensive frameworks integrate blockchain with edge computing while simultaneously meeting the requirements of security, privacy, and low latency.

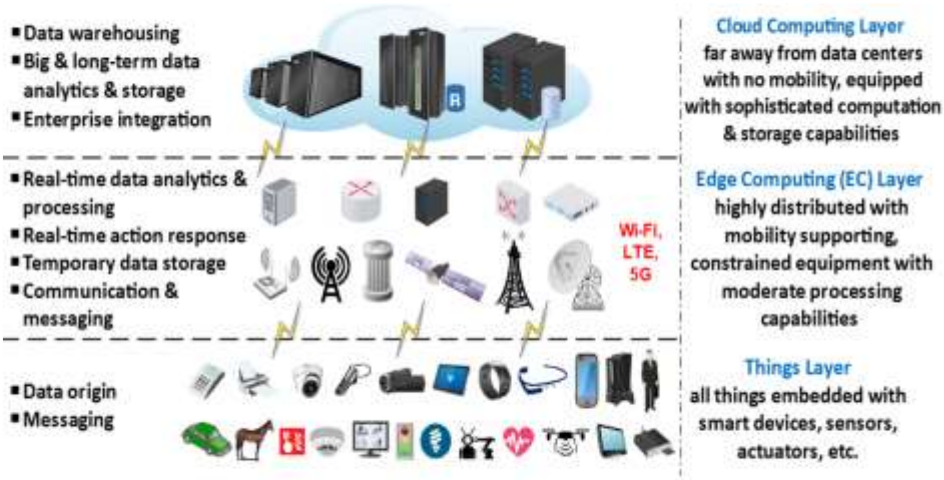

Figure 2: Standard layer architecture of EC-assisted IoT

- **Research Problem**

  How can the combination of blockchain and edge computing be successfully used to improve efficiency, security, and confidentiality in IoT networks handling large amounts of sensitive, dispersed data?

- **Objective and Contribution**

  This article addresses the Internet of Things (IoT) with Edge Computing as a blockchain-based solution to security and privacy issues. It covers the definition of security and privacy, its benefits and drawbacks, solutions and defenses, and the blockchain for the edge of things.

  The paper's contributions are as follows:

  - In-depth layer-by-layer security problems have been uncovered in the Internet of Things system.
  - The IoT architecture and its enabling technology were described in the article along with certain difficulties.
  - A thorough investigation is conducted into related technologies, such as blockchain technology integration with IoT security, machine learning, and artificial intelligence.
  - The research difficulties and the accompanying solution method using upcoming technologies (ML, AI, Blockchain) are also explained.

3. RESEARCH METHODOLOGY

The study examines contemporary technologies, architectures, and mechanisms from scholarly and commercial research using a methodical literature review and analytical approach. It comprises a layer-by-layer assessment of IoT architectures to find vulnerabilities, a comparative analysis of IoT security threats and privacy frameworks, and a categorization of solutions according to security functions such as authentication, encryption, trust modeling, and access control. Additionally, within edge computing paradigms, integration analysis of blockchain features like immutability, decentralization, and traceability is carried out. The study summarizes current knowledge and arranges it into conceptual models that illustrate how blockchain might improve edge computing platforms for the Internet of Things.

4. IOT INFRASTRUCTURE, PROTOCOLS, AND APPLICATIONS

4.1 IoT Infrastructure: Various smart objects that gather, process, compute, and interact with other smart objects make up an Internet of Things application. The three layers of IoT are the application, network, and physical layers. Many intelligently integrated items have been developed in recent sectors. According to Figure 3 [11],[12]. In addition to sensors, the Internet-of-Things architecture incorporates some new technologies. On either IoT-Cloud or IoT-Fog-Cloud, the IoT application is built. Effective IoT applications need to address security issues such as data privacy [17], machine-to-machine communication [18], real-time monitoring [19], and an IoT testbed. IoT architecture can be a distributed, decentralized structure.

4.2. Application: Many different fields are now developing IoT applications. development of numerous open-source platforms, such as the cloud-based IoTIFY platform for creating scalable IoT applications, the Bevywise IoT platform for industrial IoT, Oracle IoT, Amazon Web Services (AWS), IBM Watson, Azure IoT Suite, and Kaa. AI and ML technologies are used in the majority of open-source platforms to process and compute information intelligently.

4.2.1 Smart Retail: Along with artificial intelligence, the retail industry is also utilizing IoT services to boost productivity, optimize shop operations, and make real-time decisions on inventory system management.

4.2.2. Smart Home: An intelligent home system is created by the Internet of Things. Smart TVs, security cameras, gas and temperature sensors, light systems, and refrigerators can all sense their surroundings, interact, and connect to the internet via wired or wireless connections.

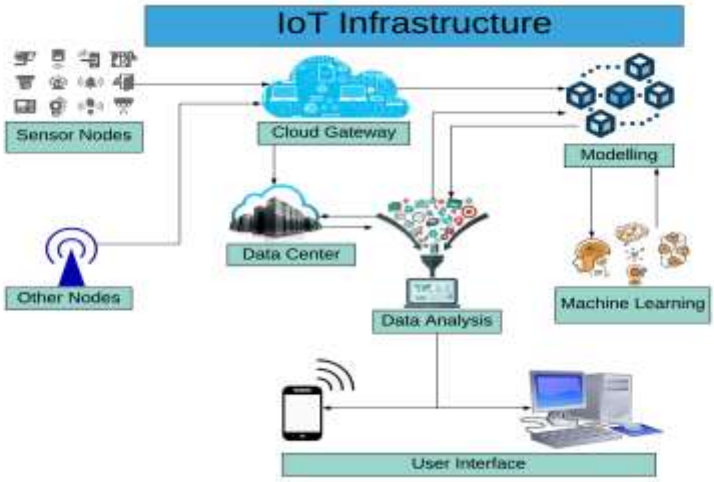

Figure: 3 IoT Infrastructure

The refrigerator itself is capable of placing an order with the authorized retail store and notifying the user. With the advancement of smart devices, the quality of life has improved. An IoT-based smart home system is designed by the authors in the study. The home was transformed into an intelligent home system using technologies like IoT and fog computing, which allow for immediate processing and remote home monitoring. Device authentication is crucial for blocking unauthorized access to the Internet of Things network. Different authentication methods for a smart home network were suggested by the authors in [21] and [20]. However, there are still certain security flaws in IoT-based smart home systems.

4.2.3. Smart City: Traffic, garbage, and environmental management are just a few of the issues facing the ever-expanding city. The city needs a way to keep an eye on and manage the issue. In publications [24] and [25], writers detailed the difficulties in establishing smart cities and conducted a thorough assessment on how IoT may address an issue that already exists. IoT and related technologies can be used to create a smart city that raises the standard of living while protecting citizens' privacy and security.

4.2.4. Smart Hospital: An IoT-cloud-based architecture for data gathering in the healthcare system has been presented by the authors of the research [22], since sensors and fog/edge computing can be used to construct IoT patient monitoring in real-time. Likewise, the authors of [23] carried out the authorization and authentication of the smart devices within the healthcare system. Since one of the primary concerns in the healthcare system is privacy, appropriate security, and privacy protocols must be created to safeguard the system.

4.3. Standard Protocol

The Internet of Things (IoT) architecture is typically divided into four main layers, each with its own set of protocols and use cases:

1. Perception Layer (Device Layer):

Protocols: Zigbee, Z-Wave, Bluetooth Low Energy (BLE), 6LoWPAN.

Use Cases: Sensor data collection, actuator control, device-to-device communication.

2. Network Layer:

Protocols: Wi-Fi, Cellular (3G, 4G, 5G), LoRaWAN, NB-IoT.

Use Cases: Data transmission, network connectivity, gateway communication.

3. Application Layer:

Protocols: HTTP, MQTT, CoAP, REST.

Use Cases: Data processing, cloud integration, data analytics, and application services.

4. Business Layer:

Protocols: REST API, SOAP.

Use Cases: Decision-making, business intelligence, integration with enterprise systems.

5. EDGE COMPUTING ASSISTED IOT

This section provides an overview of the core ideas, uses, and architecture of the integrated IoT and EC paradigm. IoT experts are pushing for the integration of EC and IoT paradigms to support critical IoT applications that require enhanced QoS described in Figure 1. Figure 2 depicts the standard three-layer architecture of the EC-assisted IoT paradigm. It comprises the same layers of the conventional EC structure, where all IoT "things" (i.e., devices and sensors) are considered end users for EC.

The EC layer is absent from traditional IoT architectures. The "Core Networks" intermediary layer sits between the Cloud layer and the EC layer in the traditional EC architecture. Fog computing (FC) architecture is another standard that makes it possible to extend cloud computing capabilities to network edges. Though the EC and FC architectures closely overlap [33], FC is more concerned with the network infrastructure layer, whereas EC is more concerned with the things layer [34]. More specifically, FC makes the EC concept repeatable so that network developers can transmit computation power from the cloud computing layer to the EC servers for a reliable and scalable performance [30]- [32].

5.1 Definition of Security and Privacy in the Context of Edge Computing Assisted IoT

As we've already discussed, at the periphery of IoT networks, EC-assisted IoT systems handle enormous volumes of data. According to the Figure. (1) This type of information is associated with a variety of vertical IoT industries' low-to-high-sensitive applications and services. When EC-assisted IoT systems are implemented conventionally (see Figure 2), wired and/or wireless communications are used to transfer data between end devices and EC nodes [7]-[9]. In contrast, public or private networks are used for data transmission from EC nodes to the cloud system [13]. Regrettably, the lack of adequate security measures in these EC-assisted system implementations leaves them open to serious security and privacy risks. Numerous studies have examined these kinds of risks. The problems of data processing in mobile EC about security, privacy, and efficiency are examined by the writers in [26]. Also covered are the chances to increase computational efficiency and safeguard data privacy while utilizing EC to support these goals. In their work, they provide safe computational offloading and secure data duplication and aggregation as solutions. The security protocols, risks, and difficulties associated with certain EC paradigms are examined in [30]. The potential for improving certain important security and privacy issues in automotive networks—particularly in revocation and authentication issues—is discussed by the authors in [6] in light of the appealing features and benefits of EC models.

5.2 Advantages of Edge Computing Assisted IoT

Assisting the IoT with EC offers various notable benefits that fall into three primary areas:

1) Communication: IoT networks with EC assistance have improved network performance in terms of lower packet data overhead, lower device power consumption, lower bandwidth utilization, and lower latency (both communication and computation) [25], [31]. As a result, the communication performance of the network as a whole is greatly enhanced, allowing it to meet the quality of service (QoS) demands of the time-sensitive Internet of Things applications and services.

2) Computation: Data processing and computing will be moved to the edge servers in EC-assisted IoT networks, relieving a significant strain from the centralized cloud servers. In terms of resource usage and priority control, this ensures improved network efficiency [28].

3) Storage: EC servers offer storage services to the Internet of Things end devices, as these devices typically have limited storage capacity. By moving every piece of data, the devices produce or gather to storage servers, this is accomplished. A considerable improvement in the quality of service will result from doing this since it will help manage load balancing and failure recovery difficulties.

4) Resource Management: The three primary resources (communication, computing, and storage) of the decentralized EC-assisted IoT networks need to be controlled, managed, and optimized. This is one of the most important problems that needs thoughtful investigation and attention. The extreme heterogeneity of service providers, IoT edge devices, apps, etc. is the cause of this problem.

6. BLOCKCHAIN FOR EDGE-OF-THINGS AND ITS SOLUTIONS

Blockchain technology is a perfect way to give EoT networks and applications exceptional security because of its special qualities, which include traceability, immutability, and decentralization. The blockchain network's network architecture makes this possible. Each block in the network holds data transactions and the hash of the node that came before it, forming a chain of blocks that is kept up to date by a consensus mechanism like proof-of-work (PoW). These blockchain characteristics guarantee that the records are safe and impenetrable [10].

We present a new BEoT architecture in this work, which is illustrated in Figure 4. Together with industrial applications and BEoT security services, the suggested architecture is made up of three primary components: blockchain, MEC, and IoT [29].

- **IoT:** Data generation and collection from physical settings are the responsibilities of IoT devices, which subsequently send the data to adjacent edge servers through base stations or access points. Certain IoT devices, like laptops and smartphones, can function as mobile blockchain entities to conduct transactions and communicate with the MEC servers directly, while more portable IoT devices can join the blockchain network through their representative gateways [27].

- **Blockchain:** To connect IoT devices, MEC servers, and end users in a decentralized manner, blockchain creates the BEoT system that operates on top of the EoT network. By utilizing its built-in features, including data consensus, smart contracts, and shared ledgers, blockchain specifically guarantees the dependable operation of BEoT systems without the need for a third party [14]. More precisely, by employing techniques like proof-of-work (PoW) controlled by a network of miners, data consensus offers verification services on user transactions.
- **Industrial Applications:** BEoT can open up new industrial uses. For instance, blockchain guarantees safe vehicular communications between dispersed vehicles in a BEoT-based smart transportation system, while MEC servers can facilitate low-latency traffic analytics [15][16].

7. MAJOR FINDINGS

- **Enhanced Security and privacy**: By combining blockchain technology with edge computing, decentralized trust is established, making IoT data verifiable and impervious to manipulation. Distributed databases reduce user data accessibility to centralized organizations and avoid single points of failure.
- **Operational Efficiency:** By processing data closer to IoT devices, edge computing lowers latency and bandwidth usage.
- **Scalable Trust Models:** Blockchain-driven Edge-of-Things (BEoT) frameworks offer trust management, attack detection, and authentication facilities without the need for middlemen

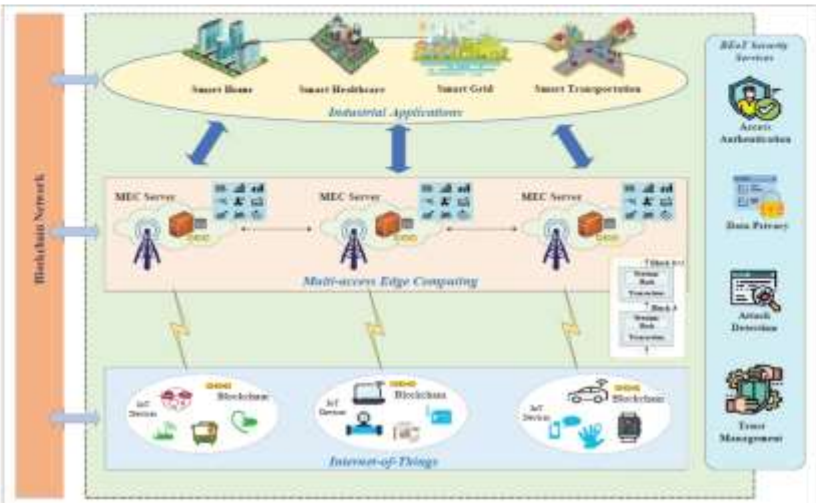

Figure 4. The generic architecture of BEoT.

8. CONCLUSION

We present BEoT in this paper, a new solution enabled by MEC and blockchain that enables low-latency computing of IoT applications while offering strong security levels at the network edge. The prospects presented by BEoT have been specifically examined in a few important applied domains, including smart grid, smart transportation, smart homes, and smart health care. Additionally, BEoT's functions in delivering security services include everything from attack detection and trust management to data privacy protection and access authentication. Lastly, some important research issues and future directions have been highlighted. We think the great advancements possible over existing BEoT techniques will open the door for fresh, creative research and solutions that will enable the next generation of BEoT.

REFERENCES

1. Al-Hasnawi, S. M. Carr, A. Gupta, Fog-Based Local and Remote Policy Enforcement for Preserving Data Privacy in the Internet of Things, Internet of Things (2019) 100069.
2. Aljumah and T. A. Ahanger, "Fog computing and security issues: A review," in 2018 7th International Conference on Computers Communications and Control (ICCCC), 2018, pp. 237–239.
3. Mosenia and N. K. Jha, "A comprehensive study of security of internet-of-things," IEEE Transactions on Emerging Topics in Computing, vol. 5, no. 4, pp. 586–602, Oct 2017.
4. Rauf, R. A. Shaikh, and A. Shah, "Security and privacy for iot and fog computing paradigm," in

2018 15th Learning and Technology Conference (L T), 2018, pp. 96–101.

5. Omoniwa, R. Hussain, M. A. Javed, S. H. Bouk, and S. A. Malik, "Fog/edge computing-based IoT (FECIoT): Architecture, applications, and research issues," IEEE Internet of Things Journal, 2018.
6. Avasalcai, I. Murturi, and S. Dustdar, Edge and Fog: A Survey, Use Cases, and Future Challenges. John Wiley & Sons, Ltd, 2020, ch. 2, pp. 43–65.
7. He, S. Chan, and M. Guizani, "Security in the internet of things supported by mobile edge computing," IEEE Communications Magazine, vol. 56, no. 8, pp. 56–61, August 2018.
8. Liu, Z. Yan, W. Ding, and M. Atiquzzaman, "A survey on secure data analytics in edge computing," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4946–4967, June 2019.
9. IDC, https://www.emc.com/leadership/digital-universe/2014iview/internet-of-things. htm. [Online]. Accessed: 26-Febrauray-2020.
10. J. A. Onieva, R. Rios, R. Roman, and J. Lopez, "Edge-assisted vehicular networks security," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8038–8045, Oct 2019.
11. J. E. Siegel, S. Kumar, and S. E. Sarma, "The future internet of things: Secure, efficient, and model-based," IEEE.
12. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125–1142, Oct 2017.
13. J. Ni, K. Zhang, X. Lin, and X. Shen, "Securing fog computing for internet of things applications: Challenges and solutions," IEEE Communications Surveys Tutorials, vol. 20, no. 1, pp. 601–628, 2018.
14. J. Ni, X. Lin, and X. S. Shen, "Toward edge-assisted internet of things: From security and efficiency perspectives," IEEE Network, vol. 33, no. 2, pp. 50–57, March 2019.
15. J. Pan and J. McElhannon, "Future edge cloud and edge computing for internet of things applications," IEEE Internet of Things Journal, vol. 5, no. 1, pp. 439–449, Feb 2018.
16. J. Pan et al., "Edgechain: An Edge-IoT Framework and Prototype Based on Blockchain and Smart Contracts," IEEE Internet of Things Journal, vol. 6, no. 3, Oct. 2018, pp. 4719–32.
17. J. Wang et al., "Blockchain-based Anonymous Authentication with Key Management for Smart Grid Edge Computing Infrastructure," IEEE Trans. Industrial Informatics, vol. 16, no. 3, Aug. 2019, pp. 1984–92.
18. J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey.
19. K. Jaiswal, S. Sobhanayak, B. K. Mohanta, D. Jena, Iot-cloud based framework for patient's data collection in smart healthcare system using raspberry-pi, in: 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA), IEEE, 2017, pp. 1–4.
20. K.-C. Chen, S.-Y. Lien, Machine-to-machine communications: Technologies and challenges, Ad Hoc Networks 18 (2014) 3–23.
21. M. A. Hoque and R. Hasan, "Towards an analysis of the architecture, security, and privacy issues in vehicular fog computing," in 2019 SoutheastCon, 2019, pp. 1–8.
22. M. Aazam, S. Zeadally, and K. A. Harras, "Fog computing architecture, evaluation, and future research directions," IEEE Communications Magazine, vol. 56, no. 5, pp. 46–52, 2018.
23. M. B. Mollah et al., "Blockchain for Future Smart Grid: A Comprehensive Survey," IEEE Internet of Things Journal, 2020, in press.
24. M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, and V. Kumar, "Security and privacy in fog computing: Challenges," IEEE Access, vol. 5, pp. 19 293–19 304, 2017.