Edge Intelligence in Modern Networks: Survey of Architectures and Frameworks for Scalable Deployment

Pradeep Nayak[1], Mithali S[2], Kuncham Harsha Vardhan Reddy[3], Leevan Michael Vaz[4], Mahamad Gouse N[5]

[1] Assistant professor, Dept. of ISE, Alvas Institute of Engg. & Tech., Karnataka, India
[2] UG Scholar, Dept. of ICB, Alvas Institute of Engg. & Tech., Karnataka, India
[3]UG Scholar, Dept. of ICB, Alvas Institute of Engg. & Tech., Karnataka, India
[4]UG Scholar, Dept. of ICB, Alvas Institute of Engg. & Tech., Karnataka, India
[5]UG Scholar, Dept. of ICB, Alvas Institute of Engg. & Tech., Karnataka, India

Emails:
pradeep@aiet.org.in[1], mithalireddys@gmail.com[2], harshareddy4099@gmail.com[3], leevanmichaelvaz@gmail.com[4], mohamedgouse313@gmail.com[5]

ABSTRACT

Edge computing has emerged as a transformative paradigm addressing the growing need for processing data closer to its source. With the exponential increase in EC devices and latency-sensitive applications, edge computing aims to reduce latency, improve bandwidth efficiency, and enable real-time decision-making. Unlike traditional cloud computing, which relies heavily on centralized data centers, edge computing leverages a decentralized architecture that distributes computational tasks to edge devices and local servers. This review explores the current edge computing architectures and frameworks, focusing on their design, deployment models, and suitability for various applications. Furthermore, this paper examines how edge computing integrates with complementary technologies such as artificial intelligence, 5G, and EC to form robust ecosystems capable of addressing diverse industry needs. Special attention is given to security and privacy considerations in edge architectures, as well as resource management techniques for optimizing performance. By analyzing state-of-the-art frameworks, including federated edge solutions and container-based deployments, this paper aims to identify their strengths, limitations,and potential research directions for further innovation in edge computing systems..

Keyword: - *Edge Computing, Decentralized Architectures, EC, Real-Time Decision-Making, 5G, Artificial Intelligence, Resource Optimization, Security Frameworks*

1. INTRODUCTION

The Edge Computing, or EC, is rapidly transforming the very fabric of our lifestyle into a technology-enabled age where devices interconnect and communicate, share data, and even function on their own without man's intervention. This technological tsunami has every application under the sun, from smart homes and wearable health monitors to industrial automation, smart cities, and much more. EC integrates physical objects with digital networks that allow the devices to act in fluid interaction with ecosystems for gathering and processing unrivaled amounts of data . In such respects, EC has become a technology that puts together several spheres of human life and science, triggering innovation and efficient augmentation of human experience and productivity.

The large-scale usage greatly challenges EC when it comes to security and privacy. Because EC devices are diverse and decentralized with normally low computational powers and heterogeneous communication protocols, robust security measures tend to become quite hard to implement in systems . Centralized traditional frameworks of security cannot be synchronized with the special demands and vulnerabilities inherent in EC environments as provided by the data management and conventional encryption techniques . These also increase the enormous volumes of data from the devices, their vulnerabilities, and data breaches coupled with unauthorized access; therefore, there is an emphasis on secure communication to ensure the integrity and confidentiality of sensitive information. Another challenge still facing EC systems is that of vulnerability to cyberattacks mainly through distributed denial of-service attacks in which the whole network may be floored through malicious traffic

when it is overpowered. These attacks take advantage of the distributed nature of EC devices, thereby indirectly leading to massive attacks on targeted systems. Results of such attacks could be destructive as they lead to operational disruption and loss of money combined with theft of user information . As a result of pervasiveness of EC in the various industrial sectors, the need for new security solutions preventing the risks is really up in a quandary .

Satoshi Nakamoto had introduced blockchain technology in the year 2009, that offers an innovative remedy for the age-old approach in tackling the security problems brought about by EC . There is no inbuilt or artificial single point of failure because the decentralized and immutable ledger adopted in recording transactions and data exchanges effectively obsoletes any form of central authority. Among its intrinsic characteristics are that blockchains are inherently transparent, traceable, and tamper-proof. Blockchain seems to be an extremely promising technology for strengthening security in the communication of the Edge Computing. Besides, blockchain technology can serve as a basis for building up trust among heterogeneous participants of the EC environment, considering the mechanisms of cryptographic validation that ensure integrity. Recently, in the last few years, the combination of blockchain with the Edge Computing has been emphasized by both researchers and practitioners. There have been various studies that mainly focus on architectures supported by blockchain technologies and their possible contributions to improving security provided by EC. For example, some existing works have previously described decentralized models of access control, in which the user can control permissions and access to data without relying on central authorities. Most frameworks have scalability, interoperability, and usability problems that do not make them applicable in real systems in practice. Based on this critical understanding of the literature, only then can gaps be identified in the currently developed solutions towards the progression of secure and efficient blockchain-based EC frameworks. This paper proposes a hybrid framework that aims to enhance EC communication security through the use of blockchain technology. Our solution transcends the lacunae of traditional measures and addresses cyber threats with a sturdier stance. The security framework brings blockchain's decentralized architecture to enable safe data management and to inspire trust among the interested parties . Secure communication for EC devices would not only reduce risks due to data breaches and unauthorized access but, in return, help ensure efficient EC operations that guarantee more reliability. Secure data management will comprise three elements: confidentiality, access control, and license management. This would call for strong encryption and hashing so that confidential information does not leak out to unauthorized parties. The access control mechanism must define the level of access a user should have and start clearly defining rights to help usher in a system whereby the owners hold the rights over their information. Additionally, proper license management is also required to gain confidence from the user end, who are further going to utilize access keys and authentication codes in a fruitful manner. All these components should blend in the framework in unison to comprehend an entirely secured EC .

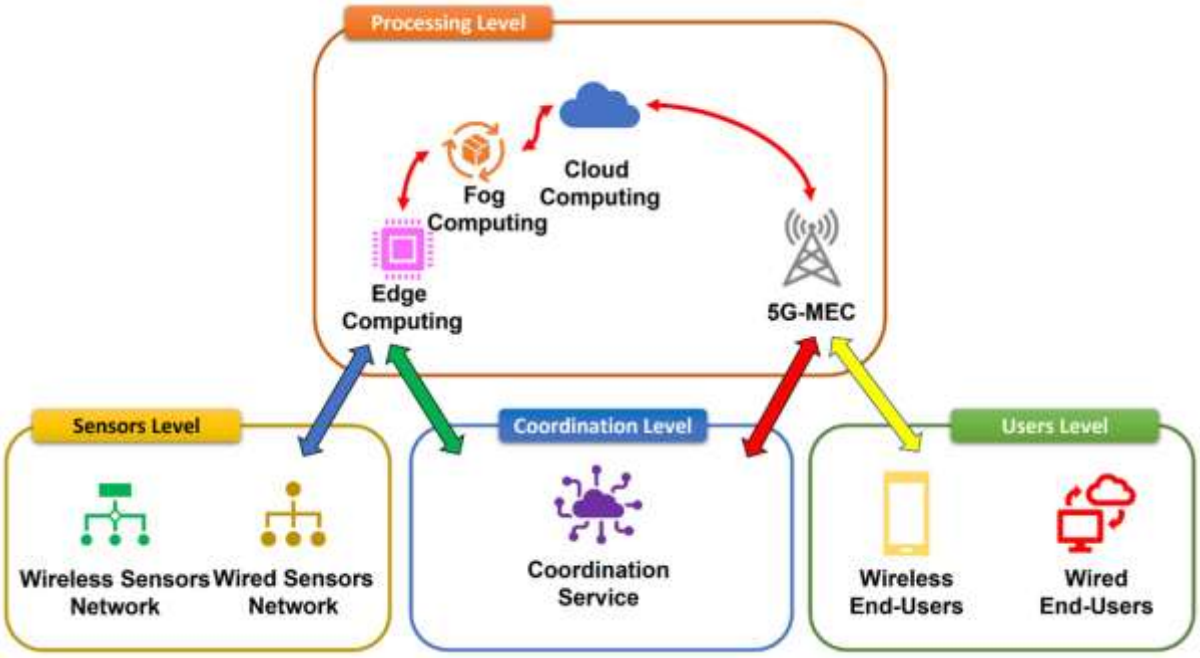
Implementing blockchain technology in EC communication provides a transformational conduit for addressing significant security concerns posed by device interconnection . Our suggested architecture seeks to improve data integrity, secrecy, and access control by taking advantage of the blockchain's decentralized, transparent, and immutable characteristics . With an eye toward the near future, in which EC devices will increasingly play a prominent role in essential applications, the need for effective security solutions must be overlooked in order to avoid information theft and limit the dangers of cyber threats . This review article tries to clarify how blockchain-based solutions will change communications for EC devices in the proceedings, laying the groundwork for future research and innovation in that vital subject.

2. RELATED WORKS

A blockchain-based Edge Computing (EC) framework, ECChain (Fig. 1), integrates the OSCAR framework and ACE authorization system to enhance communication security and reliability in EC environments . OSCAR ensures lightweight message-level security suitable for constrained EC devices, while ACE employs OAuth 2.0–based token management to facilitate scalable and secure access control. With computational tasks distributed between edge nodes and blockchain networks, the hybrid architecture ensures low latency, integrity, and tamper resistance through the Proof of Work (PoW) algorithm

Fig -1: Edge Framework

.



Minoli et al. highlighted blockchain mechanisms that improve EC applications, especially in secure Cyber-Physical Systems (CPS) communication . Blockchain has been widely applied in building trust for Machine-to-Machine (M2M) communication and peer-to-peer systems, addressing privacy and integrity challenges. Systems like ProvChain and MeDShare ensure transparent, immutable data provenance and secure decentralized exchanges. Recent work by Truong et al. improves data sharing by storing metadata on-chain and governing access via smart contracts.

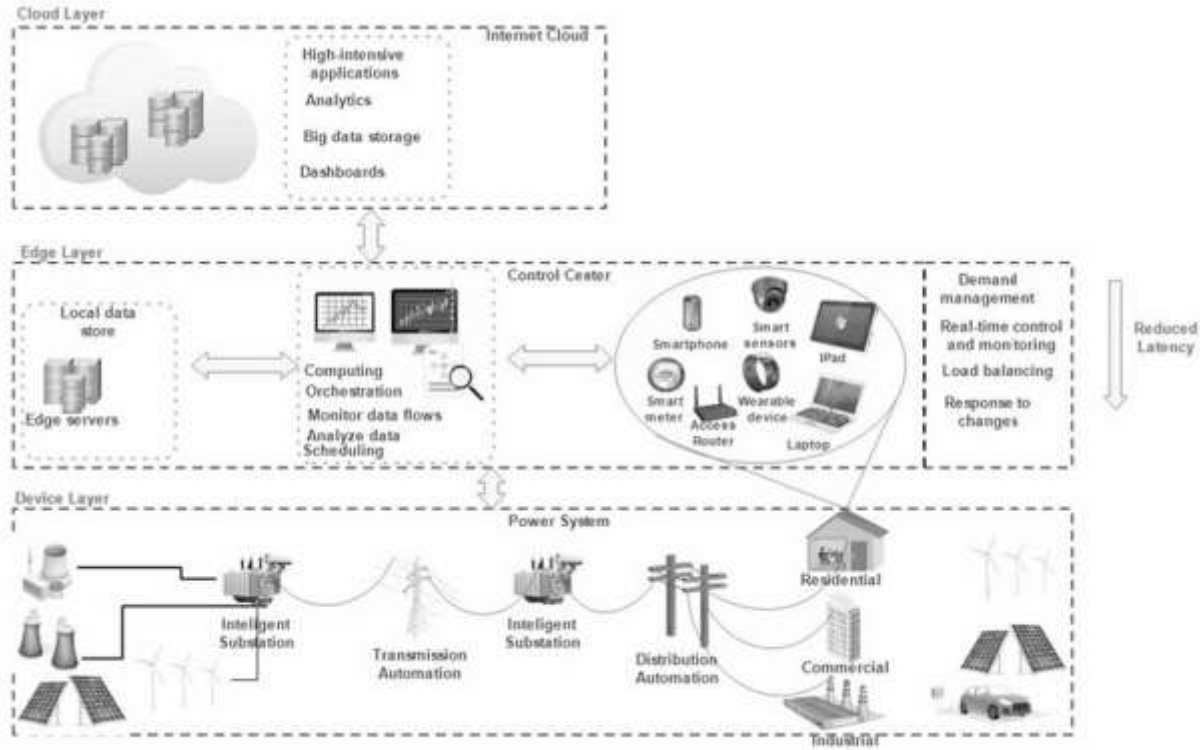


Fig -2: Generic Edge Architecture

Traditional access control models face scalability challenges in EC . Blockchain-based access control frameworks, leveraging smart contracts, offer decentralized, reliable authorization . Consortium blockchains such as Hyperledger Fabric enable permissioned EC networks ensuring privacy and performance .

In Fig. 2, a generic EC architecture is shown, demonstrating the application of cryptographic tools like zero-knowledge proof (ZKP) and homomorphic encryption for secure authentication and encrypted computation . These cryptographic enhancements bolster security and privacy, particularly in smart healthcare and smart city scenarios that rely on real-time, decentralized data processing.

3. EC CASE STUDIES USING BLOCKCHAIN

3.1. Smart City Implementations

One of the main applications for the confluence of EC and blockchain technology is in smart cities. One case study focuses on the implementation of blockchain technology in Dubai's smart city infrastructure, where it is utilized to regulate a number of services like electricity distribution, garbage management, and traffic control. The city authorities are able to establish a transparent, decentralized platform where various stakeholders, including governmental organizations and private businesses, may safely share data and cooperate on city-wide projects by fusing blockchain technology with the Edge Computing.

To ensure data integrity and reduce the danger of hacks, researchers have devised blockchain-based designs that allow for secure and decentralized communication between cars. Additionally, blockchain makes it possible to log car data in a transparent and safe manner, which is beneficial for filing insurance claims, looking into accidents, and adhering to legal requirements .

3.2. Supply Chain Management

The immutable ledger of blockchain technology guarantees the traceability and transparency of commodities as they go through the supply chain, making supply chain management one of the most important uses of blockchain in the Internet of Things. An analysis of Walmart's blockchain project case study shows how the business tracks the movement and origin of throughout its supply chain of food items. Walmart can monitor the temperature, location, and condition of perishable commodities in real-time, lowering the risk of spoilage and guaranteeing food safety, by merging blockchain technology with EC sensors. Because of blockchain's openness, customers can also confirm a product's origin, which improves supply chain accountability and confidence .

3.3. Healthcare and Data exchange

To increase the security and effectiveness of medical data exchange, the healthcare industry is combiningblockchain with EC. One prominent example of using blockchain to maintain electronic health records (EHRs) in a safe and decentralized way is the MedRec project. MedRec uses smart contracts to let patients grant or cancel permissions to healthcare professionals, giving them control over who can access their medical records [15].

Wearable health monitors and other Edge Computing (EC) devices can safely transfer patient data to the blockchain, where it is stored immutably and accessible only by authorized parties. This strategy lowers administrative burden and improves patient outcomes by strengthening data security and facilitating the efficient sharing of medical data amongst various healthcare providers.

4. NEW DEVELOPMENTS IN THE INTEGRATION OF BLOCKCHAIN AND EC

4.1. Blockchain and Federated Learning

It's a trend, which mainly incorporates training models across multiple decentralized devices, without letting the data go up to a central server. Although it supports model training among devices in the Edge Computing contexts, federated learning frameworks can incorporate different layers of security and accountability with blockchain because blockchain provides an easily accessible and unmodifiable record of contributions of data and revisions to models. Federated learning architectures based on blockchain have recently been proposed for such industrial applications as predictive maintenance, whereby devices collaborate to detect anomalies and make predictions about failures.

4.2. Blockchain for 5G and EC

As 5G networks roll out, it is conceptualized that with the integration of blockchain and EC, new opportunities will emerge for secure, real-time communication in EC environments. Due to its massive bandwidth and low latency, 5G is suitable for large-scale Edge Computing deployment, such as remote healthcare, smart factories, and autonomous cars. Blockchain offers safe and decentralized data sharing, payment, and authentication for 5Genabled EC devices. To make The synergy of blockchain and 5G technologies paves the way for secure, low-latency, and high-throughput communication within EC ecosystems. Blockchain enables decentralized identity management, efficient micro-payments, and trustworthy data exchange among heterogeneous 5G-enabled devices. With 5G's enhanced bandwidth and ultra-reliable low-latency communication (URLLC) features, EC nodes can support mission-critical applications such as autonomous vehicles, industrial IoT, and telemedicine with minimal delay.

One of the major advantages of integrating blockchain with 5G networks is network slicing management. Blockchain allows multiple virtualized network slices to be securely orchestrated and maintained without requiring a central authority. Each slice can serve specific applications or organizations, ensuring isolated and verifiable service-level agreements. Additionally, blockchain provides immutable records of resource allocation and utilization, which supports billing transparency and trust among network operators.

For example, in vehicular edge networks, blockchain enables secure information sharing among vehicles (V2V) and between vehicles and roadside units (V2I), preventing malicious data manipulation. Moreover, blockchain combined with 5G edge can facilitate real-time data verification for accident detection, congestion control, and intelligent traffic systems.

4.3. Integration Challenges

Despite these promising benefits, the integration of blockchain with EC and 5G presents challenges such as computational overhead, interoperability issues, and energy consumption. Blockchain operations, especially consensus algorithms like Proof of Work (PoW), require significant processing power and may introduce latency unsuitable for edge applications. Researchers are actively exploring lightweight alternatives like Proof of Authority (PoA) and Directed Acyclic Graph (DAG) structures to mitigate these issues.

Additionally, maintaining synchronization among numerous EC devices within a 5G network is complex. Scalability and cross-domain interoperability must be enhanced to allow smooth data transfer and policy

enforcement across different service providers. Future work focuses on adaptive consensus protocols, multi-chain systems, and AI-driven optimization to balance speed, energy, and trust in edge-blockchain-5G ecosystems.

5. FUTURE RESEARCH DIRECTIONS

Future research in Edge Intelligence emphasizes optimizing blockchain's resource efficiency and enhancing its adaptability in heterogeneous environments. Hybrid consensus mechanisms that blend PoS, PoA, and DAG principles are expected to become prominent. AI-enabled orchestration at the network edge can dynamically allocate computational tasks, manage security keys, and predict workload variations.

Moreover, privacy-preserving computation techniques such as homomorphic encryption, differential privacy, and zero-knowledge proofs (ZKPs) will play a crucial role in safeguarding data integrity without exposing sensitive information. These mechanisms will enable EC to handle confidential data in sectors like healthcare and finance more securely.

Another emerging direction involves integrating quantum-safe cryptographic primitives to prepare EC blockchain systems for post-quantum environments. This ensures long-term resilience against quantum attacks that could compromise current cryptographic standards.

6. CONCLUSIONS

This extended survey highlighted the significant role of blockchain in enhancing the scalability, transparency, and security of Edge Computing systems. By distributing intelligence and trust across network nodes, blockchain mitigates central points of failure and fosters robust EC ecosystems. The integration with 5G networks and federated learning architectures opens the door for intelligent, real-time decision-making across domains.

Nevertheless, the study also emphasizes ongoing challenges particularly in energy efficiency, interoperability, and latency reduction — which remain crucial research frontiers. The continued evolution of edge intelligence will depend on developing lightweight blockchain frameworks, adaptive AI-driven orchestration, and privacy-preserving mechanisms. As technology progresses, the convergence of EC, blockchain, and 5G will pave the way toward a future of secure, scalable, and intelligent distributed systems.

7. REFERENCES

[1] T. Hu, S. Yang, Y. Wang, G. Li, Y. Wang, G. Wang, and M. Yin, "N-Accesses: A Blockchain-Based Access Control Framework for Secure Edge Data Management," *Sensors*, MDPI, 2023.

[2] M. H. S. Mohammed, "A Hybrid Framework for Securing Data Transmission in Edge Computing Environment using Blockchain Approach," in *2021 IEEE International IoT, Electronics and Mechatronics Conference (IEMTRONICS)*, 2021.

[3] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Elsevier*, 2019.

[4] W. Ejaz and A. Anpalagan, "Blockchain Technology for Security and Privacy in Edge Computing," in *Internet of Things for Smart Cities*, SpringerBriefs in Electrical and Computer Engineering, 2019.

[5] M. Aly, F. Khomh, M. Haoues, A. Quintero, and S. Yacout, "Enforcing security in Edge Computing frameworks: A Systematic Literature Review," *Elsevier*, 2019.

[6] S. Huh, S. Cho, and S. Kim, "Managing IoT Devices using Blockchain Platform," in *ICACT2017*, Feb. 19–22, 2017, Daejeon, South Korea.

[7] R. Kamal, E. E.-D. Hemdan, and N. El-Fishway, "A review study on blockchain-based Edge Computing security and forensics," *Springer Nature*, 2021.

[8] R. Yetis and O. K. Sahingoz, "Blockchain Based Secure Communication for Edge Devices in Smart Cities," *National Defence University, Hezarfen Aeronautics and Space Technologies Institute*, Istanbul, Turkey, 2021 ,IEEE.

[9] Ali Dorri, Salil S. Kanhere, and Raja Jurdak, "Blockchain in Edge Computing: Challenges and Solutions," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 1, pp. 176-195, 2020.

[10] Xiwei Xu, Ingo Weber, and Mark Staples, "A Taxonomy of Blockchain-Based Systems for Architecture Design," *IEEE International Conference on Software Architecture*, pp. 243-252, 2017.

[11] Md Saddam Hossain and Ahsan Raja Chowdhury, "A Blockchain Based Secure Data Sharing Model for Edge Computing," *ACM International Conference on Advances in Computing and Communication*, 2018.

[12] Hassan Habib, Tarek S. Sobh, and Mahmoud Al-Qutayri, "Secure Data Management for Edge-based Smart Cities Using Blockchain," *IEEE Access*, vol. 8, pp. 175545-175559, 2020.

[13] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *IEEE International Conference on Big Data*, 2017.

[14] Yousef El Hajj, Hussain Otrok, and Azzam Mourad, "A Blockchain-Based Decentralized Data Management Framework for Edge Computing," *IEEE Transactions on Network and Service Management*, vol. 17, no. 2, pp. 404-419, 2020.

[15] Hieu Trung Huynh, Sung-Han Lee, "Blockchain-based Lightweight Authentication Mechanism for Edge Devices," *International Journal of Computer Science and Network Security*, vol. 19, no. 8, 2019.

[16] Md Ashraf Uddin, Mohsin Iftikhar, "Blockchain-based Secure Data Sharing for Edge Computing," *IEEE Access*, vol. 8, pp. 122487122497, 2020.

[17] Rafael T. de Sousa Junior, Luciano F. Rodrigues, "Blockchain Based Decentralized Framework for Edge Data Management," *Sensors 2021*, MDPI.

[18] A. K. Al Hwaitat, M. A. Almaiah, A. Ali, S. Al-Otaibi, R. Shishakly, A. Lutfi, and M. Alrawad, "A New Blockchain-Based Authentication Framework for Secure Edge Networks", *Electronics*, MDPI, vol. 12, no. 17, pp. 3618, 2023
+
[19] Z. Ullah, B. Raza, H. Shah, S. Khan, and A. Waheed, "Towards Blockchain-Based Secure Storage and Trusted Data Sharing Scheme for Edge Environment", *IEEE Access*, vol. 10, pp. 12341245, Apr. 2022.