JOURNAL OF DYNAMICS AND CONTROL

VOLUME 8 ISSUE 10

PRIORITY-AWARE SCHEDULING FOR EDGE COMPUTING IN INDUSTRIAL NETWORK

Santosh Divekar[1], Dr. Shrikant Zade[2]

[1]Research Scholar, [2]Professor, Department of CSE, G. H. Raisoni University, Saikheda, MP, India

PRIORITY-AWARE SCHEDULING FOR EDGE COMPUTING IN INDUSTRIAL NETWORK

Santosh Divekar[1], Dr. Shrikant Zade[2]
[1]Research Scholar, [2]Professor
Department of CSE, G. H. Raisoni University, Saikheda, MP, India
divekar.santosh6696@gmail.com[1], cdzshrikant@gmail.com[2]

ABSTRACT: With the rapid growth in a connected world and connected things, device networks are growing rapidly. These networks are gaining attention from different infrastructure deployment groups as it has different levels of requirement and architecture planning. As in industries, more wireless devices on a single network at multiple locations have direct or indirect connectivity, which it makes difficult for every device to synchronize with the server all the time. This creates a delay in communication with different devices. Here, an important information packet, which has to be on high priority, may be delayed. This delayed delivery of important packets may create unwanted situations in the industry. This type of system needs real-time communication management. The proposed system is to design, a master-slave and slave-slave-master data forwarding mechanism. This will ensure real-time communication of every node with the central entity by connecting directly or through a free node in the network. This approach will also enhance the connectivity reachability to every wireless node in the network.

KEYWORDS: Scheduling, Edge Computing

1. INTRODUCTION

In the rapidly evolving landscape of industrial networks, the integration of edge computing has emerged as a pivotal solution to meet the growing demand for real-time processing and analysis of data. "Design a Priority-Aware Scheduling for Edge Computing in Industrial Network" delves into the realm of priority-aware scheduling, offering a comprehensive exploration of its implications and applications within industrial settings.

Key Insights: The paper navigates through the intricacies of edge computing, shedding light on the unique challenges posed by industrial environments. Through meticulous analysis, the authors elucidate the significance of priority-aware scheduling in optimizing resource allocation and task execution at the edge. By prioritizing critical tasks over non-urgent ones, the proposed framework ensures efficient utilization of computational resources while meeting stringent latency requirements.

One of the notable strengths of the paper lies in its conceptual framework, which delineates the architecture and components of the priority-aware scheduling system. The authors provide a clear and concise overview of the scheduling algorithm, elucidating its mechanisms for task classification, prioritization, and dynamic adjustment based on changing network conditions. Moreover, the integration of machine learning techniques for predictive scheduling adds a layer of adaptability to the system, enhancing its robustness in dynamic industrial environments.

Furthermore, the paper underscores the practical implications of priority-aware scheduling through simulation-based experiments and real-world case studies. By quantitatively evaluating performance metrics such as response time, throughput, and resource utilization, the authors demonstrate the efficacy of the proposed approach in enhancing overall system efficiency and meeting industrial requirements.

Critical Analysis: While the paper offers valuable insights into the potential benefits of priority-aware scheduling, certain areas warrant further exploration. For instance, a deeper analysis of the scalability and overhead implications of implementing the proposed framework across large-scale industrial networks would provide valuable insights for practitioners. Additionally, considerations for fault tolerance mechanisms and resilience against network failures could enhance the system's reliability in mission-critical applications.

"Design a Priority-Aware Scheduling for Edge Computing in Industrial Network" presents a compelling exploration of priority-aware scheduling in the context of edge computing for industrial networks. Through its systematic approach, insightful analysis, and empirical validation, the paper offers a valuable contribution to the burgeoning field of edge computing. As industrial environments continue to evolve, the integration of priority-aware scheduling promises to unlock new avenues for efficiency, reliability, and performance optimization in industrial edge computing systems.

2. LITERATURE REVIEW

Industrial wireless networks (IWNs) have garnered considerable attention for their ability to deliver time-critical services, leveraging device-to-device (D2D) communication to minimize transmission delays. Researchers have investigated the distributed scheduling problem for D2D-enabled IWNs, considering the varying age of information (AoI) constraints associated with D2D links to ensure information freshness [1].

In the realm of Internet of Things (IoT) and Edge devices, privacy and security remain paramount due to the diverse nature of large-scale appliances and their vulnerability in various working environments. According to [2], the number of Edge devices is projected to surge, with an estimated increase of 31% from 8.74 billion devices in 2020 to potentially 33% by 2021. As Edge devices continue to proliferate, concerns about cybersecurity threats intensify. HP analysis reveals that on average, Edge devices experience around 25% vulnerabilities per device [3].

Edge devices, characterized by computational constraints, low power, and limited memory [3], play a crucial role in sensing physical environments [4]. However, their simple and fragile architecture renders them susceptible to security threats. Moreover, Edge devices face various security challenges and issues, necessitating proactive measures to address them.

As the number of Edge devices is projected to reach 25 billion by 2030 [6], pervasive and ubiquitous security measures are imperative. In recent years, security has become a pressing issue with the exponential growth in the number of Edge devices, emphasizing the importance of end-to-end communication security [7].

In response to the escalating cybersecurity threats facing Edge devices, researchers have proposed various approaches to address security issues and challenges. Bhandari and Gupta [8] conducted a systematic review focusing on fault analysis of Edge systems. Mohammad et al. [9] performed a Systematic Literature Review (SLR) on trust-based Edge recommendation techniques. Aly et al. [10] systematically analyzed security issues across different layers of the Edge. Fazal et al. [11] categorized and analyzed Edge security challenges related to hardware, network, and cloud servers. Macedo et al. [12] conducted an SLR to analyze Edge security across trust, access control, data protection, and authentication aspects. Martinez et al. [13] outlined threats, attacks, challenges, and countermeasures related to Edge security. Similarly, Wittig and Konstantas [14] elucidated existing security and privacy issues through a systematic mapping study. Sultan et al. [15] evaluated security issues and proposed solutions using blockchain technology.

Edge security threats are complex and wide-ranging. Gartner predicts that over a quarter of all cyber-attacks against businesses by 2025 will target Edge systems. Despite this, the current market often prioritizes price and convenience over security. Furthermore, there is a general lack of defense in aging firmware or architectures, along with insufficient emphasis on promoting user awareness and education.

Exposures of Edge devices are increasingly discovered and exploited, with attacks becoming more frequent and severe. Evaluations of the security and privacy of consumer Edge devices [16,17] reveal widespread vulnerabilities, with some devices exhibiting better security postures than others. Notable incidents, such as the Mirai botnet attack and the discovery of zero-day vulnerabilities in VxWorks, underscore the urgency of enhancing cybersecurity measures for Edge devices.

Moreover, Edge security is not merely a technical issue but also a policy concern. Legislations such as the European Cybersecurity Act and the US Congress's Internet of Things Cybersecurity Improvement Acts emphasize the importance of establishing proper safety, security, and privacy measures. User awareness and education regarding the purchase and use of Edge devices are also crucial aspects addressed by legislative initiatives.

Numerous surveys and studies have analyzed Edge security from various perspectives. Aly et al. [18] focused on the layers of Edge reference models, providing guidelines for understanding security issues. Ammar et al. [19] compared the architectures of Edge frameworks and platforms and discussed approaches to ensuring security and privacy. Mosenia and Jha [20] analyzed vulnerabilities affecting the Edge-side layer and proposed countermeasures. Neshenko et al. [21] offered a taxonomy of Edge vulnerabilities, while Zhou et al. [22] identified unique features of Edge devices and discussed associated threats and solutions.

In conclusion, the proliferation of Edge devices necessitates robust security measures to mitigate cybersecurity threats effectively. Legislative initiatives, research endeavors, and collaborative efforts are crucial in addressing the multifaceted security challenges posed by Edge devices and ensuring the integrity, confidentiality, and availability of data in Edge environments.

3. PROPOSED APPROACH

Scheduling jobs in communication systems and ensuring real-time guaranteed data exchange require multiple solutions, and there is still much work to be done in this area as researchers continue to explore new approaches. Upon reviewing numerous research papers, several challenges have been identified:

With the rapid expansion of the interconnected world, including IoT devices, Edge frameworks, and other connected devices, the cyber-physical network is growing at an exponential rate. Different infrastructure deployment groups are increasingly interested in these networks due to their diverse requirements and architectural planning based on specific applications.

In industrial settings, where numerous wireless devices are interconnected within a single network across multiple locations, achieving synchronization with a master data receiver at all times can be challenging. The sheer volume of devices and the complexity of their connectivity arrangements make seamless synchronization difficult to maintain.

The sequencing and synchronization of data within the network often lead to communication delays among different devices. Consequently, critical information packets, which require high-priority delivery, may experience delays, potentially resulting in undesirable situations in industrial environments.

Managing real-time communication in such systems is essential to address these challenges effectively. Moreover, each industry tends to have its own custom networking patterns tailored to specific requirements, posing a significant obstacle to achieving a standardized solution. Addressing these challenges necessitates the development of generic approaches that can accommodate the diverse networking needs of different industries while ensuring efficient and real-time communication management.

a. Proposed System

Proposed system is to design, master-slave and slave-slave-master data forwarding mechanism. This will assure real-time communication of every node with central entity by connecting directly or through free node in the network. This approach will also enhance the connectivity reachability to every wireless node in the network.

Design and development of the master-to-slave communication network for Edge devices with multiple path data forwarding creates and multiple routes in communication. This multiple path data forwarding creates a data reputation problem and also mismatch the right timing sequence of the data received from multiple nodes and multiple paths.

Receiving data from multiple paths and the multiple node waste masters' data filtering and scrutiny time and increase the processing overhead on master node. This extra load may affect the performance of the system and may result in delayed communication or wrong sequential communication. To solve the sequence problem and only collecting right data in right order leads to wait time of every node to get acknowledgement about data reception. All these are micro task and these micro tasks again waste processing time. Delayed communication form different nodes may lead to dependent process execution time or late trigger of emergency notification. Such a delayed communication in manufacturing or the production industry could generate a chaos situation. Proposed system is primarily trying to resolve the above stated issues by developing the right scheduling and communication model for Edge or IoT devices.

Here we proposed a solution to design a device to server and device-to-device data forwarding and data exchange protocol to ensure the packet delivery with highest priority to every data and high-speed communication. Figure 1.0 illustrate the idea behind the proposed system where communication channel will be created based on the demand and availability of best route for communication.

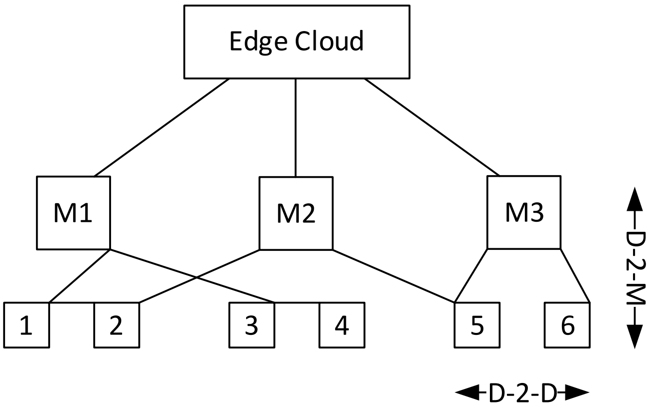

Fig. 1. System architecture

Proposed system is divided in to following development phases as a part of research implementation,

Phase 1. Design and development of the Edge device based physical or simulated network with functionality to establish bidirectional ASCII based communication between every node involved in the network. This will ensure the availability of network to understand the communication and data forwarding issues in real-time. Once this set up is ready, we can establish communication between devices in different modes

Phase 2. Developing the node-addressing scheme with roles and responsibility define of every individual node. Where every node could be a master, slave, or the forwarder node. Based on the role we will develop complete data communication and forwarding scheme this will ensure guaranteed delivery of packet from slave device to master device.

Phase 3. Once the network with right data forwarding is ready, we will start developing the optimization of the data communication in the network and finalizing the defined packet scheduling and communication mechanism for performance enhancement of the system. Here in this phase, we will implement our proposed scheduling algorithm.

Phase 4. Performance testing and the result analysis will be performed in final phase with result conclusion. This will ensure the performance and the accuracy of the proposed system.

4. IMPLEMENTATION

We can communicate with another mobile node by using the three separate networks that we employ in our suggested methods. We establish three networks in our suggested system, and we use this network tower to implement the communication node. That's why we put in place a framework that allows us to accomplish that.

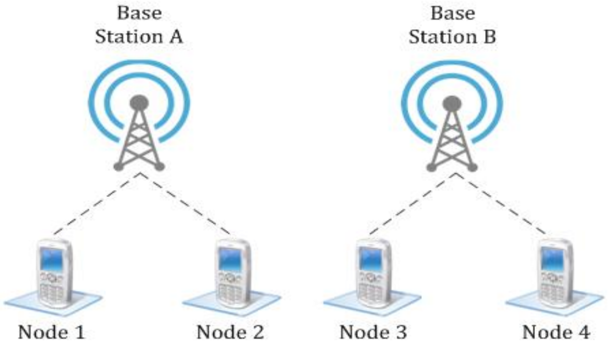

Fig. 2. Communication Structure

The heterogeneous network consists of multiple combinations of various radio technologies that collaborate to deliver optimal service. In the current network, when a mobile node wishes to communicate with another node, it first connects to the base station that is closest to it, and if network service is available, it then connects to the communicating mobile node. However, in our research, we present the method by which a mobile terminal can connect to another mobile network in case the target network is unavailable. This means that if the network service is unavailable for that specific mobile node, we offer a network connection.

a. Description and connectivity for each Phase:

Our project aims to ensure uninterrupted communication over a network even when nodes are roaming. To achieve this goal, we utilize different towers acting as base stations, each operating on a different channel. Our proposed work consists of three phases:

Discovery of available networks:. In the first stage, the node searches for available networks for communication. It selects the available network, such as its own network provider. For instance, if node 1 intends to communicate with node 3, it first checks if its designated Tower A is available. If Tower A is not present, it searches for alternative towers like B or C. Upon finding an available tower, it initiates communication using horizontal handoff.

Communication between two nodes under the same tower:. In this stage, the node selects the best-suited and readily available network provided by the tower it belongs to. For example, if Tower A covers nodes 1 and 2, communication between node 1 and node 2 occurs via Tower A. Both nodes utilize the same channel for communication under the same tower.

Communication between two nodes under different towers:. In the third stage, if the home network (Tower A) is not available, the node selects another tower for communication, employing vertical handoff. It searches for an alternative network that is free to use for data communication. This ensures seamless communication even when nodes are under different tower coverage areas.

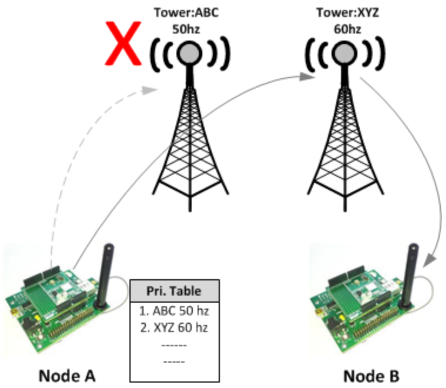

Fig. 3. Auto switching between multiple towers

A comprehensive system overview of the system depicted in Figure 4. We put in place a mechanism where nodes that are on the same frequency in the same channel can communicate with one another. And if our node is unreachable in the following section, they will use a different base station's network to communicate via a different channel. The node will initially look through every network that is accessible and free to use before choosing one. Following selection, it will make a request for a connection, which the receiving node will accept before it begins communicating with the other nodes.

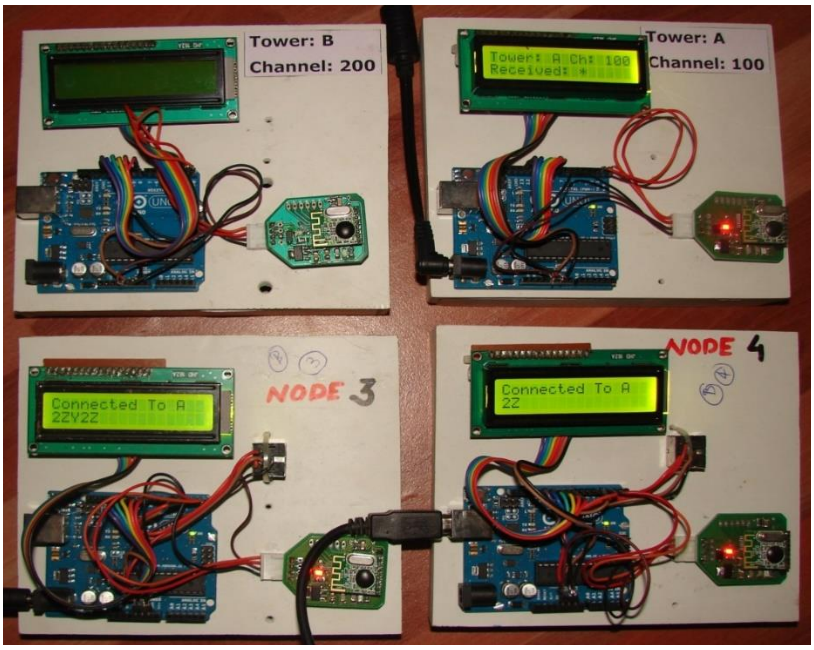

Fig. 4. Real time execution of Node in Network

Proposed model as a proof of concept demonstrated the auto shifting between multiple service available system or based unit.

5. CONCLUSION

Redesigning the Edge communication architecture to provide feasible Authentication, Identification, and communication across fixed, dynamic, or ad-hoc networks is a highly demanded requirement. We propose decentralizing the Edge service provider server deployment to achieve load balancing and fail-safe situation management through network message scheduling. This concept aims to assist Edge device service providers in establishing standardized infrastructure capable of facilitating registration, authorization, authentication, and message transfer. By distributing server deployment across the Edge network, we aim to enhance system reliability, scalability, and efficiency, thereby addressing the evolving demands of modern communication architectures. This decentralized approach enables more robust and resilient communication protocols, allowing Edge devices to securely authenticate and communicate over various network configurations. Additionally, the implementation of network message scheduling ensures efficient utilization of network resources, minimizing latency and maximizing throughput. Through this proposed solution, we anticipate significant advancements in Edge communication capabilities, paving the way for enhanced connectivity and interoperability in distributed computing environments.

References

1. Mingyan Li , Member, IEEE, Cailian Chen , Member, IEEE, Huaqing Wu , Student Member, IEEE, Age-of-Information Aware Scheduling for Edge-Assisted Industrial Wireless Networks, IEEE Transactions On Industrial Informatics, Vol. 17, No. 8, August 2021
2. Xinping Guan *, Fellow, IEEE*, and Xuemin Shen *, Fellow, IEEE*
3. A. Dean and M. O. Agyeman, ``A study of the advances ìn Edge securìty," ìn *Proc. 2nd Int. Symp. Comput. Scì. Intell. Control*, 2018, p. 15.
4. C.-T. Lì, C.-C. Lee, C.-Y. Weng, and C.-M. Chen, ``Towards secure authentìcatìng of cache ìn the reader for RFID-based Edge systems," *Peer-Peer Netw. Appl.*, vol. 11, no. 1, pp. 198_208, Jan. 2018.
5. C.-T. Lì, T.-Y.Wu, C.-L. Chen, C.-C. Lee, and C.-M. Chen, "An effìcìent user authentìcatìon and user anonymìty scheme wìth provably securìty for Edge-based medìcal care system," *Sensors*, vol. 17, no. 7, p. 1482, Jun. 2017.
6. R. Gurunath, M. Agarwal, A. Nandì, and D. Samanta, ``An overvìew: Securìty ìssue ìn Edge network," ìn *Proc. 2nd Int. Conf. Edge Socìal, Mobìle, Anal. Cloud (I-SMAC)*, Aug. 2018, pp. 104_107.
7. J. Ahamed and A. V. Rajan, ``Internet of Thìngs (Edge): Applìcatìon systems and securìty vulnerabìlìtìes," ìn *Proc. 5th Int. Conf. Electron. Devìces, Syst. Appl. (ICEDSA)*, Dec. 2016, pp. 1_5.
8. E. Buenrostro, D. Cyrus, T. Le, and V. Emamìan, "Securìty of Edge devìces," *J. Cyber Secur. Technol.*, vol. 2, no. 1, pp. 1_13, 2018.
9. V. Mohammadì, A. M. Rahmanì, A. M. Darwesh, and A. Saha_, "Trust based recommendatìon systems ìn Internet of Thìngs: A systematìc lìterature revìew," *Hum.-Centrìc Comput. Inf. Scì.*, vol. 9, no. 1, p. 21, Dec. 2019.
10. G. P. Bhandarì and R. Gupta, ``A systematìc lìterature revìew ìn fault analysìs for Edge," *Int. J. Web Scì.*, vol. 3, no. 2, pp. 130_147, 2019.
11. K. Fazal, H. Shehzad, A. Tasneem, A. Dawood, and Z. Ahmed, ``A systematìc lìterature revìew on the securìty challenges of Internet of Thìngs and theìr classì_catìon," *Int. J. Technol. Res.*, vol. 5, no. 2, pp. 40_48, 2017.
12. M. Aly, F. Khomh, M. Haoues, A. Quìntero, and S. Yacout, ``Enforcìng securìty ìn Internet of Thìngs frameworks: A systematìc lìterature revìew," *Internet Thìngs*, vol. 6, Jun. 2019, Art. no. 100050.
13. E. L. C. Macedo, E. A. R. de Olìveìra, F. H. Sìlva, R. R. Mello, F. M. G. Franca, F. C. Delìcato, J. F. de Rezende, and L. F. M. de Moraes, ``On the securìty aspects of Internet of Thìngs: A systematìc lìterature revìew," *J. Commun. Netw.*, vol. 21, no. 5, pp. 444_457, Oct. 2019.

14. J. Martínez, J. Mejía, and M. Muñoz, ``Securìty analysìs of the Internet of Thìngs: A systematìc lìterature revìew," ìn *Proc. Int. Conf. Softw. Process Improvement (CIMPS)*, Oct. 2016, pp. 1_6.
15. M. Wìttì and D. Konstantas, ``EDGE and securìty-prìvacy concerns: A systematìc mappìng study," *Int. J. Netw. Secur. Appl.*, vol. 10, no. 6, pp. 25_33, Nov. 2018.
16. A. Sultan, M. S. Arshad Malìk, and A. Mushtaq, ``Internet of Thìngs securìty ìssues and theìr solutìons wìth blockchaìn technology characterìstìcs: Asystematìc lìterature revìew," *Amer. J. Comput. Scì. Inf. Technol.*, vol. 6, no. 3, p. 27, 2018.
17. S.-R. Oh and Y.-G. Kìm, ``Securìty requìrements analysìs for the Edge," ìn *Proc. Int. Conf. Platform Technol. Servìce (PlatCon)*, Feb. 2017, pp. 1_6.
18. Loì, F.; Sìvanathan, A.; Gharakheìlì, H.H.; Radford, A.; Sìvaraman, V. Systematìcally Evaluatìng Securìty and Prìvacy for Consumer Edge Devìces. In Proceedìngs of the Workshop on Internet of Thìngs Securìty and Prìvacy (EdgeS&P), Dallas, TX, USA, 3 November 2017.
19. Alrawì, O.; Lever, C.; Antonakakìs, M.; Monrose, F. SoK: Securìty Evaluatìon of Home-Based Edge Deployments. In Proceedìngs of the 2019 IEEE Symposìum on Securìty and Prìvacy (SP), San Francìsco, CA, USA, 19–23 May 2019; pp. 1362–1380.
20. Aly, M.; Khomh, F.; Haoues, M.; Quìntero, A.; Yacout, S. Enforcìng securìty ìn Internet of Thìngs frameworks: A Systematìc Lìterature Revìew. Internet Thìngs 2019, 6, 100050.
21. Ammar, M.; Russello, G.; Crìspo, B. Internet of Thìngs: A survey on the securìty of Edge frameworks. J. Inf. Secur. Appl. 2018, 38, 8–27.
22. Neshenko, N.; Bou-Harb, E.; Crìchìgno, J.; Kaddoum, G.; Ghanì, N. Demystìfyìng Edge Securìty: An Exhaustìve Survey on Edge Vulnerabìlìtìes and a Fìrst Empìrìcal Look on Internet-Scale Edge Exploìtatìons. IEEE Commun. Surv. Tutor. 2019, 21, 2702–2733.
23. Zhou,W.; Jìa, Y.; Peng, A.; Zhang, Y.; Lìu, P. The Effect of Edge New Features on Securìty and Prìvacy: New Threats, Exìstìng Solutìons, and Challenges Yet to Be Solved. IEEE Internet Thìngs J. 2019, 6, 1606–1616.
24. Susha Surendran, Amìra Nassef, Babak D. Beheshtì. “A survey of cryptographìc algorìthms for Edge devìces” , 2018 IEEE Long Island Systems, Applìcatìons and Technology Conference (LISAT), 2018
25. MD Azharul Islam, Sanjay K. Madrìa, “A Permìssìoned Blockchaìn based Access Control System for EDGE”, 2019 IEEE Internatìonal Conference on Blockchaìn (Blockchaìn), DOI 10.1109/Blockchaìn.2019.00071