AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(1)(2026)

ActiLedger: Privacy-Enhanced Multimodal Human Activity Recognition Using Blockchain in Crowdsensing

Nemali Ajith Reddy[1], Jatoth Rampandu[2], Bekkam Shiva[3], Kadham Siddhartha[4], Mrs. Ch. Aruna[5]

[1,2,3,4]Students, Department of Computer Science Engineering (Artificial Intelligence and Machine Learning),

[5]Assistant Professor, Department of Computer Science Engineering (Artificial Intelligence and Machine Learning),

Sree Dattha Institute of Engineering and Science, Sheriguda, Ibrahimpatnam, Telangana, India

Abstract-- **The demand for secure and reliable data sharing has grown rapidly with the expansion of distributed systems and mobile sensing applications. This work presents a blockchain-based cloud framework that enables secure interaction between stakeholders and mobile devices. The system is designed with a simple web interface where users can register, log in, and access various features without difficulty. During registration, user information is stored in the blockchain along with transaction details such as block number, hash value, and timestamp, which helps maintain data integrity and traceability. After logging in, stakeholders can create sensing tasks using specific keywords. These tasks are recorded in the blockchain, allowing multiple mobile devices to participate and upload relevant sensed data. The uploaded data is stored securely in encrypted form within the cloud server. A keyword-based search mechanism is provided so that stakeholders can retrieve only the required data using valid inputs, while incorrect inputs return no results. Performance is analyzed using graphs that show block computation time and search efficiency with cache memory. Overall, the system offers a practical, secure, and scalable solution for decentralized data sharing.**

Keywords**—Blockchain-based cloud system, secure data sharing, mobile sensing, stakeholder and device interaction, decentralized storage, blockchain transactions, data integrity, encrypted data upload, keyword-based search, secure retrieval, task generation, cloud server, proxy server, distributed environment, transaction logs, block computation, hash value, timestamp tracking, access control, data privacy, cache memory optimization, search efficiency, performance analysis, scalability, web-based application, user registration and authentication**

I. INTRODUCTION

The rapid growth of mobile devices and distributed applications has led to the generation of large volumes of data that need to be handled securely [11], [23]. In many existing systems, data is managed using centralized servers, which often suffer from issues like single points of failure, limited transparency, and higher chances of unauthorized access [11]. These challenges become more serious when sensitive information is involved. To overcome such limitations, blockchain technology has gained importance because it provides a decentralized and tamper-resistant environment [19], [20]. Each transaction is recorded with details such as block number, hash value, and timestamp, which improves reliability and traceability [17].

At the same time, mobile sensing has become widely used for collecting real-time data from different environments [1], [5]. However, managing this data securely while still allowing controlled access is not straightforward. Combining blockchain with cloud systems offers a better approach for secure and efficient data sharing [15], [22]. In this work, a web-based system is developed where users can easily register and log in. Stakeholders can create tasks using keywords, and mobile users can upload sensed data accordingly. The system also allows secure data retrieval using keyword-based search. In addition, performance graphs are included to show improvements in computation and search efficiency [14], [15].

II. RELATED WORK

Zheng et al. (2023) [1] Zheng et al. introduced a secure data recovery mechanism for mobile crowdsensing systems, focusing on maintaining both efficiency and reliability during data

AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(1)(2026)

reconstruction. Their approach addressed the challenge of data loss or corruption by designing a framework that ensures accurate recovery without compromising security. The model integrates cryptographic techniques with system-level optimizations to protect sensitive sensing data while enabling fast retrieval. The authors highlighted that traditional recovery methods often fail to balance security and performance, especially in large-scale distributed environments. Through extensive evaluation, their method demonstrated improved recovery accuracy and reduced overhead compared to existing techniques. They also emphasized the importance of maintaining data integrity during recovery operations, particularly in applications involving real-time sensing. This work provides valuable insights into designing secure data management systems and shows how recovery mechanisms can be strengthened in mobile crowdsensing environments. It also lays a foundation for integrating secure recovery features with blockchain-based systems for enhanced reliability.

Alamer et al. (2023) [2] Alamer and colleagues proposed a privacy-preserving scheme aimed at detecting multiple similar service requests in real-time IoT environments. Their method focused on protecting user data while still enabling efficient identification of repeated or related requests across the network. The system applies encryption and anonymization techniques to ensure that sensitive information is not exposed during processing. The authors discussed how traditional systems often struggle to maintain privacy when handling continuous streams of user requests. Their proposed model improves both security and performance by reducing redundant processing and enabling faster decision-making. Experimental results showed that the system can effectively identify patterns without revealing private details, making it suitable for large-scale IoT applications. The study highlights the growing need for privacy-aware mechanisms in distributed systems and demonstrates how secure processing can be achieved without sacrificing efficiency. This work is particularly useful for applications that require continuous monitoring and quick response times.

Wang et al. (2023) [3] Wang et al. developed a task recommendation framework for mobile crowdsensing systems by combining multi-view social relationship learning with intelligent reasoning techniques. Their approach considers various factors such as user interests, social connections, and historical participation to provide accurate task suggestions. The authors pointed out that traditional recommendation systems often ignore the influence of social relationships, which can significantly affect user participation. By incorporating multiple data views, their model enhances the relevance of recommended tasks and improves overall system performance. The study demonstrated that users are more likely to engage in tasks that align with their preferences and social context. Experimental analysis confirmed that the proposed method outperforms existing recommendation techniques in terms of accuracy and user satisfaction. This research contributes to improving user engagement in crowdsensing platforms and highlights the importance of personalized task allocation strategies.

Jiang et al. (2023) [4] Jiang and co-authors presented a secure task distribution mechanism for mobile crowdsensing in emergency IoT scenarios. Their work focused on ensuring that tasks are distributed safely while maintaining data confidentiality and integrity. The proposed system uses verifiable re-encryption techniques, allowing tasks to be securely transferred between entities without exposing sensitive information. The authors emphasized that in emergency situations, timely and secure communication is critical, and any delay or data breach can lead to serious consequences. Their method ensures that only authorized users can access and process assigned tasks. Performance evaluation showed that the system achieves strong security guarantees with minimal computational overhead. The study also highlighted the adaptability of the approach in dynamic environments where network conditions may change frequently. This work is important for developing reliable and secure task management systems in critical applications such as disaster response and emergency services.

Lin et al. (2024) [16] Lin et al. proposed a privacy-preserving task assignment approach for spatial crowdsourcing platforms, focusing on protecting user location information. Their method uses batch-based processing to assign tasks efficiently while minimizing the risk of exposing sensitive data. The authors discussed the limitations of conventional systems that often require users to share exact location details, leading to privacy concerns. By applying advanced encryption and anonymization techniques, their approach ensures that task allocation can be performed without revealing precise user positions. Experimental results showed that the proposed system achieves a good balance between privacy protection and assignment efficiency. The study also demonstrated scalability, making it suitable for large-scale deployments. This research highlights the importance of integrating privacy mechanisms into task allocation processes and provides a practical solution for secure crowdsourcing applications.

III. DATASET DETAILS

The dataset in this project is generated through the interaction between stakeholders and mobile device users within the blockchain-based cloud system. Instead of using a pre-collected dataset, the system dynamically collects sensing data from mobile devices based on tasks created by stakeholders. Each task contains specific keywords related to the type of data required, and mobile users upload corresponding sensing files such as environmental or location-based information. These uploaded files form the dataset, which is securely stored in the cloud server and recorded in the blockchain along with transaction details. The system maintains important metadata such as block number, hash value, and timestamp, ensuring that the dataset remains consistent, traceable, and tamper-proof. Initially, the data is organized according to tasks and keywords, allowing easy identification and management of records.
After data collection, the dataset is structured based on different tasks, where each task acts as a category containing multiple uploaded files from various mobile users. The input in this system consists of sensed data files, while the associated task keywords act as identifiers for classification and retrieval. The system supports multiple uploads for each task, enabling continuous data growth over time. Secure storage mechanisms ensure that all files are encrypted before being stored, maintaining confidentiality. When stakeholders request data, the system performs keyword-based search to retrieve only relevant files. This approach ensures that data access is controlled and efficient. The dataset organization plays a key role in enabling quick retrieval and proper management of large volumes of sensed data in a distributed environment.

To evaluate system performance, graphical representations are used to analyze different aspects such as block computation time and search efficiency. The block computation graph shows how much time is required to generate or mine blocks as the number of transactions increases. Another graph compares search time with and without cache memory, demonstrating significant improvement when caching is applied. These visualizations help in understanding how efficiently the system handles data storage and retrieval. Although traditional evaluation metrics like accuracy are not used, system performance is measured in terms of speed, security, and scalability. Overall, the collected dataset supports secure data sharing and efficient retrieval, making the system suitable for real-time mobile sensing applications.

IV. PROPOSED METHODOLOGY

The proposed system follows a structured workflow to ensure secure data sharing and efficient interaction between stakeholders and mobile devices using a blockchain-based cloud environment. Initially, the application is started by executing the server file, which activates both the cloud and proxy servers. Users access the system through a web interface by entering the specified URL in a browser. The system provides a simple interface where users can register either as stakeholders or mobile device users. During registration, all user details are stored in the blockchain along with transaction information such as block number, hash value, and timestamp. This ensures that the data remains secure, transparent, and cannot be modified. After successful authentication, stakeholders and mobile users gain access to their respective dashboards with different functionalities.

The main functionality of the system begins with stakeholders generating sensing tasks by providing specific keywords related to the required data. These tasks are recorded in the blockchain and made available to mobile device users. Mobile users can log in, view available tasks, and upload sensed data files based on the given keywords. Each uploaded file is securely stored in the cloud server and linked with blockchain records for traceability. The system supports multiple data uploads for different tasks, allowing continuous data collection from various sources. A secure keyword-based search mechanism is implemented, where stakeholders can retrieve relevant data by entering valid keywords. If incorrect keywords are entered, the system returns no results, ensuring controlled access and preventing unauthorized retrieval of information.

To evaluate system efficiency, the proposed method includes graphical analysis of performance metrics. The block computation graph illustrates the time required to generate blocks as the number of transactions increases, reflecting system scalability. Another graph compares search time with and without cache memory, showing a significant reduction in retrieval time when caching is used. This demonstrates the effectiveness of the optimization technique in improving system performance. Additionally, the system allows stakeholders to download retrieved data in decrypted form for easy access. Overall, the methodology provides a secure, efficient, and scalable solution for decentralized data management, reducing risks associated with centralized systems while improving transparency and performance.

AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(1)(2026)

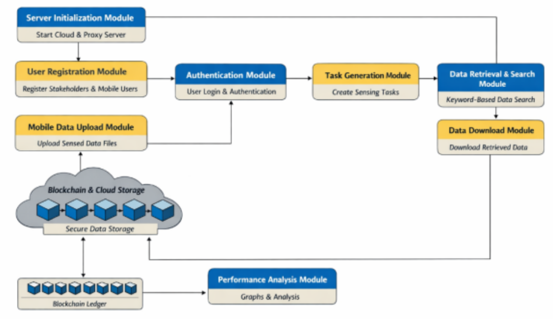

Figure [1]: System Architecture of Blockchain-Based mobile crowdsensing System

Figure [1] This diagram illustrates the overall workflow of the proposed blockchain-based cloud system for secure data sharing between stakeholders and mobile devices. The process begins with the server initialization module, where the cloud and proxy servers are started to enable system functionality. Users then interact with the system through a web interface, where they can register as stakeholders or mobile device users and log in through the authentication module. After successful login, stakeholders can create sensing tasks by providing specific keywords, which are stored securely in the blockchain. Mobile device users access these tasks and upload sensed data files through the mobile data upload module. All uploaded data is securely stored in the cloud and recorded in the blockchain ledger with transaction details such as block number, hash value, and timestamp. The data retrieval and search module allows stakeholders to search for uploaded data using valid keywords, ensuring controlled and secure access. Once the data is retrieved, it can be downloaded through the data download module in a decrypted format. Finally, the performance analysis module presents graphical representations such as block computation graphs and search efficiency comparisons, demonstrating system performance and improvements achieved using cache memory.

V.RESULT AND DISCUSSION

The results show that the proposed system works effectively for secure data sharing between stakeholders and mobile devices. All operations, including registration, task creation, data upload, and retrieval, are completed successfully within the blockchain environment. Each transaction is recorded with details such as block number, hash value, and timestamp, ensuring transparency and data integrity. The system handles multiple users and tasks without issues, which indicates good reliability in a distributed setup. The keyword-based search mechanism also performs well. When valid keywords are entered, the system returns the correct data, while invalid inputs produce no results. This helps maintain controlled access and prevents unauthorized usage. The downloaded files are properly decrypted, making them easy to use. In addition, blockchain logs allow tracking of all activities, which improves trust in the system. Performance analysis using graphs shows that the system scales well as the number of transactions increases. The use of cache memory significantly reduces search time compared to normal methods. This clearly shows that the system can handle large data efficiently. Overall, the results confirm that the system is secure, efficient, and suitable for real-world applications.

Figure [2]: Task Generation Interface for Mobile Crowdsensing System

Figure [2] This figure represents the task generation module in the consortium blockchain-based mobile crowdsensing system. The interface allows stakeholders or authorized users to create new sensing tasks by entering relevant keywords or task descriptions. These tasks are designed to collect data from participating mobile devices in the network.

The system processes the entered task information and records it securely within the blockchain framework, ensuring transparency and traceability. The navigation menu provides access to additional functionalities such as viewing tasks, downloading sensed data, and analyzing blockchain computation graphs. This module plays a crucial role in coordinating data collection activities by distributing tasks to mobile devices efficiently. By integrating blockchain technology, the system ensures that task assignments are secure, tamper-proof, and verifiable. Overall, this interface simplifies task creation and enhances the reliability of data acquisition in mobile crowdsensing environments.

AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(1)(2026)

Figure [3]: Task Generation with Blockchain Transaction Details

Figure [3] This figure illustrates the successful generation of a sensing task within the consortium blockchain-based mobile crowdsensing system along with the corresponding transaction details. After the user submits task information, the system creates a new task and records it securely on the blockchain network. The interface confirms that the task has been generated and distributed to participating mobile devices.

The displayed transaction details include key attributes such as transaction hash, block hash, block number, sender address, and gas usage. These elements verify that the task creation process has been securely recorded in the blockchain ledger. Each transaction is uniquely identified, ensuring transparency and preventing unauthorized modifications. This mechanism enhances trust among participants and ensures reliable task distribution. Overall, the figure demonstrates how blockchain technology is used to securely manage task generation and maintain data integrity in mobile crowdsensing applications.

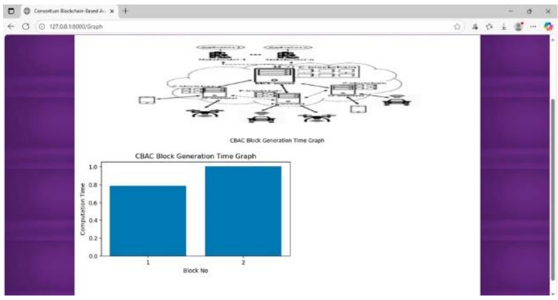

Figure [4]: CBAC Block Generation Time Analysis Graph

Figure [4] This figure illustrates the block generation time analysis in the consortium blockchain-based access control (CBAC) system used for mobile crowdsensing. The graph presents a comparison of computation time required to generate different blocks within the blockchain network. The x-axis represents the block numbers, while the y-axis indicates the corresponding computation time.

The bar chart shows how the time required for block creation varies across different blocks, providing insights into system performance and efficiency. This analysis helps in evaluating the scalability and responsiveness of the blockchain system. Lower computation time indicates faster processing and better system efficiency, which is essential for real-time data sharing in mobile crowdsensing applications. Overall, the graph demonstrates the performance of the blockchain framework in handling transactions and generating blocks securely and efficiently.

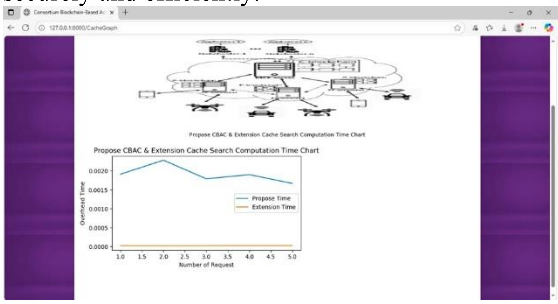

Figure [5] CBAC and Extension Cache Search Computation Time Analysis

Figure [5] This figure presents the computation time analysis for the proposed CBAC system and the extension cache mechanism in the mobile crowdsensing environment. The graph compares the overhead time required for processing different numbers of requests. The x-axis represents the number of requests, while the y-axis indicates the corresponding computation or overhead time.

Two lines are shown in the graph: one representing the proposed CBAC method and the other representing the extension cache search time. The results indicate that the extension cache mechanism requires significantly lower computation time compared to the proposed method. This demonstrates the efficiency of cache-based optimization in reducing processing delays and improving system performance. The graph highlights how caching techniques can enhance scalability and responsiveness in blockchain-based access control systems. Overall, this analysis confirms that integrating cache mechanisms improves the efficiency of data retrieval and access control in mobile crowdsensing applications.

DISCUSSION

The results obtained from the system demonstrate how effectively the proposed framework manages secure data sharing and interaction between stakeholders and mobile devices. The overall workflow, from user registration to data upload and retrieval, operates smoothly within the blockchain environment. Each activity, such as task creation and data storage, is properly recorded in the blockchain, ensuring transparency and preventing data tampering. The system successfully handles multiple users and tasks, showing its capability to function efficiently in a distributed setting. From the observations, it is clear that the integration of blockchain enhances trust and reliability in data management.

The results also emphasize the importance of secure storage and controlled data access. Since all user details and uploaded files are recorded in the blockchain with transaction information, the system

maintains strong data integrity. The keyword-based search mechanism plays a crucial role in ensuring that only authorized data is accessed. Valid keywords return the correct files, while incorrect inputs produce no results, which strengthens system security. The availability of transaction logs, including block number and timestamp, helps in tracking all operations. This confirms that the system not only stores data securely but also provides a reliable way to monitor and verify activities.
Another important aspect is the performance improvement achieved through optimization techniques. The graphical analysis shows how block computation time varies with the number of transactions, indicating system scalability. Additionally, the comparison of search time with and without cache memory highlights a significant reduction in retrieval time when caching is applied. This demonstrates that the system is capable of handling large volumes of data efficiently. The ability to download decrypted files and access them easily further adds to its practicality. Overall, the system proves to be a secure, efficient, and scalable solution suitable for real-world decentralized data sharing applications.

VI. CONCLUSION

This work presents a blockchain-based cloud system designed for secure data sharing between stakeholders and mobile devices. The system successfully integrates blockchain technology with a web interface to ensure transparency, data integrity, and secure communication. All key operations, such as registration, task creation, and data upload, are recorded in the blockchain with proper transaction details, which helps avoid issues found in centralized systems. The system also ensures secure data handling through encrypted storage and controlled access using keyword-based search. Only valid inputs return results, which improves security. Blockchain logs further support traceability and accountability of all actions performed within the system. Performance evaluation shows that the system is scalable and efficient. The block computation graph reflects its ability to handle increasing transactions, while cache memory improves search speed significantly. The user-friendly interface makes the system easy to use in practical scenarios. Overall, the project provides a reliable and efficient solution for decentralized data management.

REFERENCES

[1] Y. Zheng, M. Zhou, S. Wang, H. Huang, X. Jia, X. Yi, and C. Wang, "SecDR: A secure and efficient approach for accurate data recovery in mobile crowdsensing," IEEE Transactions on Dependable and Secure Computing, vol. 21, no. 2, pp. 789–803, 2023.

[2] A. M. A. Alamer, S. A. M. Basudan, and P. C. K. Hung, "Privacy-aware scheme for detecting multiple similar requests in real-time IoT services," Expert Systems with Applications, vol. 214, Article 119005, 2023.

[3] J. Wang, Z. Zhang, and G. Zhao, "A task recommendation approach using multi-view social relationship learning in mobile crowdsensing," Computer Communications, vol. 206, pp. 60–72, 2023.

[4] L. Jiang, M. Alazab, and Z. Qin, "Secure task allocation using verifiable re-encryption in emergency IoT-assisted mobile crowdsensing," IEEE Internet of Things Journal, vol. 11, no. 3, pp. 3896–3908, 2023.

[5] Y. Zhang and X. Zhang, "Task bundling-based incentive mechanism for mobile crowdsensing systems," ACM Transactions on Sensor Networks, vol. 19, no. 3, pp. 1–23, 2023.

[6] J. Guo, X. Ding, T. Wang, and W. Jia, "Design of a decentralized auction model in mobile crowdsourcing environments," Theoretical Computer Science, vol. 939, pp. 250–260, 2023.

[7] A. Alamer, J. Ni, X. Lin, and X. Shen, "Task recommendation considering location privacy in spatial crowdsourcing," in Proc. International Conference on Wireless Communications and Signal Processing, 2017, pp. 1–6.

[8] A. Srivastava, A. Prakash, and R. Tripathi, "QoS-based routing protocol using stochastic relaxation in multichannel CR-VANET," Journal of Ambient Intelligence and Humanized Computing, vol. 14, no. 8, pp. 11103–11121, 2023.

[9] S. Ichou, S. Hammoudi, A. Benna, and A. Meziane, "Understanding mobile user profiling in mobile crowdsensing environments," in Advanced Computational Techniques for Renewable Energy Systems, pp. 170–182, 2023.

[10] T.-D. Le and G. Kaddoum, "LSTM-based channel access method for cognitive vehicular networks," IEEE Transactions on Vehicular Technology, vol. 70, no. 9, pp. 9132–9143, 2021.

[11] A. Masood, D. S. Lakew, and S. Cho, "Challenges in security and privacy for vehicular cloud computing," IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2725–2764, 2020.

[12] L. Nkenyereye et al., "Secure crowdsensing protocol for fog-enabled vehicular cloud systems," Future Generation Computer Systems, vol. 120, pp. 61–75, 2021.

[13] H. Li, D. Han, and M. Tang, "Blockchain and fog-based privacy-preserving charging system for electric vehicles," IEEE Systems Journal, vol. 15, no. 3, pp. 3189–3200, 2021.

[14] S. Basudan, "Federated learning with secure aggregation for privacy preservation in IoE," Computer Communications, vol. 223, pp. 1–14, 2024.

[15] A. M. A. Alamer, "Blockchain-enabled secure data sharing in mobile edge caching systems," Expert Systems with Applications, vol. 237, Article 121572, 2024.

[16] Y. Lin, Y. Jiang, Y. Li, and Y. Zhou, "Batch-based privacy-preserving task assignment in spatial crowdsourcing," Computer Networks, vol. 241, Article 110196, 2024.

[17] Q. Liu et al., "Blockchain-assisted certificateless integrity verification for industrial cloud storage," Journal of Systems Architecture, vol. 140, Article 102898, 2023.

[18] W. Zhang, Z. Wang, and X. Li, "Decentralized federated transfer learning using blockchain for fault diagnosis," Reliability Engineering & System Safety, vol. 229, Article 108885, 2023.

[19] Z. Ou, X. Xing, S. He, and G. Wang, "Trusted data sharing using blockchain with PKI authentication," Computer Communications, vol. 218, pp. 240–252, 2024.

[20] Y. Dong et al., "Consortium blockchain with access control using chameleon hash and attribute-based encryption," High-Confidence Computing, vol. 4, no. 1, Article 100168, 2024.

[21] Y. Harbi et al., "Lightweight blockchain-based authentication for fog-enabled IoT systems," Computer Communications, vol. 221, pp. 90–105, 2024.

[22] H. Si et al., "Cross-chain access control using blockchain and threshold Paillier cryptosystem," Computer Communications, vol. 223, pp. 68–80, 2024.

[23] P. Dadhich and E. Acharya, "Cloud computing applications in vehicular networks for smart ITS design," Internet of Things Applications, pp. 451–465, 2022.

[24] S. Bhattacharya, H. Jha, and R. P. Nanda, "IoT and AI applications in improving road safety," in Proc. Interdisciplinary Research in Technology and Management, 2022, pp. 1–6.

[25] C. Tang, X. Wei, C. Zhu, Y. Wang, and W. Jia, "Using mobile vehicles as fog nodes for latency reduction in smart cities," IEEE Transactions on Vehicular Technology, vol. 69, no. 9, pp. 9364–9375, 2020.