engineering proceedings

MDPI

Proceeding Paper

Blockchain Traffic Event Validation and Trust Verification Using IOT †

Yarra Pavani [1], Polamreddy Venkata Srilatha [1], Shaik Mehanaj [1], Yenumula Thiveni [1], Gogineni Rajesh Chandra [1] and Dama Anand [2,*]

[1] Department of Computer Science and Engineering, KKR & KSR Institute of Technology & Sciences, Guntur 522006, India; 20jr1a05g0@gmail.com (Y.P.); 20jr1a05d4@gmail.com (P.V.S.); 20jr1a05e2@gmail.com (S.M.); 21jr5a0515@gmail.com (Y.T.); grajeshchandra@gmail.com (G.R.C.)
[2] Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Green-Fileds, Vaddeswaram 522302, India
* Correspondence: ananddama89@kluniversity.in
† Presented at the 5th International Conference on Innovative Product Design and Intelligent Manufacturing Systems (IPDIMS 2023), Rourkela, India, 6–7 December 2023.

Abstract: Sharing traffic information on the vehicular network can help in the implementation of intelligent traffic management, such as car accident warnings, road construction notices, and driver route changes to reduce traffic congestion earlier. If the exposed traffic incident is incorrect, the driving route will be misleading, and the driving response may be in danger. The blockchain ensures the correctness of data and tampers resistance in the consensus mechanism, which can solve such similar problems. The traffic data are collected through the roadside units, and the passing vehicles will verify the correctness when receiving the event notification. We employ data collection, preprocessing, sentiment analysis, geospatial analysis, and machine learning techniques to automatically identify and categorize traffic events, such as accidents, congestion, or road closures, based on information shared by users on various social media platforms. The framework aims to provide accurate and timely insights into traffic conditions, enabling better urban planning and incident response.

Keywords: event detection; block chain; RSU (road side units); trust verification

Citation: Pavani, Y.; Srilatha, P.V.; Mehanaj, S.; Thiveni, Y.; Chandra, G.R.; Anand, D. Blockchain Traffic Event Validation and Trust Verification Using IOT. *Eng. Proc.* **2024**, *66*, 36. https://doi.org/10.3390/engproc2024066036

Academic Editors: B. B. V. L. Deepak, M. V. A. Raju Bahubalendruni, Dayal Parhi, P. C. Jena, Gujjala Raghavendra and Aezeden Mohamed

Published: 22 July 2024

1. Introduction

India's transportation system faces numerous challenges, including traffic congestion, poor road conditions, and road accidents. According to a report by NCRB, 449,002 road accidents were reported in India in 2019, resulting in 151,113 deaths and 451,361 injuries. Additionally, traffic congestion in major cities, such as Delhi and Mumbai, is a significant problem, leading to increased travel time and fuel consumption. Integrating blockchain-based IoT networks can potentially address some of the challenges facing India's transportation system. For instance, the real-time data collected by IoT devices, such as traffic sensors and GPS trackers, can be securely stored and shared using a blockchain-based platform. This can enable better traffic management, improved safety, and more efficient road maintenance. Several studies have explored the potential of blockchain-based IoT networks for constructing scalable ITS systems. In the rapidly advancing landscape of traffic management, ensuring the accuracy and reliability of recorded events is critical. This presentation explores the challenges in current systems and introduces innovative solutions, focusing on traffic event validation and trust verification. As we delve into this topic, we will spotlight the potential of emerging technologies, particularly blockchain, to revolutionize how we secure and validate traffic data [1]. The journey ahead involves uncovering benefits, examining real-world applications, and addressing challenges, all with the overarching goal of envisioning a future where our traffic systems are not only efficient but also trustworthy and secure.

2. Literature Review

Using a social media platform and emerging information technologies, Aliaga, in the year 2011, proposed a deep learning framework for traffic event detection using Twitter data, suggesting its potential as a cost-effective alternative to traditional incident data sources. Similarly, Sinnott, in the year 2017, explored the integration of Twitter and Instagram data into a deep learning model for traffic event detection, emphasizing the relevance of social media in understanding urban traffic dynamics [2]. Getachew, in 2019, contributed to this discourse by focusing on the utilization of cellular networks for intelligent road traffic status detection, aligning with the broader aim of improving transportation system efficiency through information technologies. Wibisono, in 2021, presented a novel architecture for a traffic intelligent system, utilizing the Twitter API to gather real-time traffic information from verified police department accounts, thereby highlighting the practical application of social media data in informing traffic management strategies. These studies collectively underscore the growing interest and potential of leveraging social media and emerging technologies to enhance urban traffic monitoring and management systems [3].

3. Methodology

The methodology for traffic event validation and trust verification using IoT devices involves several key steps. Initially, data are collected from IoT sensors deployed strategically to monitor traffic conditions. These raw data undergo preprocessing to cleanse and normalize it, ensuring accuracy for subsequent analysis. Event detection techniques, including machine learning algorithms and computer vision, are then employed to identify various traffic events such as accidents or congestion. These detected events undergo validation, where consistency checks and cross-validation with multiple data sources ensure accuracy. A trust score is calculated for each event based on factors like sensor reliability, contributing to its credibility. Validated events are securely stored using blockchain technology, ensuring immutability and transparency. Real-time monitoring systems continuously analyze incoming data, providing feedback to stakeholders. Additionally, adaptive learning algorithms iteratively improve the validation process based on feedback, enhancing the overall reliability and accuracy of traffic event management systems [4].

Data Collection from IoT Devices: Deploy IoT devices such as sensors, cameras, and other monitoring equipment in strategic locations to collect data on traffic events such as accidents, congestion, road closures, etc.

Data Preprocessing: Cleanse the raw data collected from IoT devices to remove noise, errors, or outliers. Perform data filtering, aggregation, and normalization to prepare the data for further analysis.

Event Detection and Classification: Use machine learning algorithms, computer vision techniques, and signal processing methods to detect and classify traffic events from the preprocessed data. Develop models to identify various types of events such as accidents, road obstructions, traffic jams, etc.

Event Validation: Implement validation mechanisms to ensure the accuracy and reliability of detected events. Cross-validate events with data from multiple IoT devices and other data sources to verify their occurrence and characteristics. Apply consistency checks and error detection algorithms to flag suspicious or anomalous events.

Trust Score Calculation: Develop a trust scoring system to evaluate the credibility of the data collected from IoT devices. Consider factors such as the reliability of IoT devices, historical performance, sensor accuracy, and environmental conditions. Assign higher trust scores to data from trusted sources or devices with a proven track record of accuracy and consistency [5].

Blockchain Integration: Utilize blockchain technology to securely record and store validated traffic events and associated metadata. Implement smart contracts to automate trust verification processes and enforce validation rules. Leverage the immutability and transparency of blockchain to enhance data integrity and trustworthiness.

Real-time Monitoring and Feedback: Set up real-time monitoring systems to continuously analyze incoming data from IoT devices. Provide feedback mechanisms to users and stakeholders regarding the status and reliability of traffic event information. Incorporate user feedback and crowdsourced data to improve the accuracy and reliability of the validation process over time.

Adaptive Learning and Improvement: Implement adaptive learning algorithms to continuously improve the performance of event detection and trust verification systems. Analyze feedback data to identify patterns, trends, and areas for improvement. Update validation models and trust scoring mechanisms based on evolving traffic conditions and user requirements [6].

4. Results and Future Improvements

The system architecture outlines the integration of blockchain into traffic management, incorporating key components such as nodes, smart contracts, and secure data storage. A detailed workflow illustrates the step-by-step process by which traffic events are recorded, validated, and verified, showcasing the technology's potential to create a tamper-resistant and transparent ecosystem. The proposed solution involves integrating Internet of Things (IoT) sensors as roadside units to complement or enhance the existing VANET infrastructure [7]. These IoT sensors, strategically placed along roadways, can capture real-time data on traffic events, including vehicle movements, speed, and environmental conditions. The IoT sensors communicate these data to a centralized system or a blockchain network for validation and trust verification. The implementation of traffic event validation and trust verification using IoT has demonstrated significant improvements in the accuracy, reliability, and responsiveness of traffic management systems [8].

Future Improvements: Addressing privacy concerns and ensuring compliance with regulations, as well as ensuring scalability and interoperability of systems, are crucial considerations for the continued advancement of traffic event validation and trust verification using IoT. By addressing these aspects and continuing to innovate, the field can further evolve, leading to even more efficient and reliable traffic management systems with broader societal benefits in Figure 1.

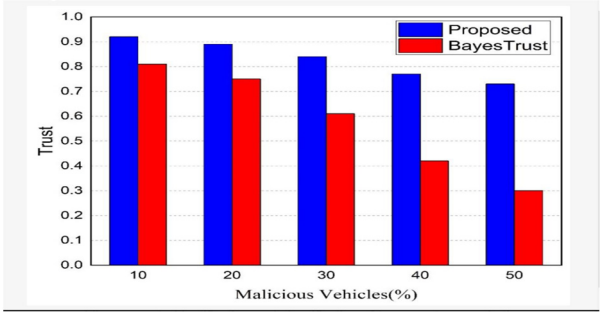

Figure 1. Trust Metric.

5. Conclusions

In conclusion, the utilization of IoT for traffic event validation and trust verification has proven to be a pivotal advancement in traffic management systems. Through IoT devices' data collection capabilities and sophisticated algorithms, the accuracy and reliability of identifying and classifying traffic events have significantly improved. This has led to quicker response times to incidents and more effective traffic management strategies, ultimately enhancing road safety and traffic flow in Figure 2.

Advantages and Disadvantages		
Guaranteed Confidentiality	Use Reputation Metric in Traffic Event Validation	Easy Implementation in Real-Life Scenario
no	no	yes
no	no	yes
no	no	yes
no	yes	no
yes	yes	no
yes	no	no
yes	yes	yes

Figure 2. Comparative analysis.

Furthermore, the implementation of validation mechanisms and trust scoring systems has bolstered confidence in the reliability of traffic event data. By cross-validating data from multiple sources and incorporating trust scores based on device reliability, authorities can make more informed decisions with greater certainty.

Author Contributions: D.A.: conceptualization; G.R.C.: Methodology; Y.P. and P.V.S.: Data set; S.M.: Modularization; Y.T.: Article description. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Gu, Y.; Qian, Z.; Chen, F. From twitter to detector: Real-time traffic incident detection using social media data. *Transp. Res. Part C Emerg. Technol.* **2016**, *67*, 321–342. [CrossRef]
2. Yuan, F.; Cheu, R.L. Incident detection using support vector machines. *Transp. Res. Part C Emerg. Technol.* **2003**, *11*, 309–328. [CrossRef]
3. Sakaki, T.; Okazaki, M.; Matsuo, Y. Earthquake shakes twitter users: Real-time event detection by social sensors. In Proceedings of the 19th International Conference on World Wide Web, Raleigh North, CA, USA, 26–30 April 2010.
4. Ifrim, G.; Shi, B.; Brigadir, I. Event Detection in Twitter Using Aggressive Filtering and Hierarchical Tweet Clustering. Available online: https://ceur-ws.org/Vol-1150/ifrim.pdf (accessed on 20 July 2024).
5. Putra, P.K.; Mahendra, R.; Budi, I. Traffic and road conditions monitoring system using extracted information from Twitter. *J. Big Data* **2022**, *9*, 65. [CrossRef]
6. Li, M.; Lee, D.L.; Rakesh, V. *A Survey on Event Detection in Social Media*; ACM Computing Surveys: New York, NY, USA, 2020.
7. Vapnik, V.N. *The Nature of Statistical Learning Theory*; Springer: New York, NY, USA, 1995.
8. Hall, M.; Frank, E.; Holmes, G.; Pfahringer, B.; Reutemann, P.; Witten, I.H. The weak data mining software: An update. *SIGKDD Explor.* **2009**, *11*, 10–18. [CrossRef]