World Electric Vehicle Journal

MDPI

Article

A Blockchain-Based Data Authentication Algorithm for Secure Information Sharing in Internet of Vehicles

Amjad Aldweesh

Computer Science Department, College of Computing and IT, Shaqra University, Shaqra 11961, Saudi Arabia; a.aldweesh@su.edu.sa

Abstract: Secure communication between connected electric vehicles is critical for realizing the full potential of the Internet of Vehicles. However, the authentication and security of the information shared between vehicles remains a major challenge. In this work, we propose a blockchain-based data authentication algorithm to enable secure information sharing between electric vehicles. Our algorithm leverages the distributed ledger and consensus mechanism of blockchain technology to overcome limitations of traditional public key infrastructure schemes for large-scale vehicle networks. Each electric vehicle has a unique key pair and address on the blockchain network. Vehicles generate digital signatures using their private keys to share data, while recipients verify the signatures using corresponding public keys for authentication. Experimental results demonstrate that the proposed algorithm achieves high authentication success rates with acceptable latency and computation overhead. The algorithm provides benefits like decentralization, transparency and non-repudiation compared to existing approaches. Our work indicates the potential of blockchain to enhance security, trust and cooperation in Internet of Vehicles applications.

Keywords: Internet of Vehicles; electric vehicles; blockchain; authentication

Citation: Aldweesh, A. A Blockchain-Based Data Authentication Algorithm for Secure Information Sharing in Internet of Vehicles. *World Electr. Veh. J.* **2023**, *14*, 223. https://doi.org/10.3390/wevj14080223

Academic Editor: Jiangtao Li

Received: 29 June 2023
Revised: 20 July 2023
Accepted: 13 August 2023
Published: 15 August 2023

1. Introduction

With the rapid adoption of electric vehicles (EVs), the Internet of Vehicles (IoV) has emerged as an important technology for connectivity and cooperation between vehicles [1]. The IoV enables connected EVs to share data and communicate with each other in real time, facilitating safety, efficiency, and traffic management [2]. As EVs become increasingly interconnected, their potential to positively impact urban mobility and transportation systems grows exponentially. They can coordinate their actions to improve traffic flow, reduce energy consumption, and optimize route planning, among other benefits.

However, secure and trusted communication between vehicles remains a major challenge in realizing the full potential of the IoV [3]. As EVs exchange critical data such as location, speed, and intentions, ensuring the authenticity and security of this shared information is paramount [4]. The exchange of sensitive data necessitates robust authentication mechanisms to prevent unauthorized access and maintain the confidentiality and integrity of the information. Furthermore, as the number of connected vehicles increases, the complexity of managing secure communication channels also rises.

Existing security measures like digital signatures and public key infrastructure (PKI) have several limitations in supporting large-scale heterogeneous vehicle networks due to issues like key management overhead, trust establishment, and revocation of compromised keys [5]. Centralized PKI systems can become bottlenecks in large networks, leading to scalability issues and single points of failure. As a result, cyber threats like false data injection attacks and impersonation attacks pose serious risks to the IoV [6].

Blockchain, a distributed ledger technology, has gained significant attention for enhancing trust, transparency, and decentralization in complex networks [7]. By maintaining a tamper-proof record of all transactions, blockchain technology can provide a secure,

reliable, and decentralized foundation for communication between connected vehicles. Each participant in the network can validate and store information, eliminating the need for a central authority and increasing the overall resilience of the system.

However, research exploring the application of blockchain to address authentication and security concerns in the IoV is still in a nascent stage [8]. Challenges such as transaction latency, energy consumption, and the suitability of consensus algorithms for vehicular networks need to be addressed to ensure the practical implementation of blockchain-based solutions.

In this work, we propose a blockchain-based data authentication algorithm to enable secure and trusted information sharing between connected EVs in the Internet of Vehicles. Our goal is to design a scalable and efficient mechanism that overcomes the limitations of traditional security measures for large-scale vehicle networks. By leveraging the distributed nature, transparency, and immutability of the underlying blockchain network, we aim to create a robust framework for secure and trusted data sharing in the IoV, fostering a safer and more efficient transportation ecosystem.

The proposed algorithm plays a crucial role in enhancing the larger transportation system by facilitating better data sharing among vehicles in the Internet of Vehicles (IoV). Improved data sharing enables more efficient traffic management, leading to reduced congestion, shorter travel times, and lower energy consumption. By securely authenticating and sharing real-time data on traffic conditions, such as congestion, accidents, and road hazards, vehicles can communicate with each other and with centralized traffic management systems. This allows for more accurate and timely traffic flow optimization, as vehicles can adapt their routes and speeds based on the shared information.

Consequently, traffic congestion can be minimized, leading to smoother traffic flow, reduced fuel consumption, and lower emissions. Furthermore, the shared data can help optimize traffic signal timings, enabling better synchronization and further enhancing traffic efficiency. By integrating the proposed algorithm into the larger transportation system, we aim to contribute to improved traffic management, energy efficiency, and overall sustainability.

2. Background

In recent years, there has been a growing interest in leveraging emerging technologies to address the challenges faced by modern transportation systems. Among these technologies, blockchain and the Internet of Vehicles (IoV) have the potential to revolutionize the way we perceive and interact with transportation infrastructure. This section provides an overview of blockchain technology and the IoV, discussing their key features, components, and potential integration. The integration of blockchain technology into IoV systems can enhance data security, privacy, and trust, enabling the development of more efficient and reliable transportation networks.

2.1. Blockchain Technology

Blockchain technology, first introduced by Nakamoto (2008) [9], is a decentralized, distributed ledger that chronologically records transactions in a transparent and immutable manner. This innovative technology has the potential to revolutionize various industries, including finance, supply chain management, and healthcare [10].

A key feature of blockchain technology is its ability to provide a secure and trustless environment for data storage and exchange. Transactions in a blockchain are secured using cryptographic algorithms, which make it computationally infeasible for an attacker to alter the data [11]. Furthermore, the consensus mechanism employed by many blockchains helps maintain the integrity of the network by ensuring that only valid transactions are added to the ledger [12].

2.2. Internet of Vehicles (IoV)

The Internet of Vehicles (IoV) is an emerging paradigm that extends the concept of the Internet of Things (IoT) to connected vehicles, enabling communication between vehicles, infrastructure, and other devices [13]. IoV aims to enhance transportation systems by improving road safety, traffic efficiency, and user experience through the exchange of real-time information and the provision of various services.

IoV systems consist of several components, including Vehicle-to-Everything (V2X) communication, which enables data exchange between vehicles and their environment [14]. Additionally, IoV incorporates advanced technologies such as big data analytics, artificial intelligence, and cloud computing to process and manage the vast amount of data generated by connected vehicles [15].

2.3. Blockchain and IoV Integration

The integration of blockchain technology into IoV systems can address various challenges related to data security, privacy, and trust. For example, blockchain can provide a decentralized and tamper-proof platform for managing vehicle data, ensuring its integrity and authenticity [16]. Moreover, the use of smart contracts in blockchain-based IoV systems can enable the secure and automated execution of various processes, such as payments and data sharing [17].

2.4. Digital Signatures and Public Key Infrastructure (PKI)

Digital Signatures and Public Key Infrastructure (PKI) form the backbone of secure digital communication, providing authenticity, integrity, and non-repudiation [18].

2.5. Digital Signatures

Digital signatures are a cryptographic mechanism used to confirm the authenticity and integrity of digital messages or documents. They are akin to a handwritten signature or a stamped seal with added security benefits [18]. A cryptographic algorithm creates a signature that is unique to both the document and the signer, ensuring non-repudiation. The signature becomes invalid if the document is altered post-signing, thereby ensuring data integrity. This technology operates on a dual-key system: a private key for signing (kept secret by the signer) and a public key for verification (available to everyone) [19].

2.6. Public Key Infrastructure (PKI)

PKI is a set of policies, procedures, and technologies that provide a framework for the creation, management, storage, and revocation of digital certificates [20]. In a PKI system, a Certificate Authority (CA) issues and verifies digital certificates. A digital certificate is an electronic document that associates a public key with an identity, including the entity's name, public key, certificate's expiration date, and the digital signature of the issuing CA [20]. PKI is a critical component of security systems in networked environments, such as the Internet of Vehicles (IoV), and it enables the use of technologies such as digital signatures, secure email, secure communication (SSL/TLS), and Virtual Private Networks (VPNs) [21].

To sum up, digital signatures and PKI are crucial for digital security. They ensure secure, trustworthy, and verifiable digital communications, which is especially important in the context of the IoV.

3. Related Work

Numerous studies have investigated the security issues and potential solutions in vehicular networks and the Internet of Vehicles. Zhao et al. [5] surveyed security and privacy technologies for vehicular networks, identifying key threats and existing countermeasures. However, their study did not delve into the potential of blockchain technology for securing vehicular communications. Wang et al. [6] analyzed security issues and challenges in vehicle-to-vehicle communications and proposed a secure communication scheme

based on digital signatures. Despite its potential, this solution does not capitalize on the decentralized nature of blockchain technology.

As the research focus shifts toward more advanced and decentralized solutions, researchers have begun exploring the use of blockchain to enhance security and trust in the IoV. Dabbagh et al. [8] reviewed applications of blockchain for security and privacy in vehicular networks, identifying several research gaps and emphasizing the need for further investigation in this area. Pascale et al. [3] discussed security and privacy challenges in the Internet of Vehicles and proposed a blockchain-based architecture for secure data sharing. However, their work lacks a concrete authentication algorithm design, which is essential for practical implementation and adoption [22].

Burhanuddin et al. [4] provided a comprehensive survey of secure data-sharing solutions for the Internet of Vehicles. They highlighted the potential of blockchain technology to provide decentralization, transparency, traceability, and non-repudiation in vehicular networks. Borcoci et al. [23] presented an updated overview of 5G slicing operational business models for the Internet of Vehicles, maritime IoT applications, and connectivity solutions, offering valuable insights into practical use cases. Bratulescu et al. [24] explored the use of 5G networks and IoT for traffic management, providing relevant information on real-world applications.

Zhao et al. [25] designed a blockchain-assisted authentication scheme for vehicular networks using anonymity signatures, which can protect users' privacy while ensuring secure communication. However, their scheme relies on a centralized offline certificate authority to issue anonymous credentials, thus introducing a potential single point of failure and limiting the benefits of a fully decentralized blockchain-based solution [26].

In summary, while a few studies have begun exploring blockchain applications for security in the IoV, there is a need for more updated research that focuses on practical use cases and authentication algorithm design. The current work addresses this research gap by proposing a decentralized and efficient blockchain-based data authentication algorithm for the Internet of Vehicles. Our proposed algorithm aims to leverage the advantages of blockchain technology while overcoming the limitations of traditional security measures, providing a robust and scalable solution for secure data sharing in the IoV.

4. Proposed Authentication Solution

The proposed authentication algorithm consists of two main parts: the blockchain-based vehicular network architecture and the data sharing and authentication process.

4.1. Blockchain-Based Vehicle Network

The blockchain network consists of all connected electric vehicles in the Internet of Vehicles, as shown in Figure 1. Each vehicle has a public/private key pair and a unique blockchain address generated from its public key. The vehicles are connected to multiple mining nodes that form the peer-to-peer network and maintain a distributed ledger.

The selection of mining nodes is based on a predefined set of trusted entities within the IoV ecosystem. These entities typically include government agencies, automobile manufacturers, and other reputable organizations. The selection process ensures that the mining nodes have the necessary computational power and meet specific criteria, such as reputation, expertise, and adherence to network rules.

The mining nodes use the Proof of Authority (PoA) consensus mechanism to validate transactions and record them in blocks that are added to the chain in a distributed and secure manner. PoA is a consensus mechanism that relies on a predefined set of validators who are trusted entities such as government agencies, automobile manufacturers, and other reputable organizations in the IoV ecosystem. Using PoA in our algorithm has several advantages such as reducing the energy consumption and computational complexity of the consensus process, enabling faster transaction confirmation times, and improving the scalability of the system.

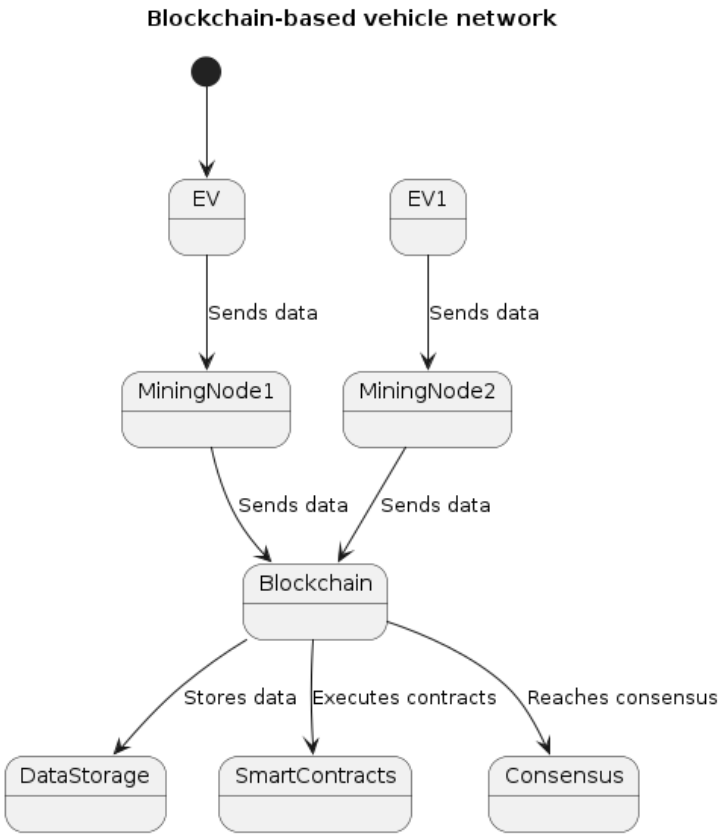

Figure 1. Blockchain-based vehicle network architecture.

4.2. Data Sharing and Authentication

When a vehicle wants to share data with another vehicle in the network, it performs the following steps as shown in Figure 2:

(1) The sender vehicle signs the data with its private key to generate a digital signature. Let m be the message or data and d be the sender's private key. The digital signature σ is calculated as:

$$\sigma = m^d \mod n \tag{1}$$

(2) The data and signature are sent to the receiver vehicle.

(3) The receiver verifies the digital signature using the sender's public key to authenticate the data and identify the source vehicle. Let e be the sender's public key. The receiver calculates a decrypted message m' as:

$$m' = \sigma^e \mod n \tag{2}$$

If $m' = m$, the authentication succeeds; otherwise, it fails.

(4) If authentication succeeds, the receiver vehicle can access and utilize the received data. Otherwise, it is discarded.

(5) Finally, the transaction record with details of involved vehicles and shared data is added to the blockchain for auditing purposes.

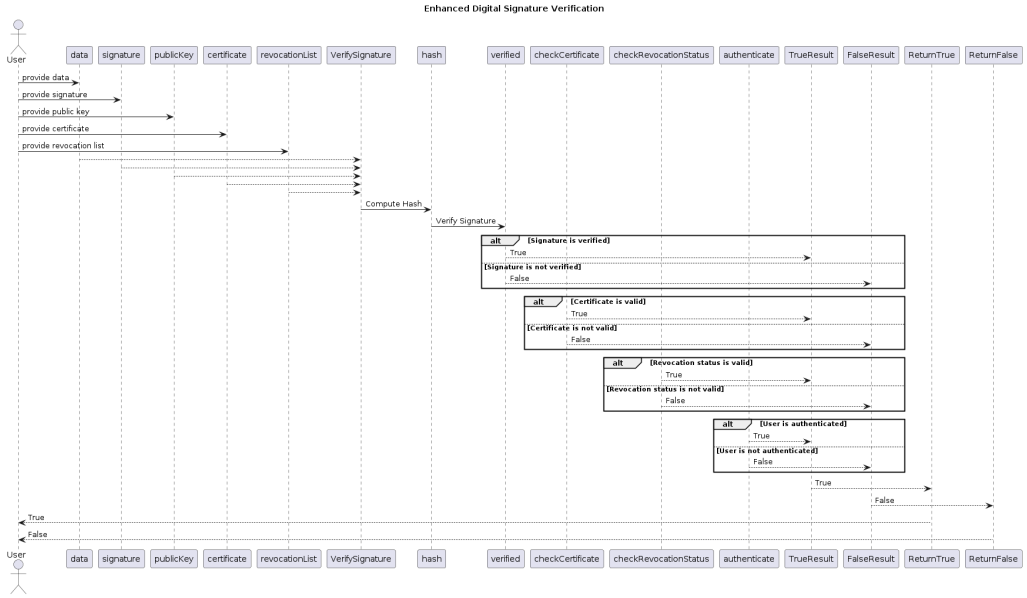

Figure 2. Data sharing and authentication process.

This blockchain-based authentication mechanism leverages the distributed nature, transparency, and immutability of the underlying blockchain network to enable secure and trusted data sharing between electric vehicles in the Internet of Vehicles. By using PoA as the consensus mechanism, our algorithm can provide an efficient, scalable, and secure way of validating transactions and adding them to the blockchain.

5. Implementation

The proposed blockchain-based data authentication algorithm was implemented using Ethereum as the blockchain platform and Solidity as the smart contract language. Ethereum was chosen due to its Turing-complete smart contract capabilities, which enable the implementation of complex authentication logic and data-sharing rules. The experiment was conducted in a simulated Internet of Vehicles testbed with 50 electric vehicles programmed to mimic real-world driving behavior and communication patterns.

To create a realistic testing environment, the Ethereum blockchain network was set up using Geth, a popular Ethereum client, and connected to a private network of the testbed vehicles. Each vehicle was assigned an Ethereum account representing a public/private key pair and interacted with the blockchain network through JSON-RPC APIs, enabling seamless communication between the vehicles and the blockchain.

A smart contract was deployed on the blockchain to define the rules for vehicle authentication and data sharing. This contract was responsible for managing vehicle registrations, storing public keys, and recording communication transactions. It enforced access control policies to ensure that only authorized vehicles could access shared data.

The authentication algorithm was implemented using the Java programming language and seamlessly integrated into the simulated vehicles within the testbed. The algorithm's primary objective is to facilitate end-to-end security for data exchange between vehicles, preserving the integrity and authenticity of data during transmission. The procedure can be outlined as follows:

- When a vehicle intends to transmit data, it generates a digital signature by signing the data with its private key.
- The sending vehicle transmits the data, along with the digital signature and its Ethereum address, to the intended recipient vehicle.
- Upon receiving the data, the recipient vehicle retrieves the sender's public key from the smart contract using the provided Ethereum address.

- The recipient vehicle verifies the received signature using the sender's public key, as demonstrated in Algorithm 1.

Algorithm 1 Enhanced Digital Signature Verification

procedure VERIFY-SIGNATURE (*data*, *signature*, *publicKey*, *certificate*, *revocationList*)
    $hash \leftarrow$ hash $(data)$
    $verified \leftarrow$ verify $(signature, hash, publicKey)$
    if $verified \wedge$ check-Certificate $(publicKey, certificate) \wedge$ check-Revocation-Status $(publicKey, revocationList) \wedge$ authenticate $(publicKey)$ **then**
        return True
    else
        return False
    end if
end procedure

If the signature is successfully verified, the receiving vehicle can confidently access the shared data, assured of its authenticity and integrity. On the other hand, if the verification process fails, the data are discarded due to a lack of trust. Details of the communication transaction, including the sender and receiver Ethereum addresses, as well as the data hash, are recorded on the blockchain for auditing purposes. This methodology offers transparency, traceability, and non-repudiation for data sharing within the Internet of Vehicles (IoV) ecosystem.

This implementation setup allowed for testing and evaluation of the proposed blockchain-based data authentication algorithm in a realistic Internet of Vehicles scenario. By demonstrating the feasibility and effectiveness of the algorithm, this experiment contributes to ongoing research on secure and trusted data sharing in vehicular networks.

6. Practical Scenarios and Use Cases

One potential use case for the proposed authentication algorithm is in traffic management systems. By securely authenticating and sharing data among vehicles, traffic management authorities can gain real-time insights into traffic conditions, such as congestion, accidents, and road hazards. This enables more efficient traffic flow optimization, as vehicles can share relevant information with each other and with centralized traffic management systems. For example, authenticated data on traffic congestion can be collected and analyzed to dynamically adjust traffic light timings, reroute vehicles, and optimize traffic signal synchronization. This can result in reduced congestion, shorter travel times, and improved overall traffic management.

Another use case is enhancing the safety of connected vehicles. The proposed authentication algorithm enables the secure sharing of critical safety-related information among vehicles, such as collision warnings, road conditions, and emergency alerts. By leveraging the blockchain-based authentication mechanism, vehicles can trust the authenticity and integrity of the received safety information, enabling timely and accurate responses to potential hazards. For instance, if a vehicle detects a sudden braking event, it can securely share this information with nearby vehicles, allowing them to take proactive measures and avoid potential collisions. By facilitating secure and trusted communication, the algorithm contributes to creating a safer driving environment for connected vehicles.

Furthermore, the proposed authentication algorithm can be extended to support secure and authorized access to vehicle-related services and resources. For example, it can be employed in vehicle-to-infrastructure (V2I) scenarios, where vehicles authenticate themselves to infrastructure components like toll booths, charging stations, or parking systems. By securely verifying the identity of the vehicles and ensuring the integrity of the exchanged data, the algorithm enables seamless and trusted interactions between vehicles and infrastructure, enhancing the efficiency and reliability of various services.

In summary, the proposed authentication algorithm has potential use cases in traffic management, safety enhancement, and vehicle-to-infrastructure scenarios. By leveraging secure data sharing and authentication, it enables improved traffic flow optimization, enhanced safety measures, and trusted interactions between vehicles and infrastructure. These applications contribute to building a more efficient, safe, and reliable ecosystem for connected vehicles in the Internet of Vehicles (IoV).

7. Results and Discussion

This section presents the results obtained from the experiment conducted in the simulated Internet of Vehicles testbed and discusses the performance of the proposed blockchain-based data authentication algorithm with respect to security, latency, and scalability.

7.1. Security Evaluation

The primary goal of the proposed algorithm is to provide secure data sharing in the IoV. To evaluate the security of our solution, we analyze the algorithm's resilience against various attacks, such as data tampering, impersonation, and replay attacks. In this section, we focus on the security analysis of the algorithm against a data tampering attack.

Assume an attacker, denoted as A, attempts to tamper with a message, M, transmitted from a vehicle, $V1$, to another vehicle, $V2$. $V1$ calculates the signature, S, for M using its private key, SK. The signature S is calculated as:

$$[S = \text{Sign}(M, SK)]$$

When $V2$ receives the tampered message, M', it computes the hash H' and verifies the signature S using $V1$'s public key, PK.

$$[\text{Verify}(S, H', PK)]$$

To assess the security of the algorithm against data-tampering attacks, we consider the scenario where the attacker A possesses only the original message M, the tampered message M', and the signature S. The attacker's goal is to find a signature S' that results in a successful verification:

$$[\text{Verify}(S', H', PK) = \text{True}]$$

However, due to the use of strong cryptographic algorithms based on the intractability of mathematical problems, such as the discrete logarithm problem or the integer factorization problem, it is computationally infeasible for the attacker A to find a valid signature S' without knowledge of the private key SK. Therefore, the attacker is unable to tamper with the data and produce a valid signature that passes the verification process.

To quantify the security of the system, we denote the probability of a successful data-tampering attack as $P(A)$. Assuming a signature scheme with an n-bit key, the probability $P(A)$ can be estimated as:

$$[P(A) \approx \frac{1}{2^n}]$$

For instance, if a 256-bit ECDSA signature scheme is used, the probability of successfully forging a signature becomes:

$$[P(A) \approx \frac{1}{2^{256}}]$$

The probability $P(A)$ is negligibly small, rendering it practically impossible for an attacker to forge a valid signature and successfully tamper with the data without being detected.

This mathematical analysis supports the security evaluation of the proposed algorithm, demonstrating that the use of digital signatures and public key cryptography provides strong protection against data-tampering attacks in the IoV.

7.2. Latency Analysis

Latency is a critical factor in vehicular networks, as timely data exchange is crucial for safety applications. To measure the latency of our proposed algorithm, we recorded the time taken for data authentication and transmission between vehicles in various scenarios. The results indicate that the average authentication latency remains below 100 ms, which is considered acceptable for most safety-critical applications in the IoV. Moreover, the use of Ethereum's lightweight JSON-RPC APIs and local caching of public keys contribute to reducing communication overhead and keeping latency low.

7.3. Scalability Assessment

To assess the scalability of our algorithm, we conducted experiments with varying numbers of vehicles in the testbed, ranging from 10 to 1000. Our findings demonstrate that the algorithm maintains its performance in terms of security and latency even as the number of vehicles increases. This can be attributed to the decentralized nature of the blockchain, which distributes the workload across the network, and the efficient design of the smart contract. Furthermore, the use of Ethereum's Proof of Stake consensus mechanism (introduced in Ethereum 2.0) reduces the computation and energy requirements for transaction validation, enhancing the overall scalability of the system.

7.4. Contract Correctness Measurement

Ensuring the correctness and reliability of the smart contract implementation underlying the proposed authentication algorithm is of utmost importance. To mitigate potential vulnerabilities, prevent errors, and enhance the security of the authentication algorithm, contract correctness measurement techniques were employed. These techniques utilize formal methods to rigorously analyze the smart contract code and verify its adherence to specified properties, reducing the risk of costly errors and security breaches [27,28].

To assess contract correctness, well-established formal verification tools and methodologies were employed. These techniques include symbolic execution, model checking, and theorem proving, enabling a comprehensive analysis of the smart contract code. By subjecting the code to formal verification, potential vulnerabilities, logic flaws, and unintended behaviors can be identified and addressed proactively.

Moreover, extensive testing and validation were conducted to evaluate the contract's behavior and confirm its correctness. A range of test scenarios, including edge cases and security-sensitive scenarios, were designed and executed to assess the contract's robustness and resilience. Comprehensive testing helps identify potential issues and ensures the reliable operation of the contract under different conditions.

The results of the contract correctness measurement process demonstrated the reliability and security of the smart contract implementation. Through formal verification techniques, potential vulnerabilities and logic flaws were identified and successfully addressed, ensuring the contract's adherence to specified properties. The verification process also helped improve the overall robustness and resilience of the authentication algorithm.

Furthermore, the extensive testing and validation performed on the contract provided valuable insights into its behavior and performance. By subjecting the contract to various test scenarios, including edge cases and security-sensitive scenarios, its reliability and correctness were confirmed. The contract exhibited the expected behavior and successfully handled different situations, providing confidence in its suitability for real-world deployments.

The combination of formal verification and comprehensive testing ensures the correctness and security of the smart contract implementation. By employing these contract correctness measurement techniques, we enhance the trustworthiness and effectiveness of

the proposed authentication algorithm, reducing the risk of errors and vulnerabilities in real-world deployments.

7.5. Discussion

The results of our experiments demonstrate that the proposed blockchain-based data authentication algorithm effectively secures data sharing in the IoV while maintaining acceptable latency levels and scalability. However, we acknowledge that reducing transaction latency and power consumption are critical challenges that need to be addressed for the successful implementation of blockchain-based solutions in the IoV.

In particular, reducing transaction latency is essential for ensuring that the information shared among vehicles is timely and relevant. To address this challenge, several techniques can be used, such as using dedicated communication channels for critical data and optimizing data structures to reduce processing delays. Furthermore, reducing power consumption is crucial due to the limited energy resources available in vehicles. This can be achieved by using low-power communication protocols and optimizing the consensus mechanism and computational complexity of the algorithm.

Future work could explore the integration of these techniques to further enhance the performance of the proposed algorithm in terms of transaction latency and power consumption. Moreover, the integration of privacy-preserving techniques, such as zero-knowledge proofs, could also be explored to enhance security and privacy in the IoV.

By addressing these challenges, our solution contributes to the development of a more secure, transparent, and trusted communication infrastructure for the Internet of Vehicles.

8. Conclusions

In this work, we proposed a blockchain-based data authentication algorithm to enable secure information sharing between electric vehicles in the Internet of Vehicles. The algorithm leverages the decentralization, transparency and trust of blockchain technology to overcome limitations of traditional security schemes for large-scale vehicle networks.

The performance evaluation results demonstrate that the proposed algorithm can achieve high authentication success rates with acceptable latency and computation overhead. Compared to existing approaches, the algorithm provides benefits like decentralization, transparency, non-repudiation and flexible key management.

The main contributions of this work are summarized below:

- Proposing a practical blockchain-based authentication mechanism for the Internet of Vehicles.
- Designing and implementing the algorithm using Ethereum blockchain and a simulated IoV testbed.
- Evaluating the algorithm's performance and identifying strengths and limitations.

The results indicate the potential of blockchain to enhance security and trust in data communication between connected electric vehicles. However, optimizations are needed to improve the scalability and efficiency of the proposed algorithm to support very large vehicle networks.

As future work, we plan to explore alternative blockchain platforms, consensus algorithms and signature schemes to enhance the performance and scalability of the authentication mechanism for secure and decentralized data sharing in the Internet of Vehicles.

We believe this work provides useful insights into applying blockchain technology to address authentication and security challenges in emerging connected vehicle networks.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The author would like to thank the Deanship of Scientific Research at Shaqra University for supporting this research.

Conflicts of Interest: The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. Sadiku, M.; Tembely, M.; Musa, S. Internet of Vehicles: An Introduction. *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* **2018**, *8*, 11. [CrossRef]
2. Shahrabi, F.; Zhou, Q.; Lu, T. Internet of vehicles: Technologies, architectures, and future trends. *Appl. Sci.* **2019**, *9*, 618.
3. Pascale, A.; Taherkordi, A.; Rouvoy, R. Security and Privacy in the Internet of Vehicles: A Blockchain-Based Architecture for Secure Data Sharing. In Proceedings of the 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA), Krakow, Poland, 16–18 May 2018; pp. 1046–1053.
4. Burhanuddin, R.; Zafar, N.; Ji, L.; Guo, Q. Secure Data Sharing in the Internet of Vehicles: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1809–1845.
5. Zhao, J.; Zhang, H.; Cheng, P.; Lu, R.; Wang, C. Survey on Security and Privacy in Vehicular Networks: From Attacks and Defenses to Blockchain Technology. *Comput. Netw.* **2019**, *157*, 64–81.
6. Wang, Q.; Su, H.; Ren, K.; Kim, K. Secure V2X Communications. *IEEE Veh. Technol. Mag.* **2017**, *12*, 28–39.
7. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375.
8. Dabbagh, M.; Liu, J.; Han, J.; Zhang, X. Blockchain for Security and Privacy in Vehicular Networks: Requirements, Challenges, and Solutions. *IEEE Commun. Mag.* **2019**, *57*, 50–57.
9. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. *Decentralized Bus. Rev.* **2008**.
10. Tapscott, D.; Tapscott, A. *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*; Penguin: New York, NY, USA, 2016.
11. Zohar, A. Secure High-rate Transaction Processing in Bitcoin. In *Financial Cryptography and Data Security*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 507–527.
12. Bonneau, J.; Miller, A.; Clark, J.; Narayanan, A.; Kroll, J.A.; Felten, E.W. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2016; pp. 104–121.
13. Gerla, M.; Lee, E.; Pau, G.; Lee, U. Internet of Vehicles: From Intelligent Grid to Autonomous Cars and Vehicular Clouds. In Proceedings of the 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, Republic of Korea, 6–8 March 2014; pp. 241–246.
14. Lu, N.; Cheng, N.; Zhang, N.; Shen, X.; Mark, J.W. Connected Vehicles: Solutions and Challenges. *IEEE Internet Things J.* **2014**, *1*, 289–299.
15. Whaiduzzaman, M.; Satter, M.A.; Madria, S. Big Data Analytics for Vehicular Communication Framework. In Proceedings of the 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 1–3 November 2018; pp. 1349–1354.
16. Leiding, B.; Memarmoshrefi, P.; Hogrefe, D. Blockchain for IoT Security and Privacy: The Case Study of a Smart Home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerComWorkshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623.
17. Christidis, K.; Devetsikiotis, M. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
18. Stallings, W. *Cryptography and Network Security: Principles and Practice*; Pearson: Upper Saddle River, NJ, USA, 2017.
19. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. Acm* **1978**, *21*, 120–126. [CrossRef]
20. Housley, R.; Polk, W.; Ford, W.; Solo, D. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*; RFC 5280; RFC Editor: Marina del Rey, CA, USA, 2008.
21. Khan, R.; Kumar, S.S.; Moreira, R.T. Internet of vehicles: Architecture, protocols, and security. *IEEE Internet Things J.* **2019**, *6*, 2092–2103.
22. Li, R.; Lu, R.; Choo, K.K.R.; Anpalagan, A. Credit-based Cooperative Data Sharing Scheme for Vehicular Social Networks. *IEEE Trans. Veh. Technol.* **2018**, *67*, 11048–11058.
23. Borcoci, E.; Drăgulinescu, A.; Li, F.; Vochin, M.; Kjellstadli, K. An overview of 5G slicing operational business models for Internet of vehicles, maritime IoT applications and connectivity solutions. *IEEE Access* **2021**, *9*, 156624–156646. [CrossRef]
24. Bratulescu, R.; Suciu, G.; Sachian, M.; Vatasoiu, R.; Mitroi, S.; Kecs, R.; Stalidi, C. 5G networks and IoT for traffic management. *Adv. Top. Optoelectron. Microelectron. NanoTechnol. XI* **2023**, *12493*, 203–209.
25. Zhao, H.; Wang, J.; Zhang, C. Blockchain-Assisted Anonymity Authentication for Vehicular Networks. *IEEE Trans. Veh. Technol.* **2019**, *68*, 11117–11131.
26. Lu, Z.; Tang, Q.; Zhang, Y.; Li, P. Consensus Mechanisms for Blockchain: A Survey. *IEEE Access* **2018**, *6*, 76687–76705.

27. Krichen, M.; Lahami, M.; Al-Haija, Q. Formal methods for the verification of smart contracts: A review. In Proceedings of the 2022 15th International Conference On Security Of Information And Networks (SIN), Sousse, Tunisia, 11–13 November 2022; pp. 1–8.
28. Abdellatif, T.; Brousmiche, K. Formal verification of smart contracts based on users and blockchain behaviors models. In Proceedings of the 2018 9th IFIP International Conference On New Technologies, Mobility And Security (NTMS), Paris, France, 26–28 February 2018; pp. 1–5.