RESEARCH ARTICLE

Enhancing Authentication Security in Internet of Vehicles: A Blockchain-Driven Approach for Trustworthy Communication

Muhammad Hassnain Ali Haider[1], Muhammad Fayaz[2], Yue Zhang[2], Haseena Noureen[3], Zeeshan Ali Haider[4,*], Fida Muhammad Khan[4], Inam Ullah Khan[4] and Md Moklesur Rahman[5]

[1] Department of Electrical Engineering, Sarhad University of Science & Information Technology, 25000 Peshawar, Pakistan
[2] Department of Computer Science and Engineering, Sejong University, Seoul 05006, South Korea
[3] Department of Computer Science and Information Technology, University of Malakand, Malakand 23050, Pakistan
[4] Department of Computer Science, Qurtuba University of Science and Information Technology, Peshawar 25000, Pakistan
[5] IMT Atlantique, 655 Avenue du Technopôle, 29280 Plouzané, France

Abstract

The Internet of Vehicles (IoVs) is an emerging technology that enhances transportation systems by enabling interactions between vehicles, infrastructure, and other entities. Securing IoV networks from cyber threats like eavesdropping, data tampering, and intrusions is a major challenge. This research presents a Blockchain-Enabled Secure Authentication Protocol for IoVs (BESA-IOV), which leverages blockchain's decentralized and tamper-resistant nature for secure communication in vehicular networks. By utilizing ECC-based lightweight cryptography and blockchain-based public key management, it ensures strong authentication, confidentiality, and integrity. The results show that BESA-IOV significantly reduces authentication delay and computational cost compared to protocols such as NOTSA, RVAC, VANET-Auth, and SecureIoV. Extensive simulations indicate that BESA-IOV reduces authentication delay by 35% and computational overhead by 40%, enhancing real-time communication in the IoV environment. BESA-IOV is secure, efficient, and scalable for next-generation IoV systems.

Keywords: internet of vehicles (IoV), blockchain-enabled secure authentication protocol (BESA), blockchain, secure authentication.

1 Introduction

The Internet of Vehicles (IoVs) modifies the most important aspect of transportation systems and has brought some changes to computing, which can better solve the problems of transportation systems in terms of safety, efficiency, and

Submitted: 26 February 2024
Accepted: 22 March 2024
Published: 31 March 2024

Vol. 1, **No.** 1, 2024.
10.62762/TACS.2024.835144

***Corresponding author:**
✉ Zeeshan Ali Haider
Zeeshan.ali9049@gmail.com

Citation
Haider, M. H. A., Fayaz, M., Zhang, Y., Noureen, H., Haider, Z. A., Khan, F. M., Khan, I. U., & Rahman, M. M. (2024). Enhancing Authentication Security in Internet of Vehicles: A Blockchain-Driven Approach for Trustworthy Communication. *ICCK Transactions on Advanced Computing and Systems*, 1(1), 48–62.

intelligence. Vehicle-to-Everything (V2X) communication (including Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication) are at the core of future IoVs, and these networks are currently being expanded on top of classical Vehicular Ad Hoc Networks (VANETs) [1, 2]. These advancements pave the way for real-time information exchange between vehicles, infrastructure, and the cloud, underpinning essential applications such as self-driving vehicles, traffic optimization, and emergency notifications [3, 4]. Due to their open nature, vehicular communication networks are vulnerable to various security threats such as eavesdropping, data corruption, and attacks that compromise the confidentiality and availability of communication, etc.

A scalable and secure authentication scheme is one of the most challenging requirements for impactful communication security in IoVs [5]. The dynamic features of vehicular networks, such as high mobility, dynamic network topology, and limited resources, make it challenging for the existing security protocols [6, 7]. Centralized solutions are vulnerable to single points of failure and may not scale as necessary for massive-scale deployments of IoVs [8, 9]. Furthermore, conventional authentication schemes also introduce a high computational overhead that causes latency and inefficiency, degrading the performance of real-time Internet of Vehicles (IoV) applications.

These challenges find a promising solution with the decentralized, transparent, and tamper-proof nature of Blockchain technology. Blockchain provides a decentralized and secure ledger, ensuring message authenticity and integrity in IoV networks while eliminating reliance on a central authority. Moreover, consensus mechanisms on the blockchain support scalable authentication without involving significant computational capabilities, thus making blockchain technology ideally fit for use in the IoV ecosystem. Figure 1 shows the Internet of Vehicles (IoV) ecosystem with Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Roadside Unit (V2R), and Vehicle-to-Grid (V2G) communications. This fig also highlights that cloud servers, trusted authority, and blockchain play a role in securing and managing communication in the case of IoV.

This paper presents a new Blockchain-Enabled Secure Authentication Protocol for IoVs (BESA-IOV). The proposed protocol exploits blockchain intelligent contract features with the aim of offering a lightweight, efficient, and secure authentication mechanism that reduces communication overhead and ensures data privacy and integrity. In this paper, we perform a comprehensive analysis of the BESA-IOV's performance against existing authentication protocols and show that it provides improved authentication delay, scalability, and security. We demonstrate that our proposed BESA-IOV is a promising approach for next-generation IoVs via simulation and experimental validation, increasing the trustworthiness and security of communication among vehicles in vehicular networks.

This manuscript contributes to the relevant details below:

1. We present a new lightweight, secure authentication protocol—Blockchain-Enabled Secure Authentication Protocol for IoVs (BESA-IOV) for IoVs.
2. We analyze the performance of BESA-IOV via extensive simulations and show its scalability and security and that it has a low computational overhead.
3. We compare the BESA-IOV protocol to the existing IoV authentication approaches and prove that it outperforms them in terms of authentication time, communication cost, and scalability.
4. We discuss how blockchain can be used for security communication and can also resolve security challenges that might arise because of ever-increasing IoVs deployments.

The remaining part of the paper is structured as follows: Section 2 presents a detailed survey of vehicle authentication schemes in IoV systems, emphasizing their drawbacks and implications for enhanced solutions. Section 3 discusses the proposed Blockchain-Enabled Secure Authentication Protocol for IoVs (BESA-IOV), including its architecture and components. In Section 4, we provide a performance evaluation of the BESA-IOV protocol through simulations, as well as comparisons with existing IoV authentication schemes in terms of important aspects such as scalability, communication efficiency, and authentication delay. Lastly, Section 5 concludes the paper with the contributions and implications of the proposed protocol toward IoV security while also discussing future research directions for improving the scalability and security of blockchain-based

authentication systems in vehicular networks.

2 Related Work

The Internet of Vehicles (IoVs) is one of the most promising applications of Internet of Things (IoT) technologies and causes a paradigm shift in the transportation domain toward improved safety, efficiency, and intelligence [10, 11]. Since IoVs allow interaction between vehicles, infrastructure, and other actors, guaranteeing secure communication has been one of the main issues [12]. The fact that only legitimate vehicles and infrastructure can send messages to each other and malicious agents are excluded from accessing the communication medium makes authentication one of the fundamental components for securing IoV systems.

Vehicular networks commonly utilize certificate-based authentication methods, with vehicles preloaded with digital certificates issued by a trusted authority [13], to verify the identity of the vehicles and secure communications [14, 15]. Certificates also incur considerable costs here because of the overhead to create, distribute, and verify certificates, representing a serious scalability challenge for certificate-based protocols [16]. Furthermore, they usually fail to respond to the changes in an IoV network where vehicles continuously enter and exit the network [17]. Some privacy-preserving authentication systems employ pseudonyms to protect vehicle identity in a cooperative communication environment [18]. But sure, these protocols enhance privacy, they're not without challenges, particularly in the management of securely updating pseudonyms to avoid identity correlation [19, 20]. However, these protocols face scalability issues and require further optimization, especially when it comes to large-scale IoV deployments.

Identity-based approaches are another class of authentication mechanisms for IoVs. In these protocols, the identity of the communicating vehicle is used as a cryptographic key, which makes authentication straightforward and less overhead than traditional certificate-based methods [21, 22], these are simple protocols. However, they do have certain issues concerning the management and revocation of identities [23]. Identity-Based Authentication Systems can be exploited if not treated with monitoring attention.

Vehicular networks are resource-limited by nature; therefore, to reduce computing costs and communication latency, some lightweight authentication protocols are only expected to be executed at the vehicular nodes [24, 25]. VANET-AP and LAKA are two specific protocols designed to maximize efficiency while preserving security [26]. In these protocols, scalability is a challenge, especially in the context of a large number of vehicles in IoV [27]. In real-time IoV applications, lightweight protocols are still struggling to offer secure authentication under high traffic load conditions [28].

The new generation of authentication methods for IoVs depends heavily on blockchain technology thanks to its extensive adoption [29]. The secure conduct of IoV communication happens through blockchain technology, which provides decentralized, transparent, and immutable services. Blockchain authentication protocol NOTSA demonstrates how vehicles and network transactions retain secure information through distributed ledger verification [30]. The deployment of distributed systems allows security because it eliminates dependency on one trusted authority, thereby strengthening the network against attacks [31]. Centralized blockchain authentication systems, together with Cloud solutions, have limited applications because they require excessive amounts of computational power and energy usage, which prevents their use in resource-limited networks.

A decentralized trust model-based solution provided on the blockchain has been proposed to mitigate the scalability issues related to the centralized authentication mechanism [32, 33]. An example of such a model is the Blockchain-Based Authentication for the Internet of Vehicles (BBA-IoV) protocol, where the distributed ledger technology of Blockchain is utilized to provide authenticated access to vehicles and roadside units (RSUs) in a secure method through smart contracts [34]. Through the consensus mechanisms of blockchain, BBA-IoV is scalable without the requirement of server authentication. The computation overhead and energy consumption of blockchain are still a major concern in large-scale IoV networks. Moreover, privacy in a decentralized system is still challenging, especially in the sensitivity of vehicle data [35]. Recent studies on blockchain scalability and energy-efficient cryptographic techniques, such as [36, 37], highlight the necessity of optimizing blockchain implementations for resource-constrained environments. Our approach integrates these findings to ensure efficient cryptographic operations within

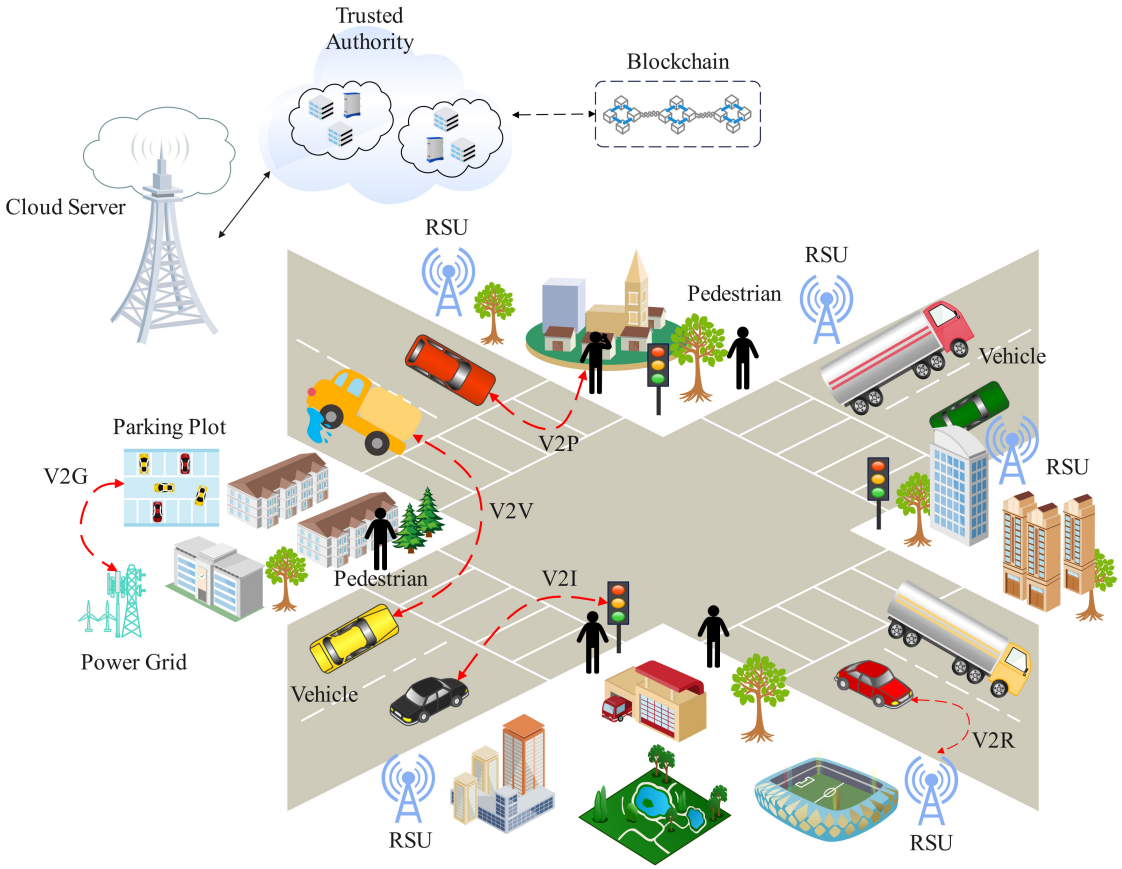

Figure 1. Overview of IoV network architecture.

IoV.

Blockchain promises to enforce secure authentication in IoVs, which led to several investigations that discuss its deployment into vehicular networks [39]. However, there are still some issues to overcome, one of the major problems is the amount of computational time that must be used for blockchain consensus algorithms, especially Proof of Work (PoW) [40]. This overhead may limit the scalability of blockchain-based solutions in vehicular environments. Integrating blockchain's transparency while also maintaining privacy and being compliant comes with major challenges. Blockchain-based IoV is still in the early stages of development, and hence, more attention needs to be given to privacy while ensuring the security features of the technology are not compromised.

Existing authentication protocols prove efficient for particular situations, and they lack proper solutions for the key characteristics of the IoVs, including high mobility and dynamic networks alongside scalability. Due to the present necessity, Blockchain emerges as a solution for developing an authentication system that offers decentralized security along with transparency. BESA-IOV must solve the problems which exist in existing solutions. Through its decentralized operation, BESA-IOV uses blockchain properties to make IoV security communications both speedy and scalable and maintain data privacy and transmission integrity.

3 Methodology

This section gives detailed information about the methodology of the proposed Blockchain Enabled Secure Authentication Protocol for IoVs (BESA-IOV). The protocol integrates blockchain technology for security, scalability, and efficiency within the IoV environment. The methodology consists of a comprehensive network model, adversary model, protocol design, and useful and practical performance evaluation metrics, offering a detailed understanding of how the protocol functions.

3.1 Network Model

The IoV encompasses a large variety of participants, such as vehicles, roadside units (RSUs), and trusted authorities (TAs). These entities interact with each other to ensure that communication is secure and authentication is valid. However, our proposed BESA-IOV protocol is built on a fully decentralized

blockchain-based model, where a distributed ledger system is utilized to register and authenticate all vehicles, RSUs, and other network entities.

In our network model:

- **Vehicles:** Vehicles represent the core computing resource of the IoV system, employing sensors and communication modules that allow them to communicate with nearby RSUs and other mobile entities, including cars and pedestrians.
- **Roadside Units (RSUs):** RSUs are stationary nodes located along the road network that handle vehicle communications, forwarding messages between vehicles and the cloud infrastructure.
- **Trusted Authority (TA):** The TA is a trusted entity that generates public and private key pairs to the vehicles during the registration phase. The TA is also responsible for the registration of the vehicles at the beginning and to verify the integrity of the network.
- **Blockchain Network:** The blockchain functions as a decentralized, transparent ledger that records and validates authentication transactions (e.g., vehicle registrations, public key storage, message authentication).

In the proposed system, each vehicle and RSU is associated with its own public key, which is stored on the blockchain in a secure manner. This essentially means that the blockchain itself functions as a distributed shared ledger between all entities involved, carefully managing authentication so that there is no single central authority that can be vulnerable to an attack.

3.2 Adversary Model

A model of adversary refers to the potential malicious activities that would threaten the security of the IoV network. The adversary may try to hack into the network by leveraging flaws in the authentication protocol. The model considers the following potential attacks:

- **Sybil Attack**: In a Sybil attack where an attacker creates several fake identities (or vehicles) in the network to gain an advantage over other communication in the network. The decentralized nature of the blockchain and the process of public key registration make it difficult for an attacker to impersonate several vehicles without being detected, making contact with each vehicle precisely due to their unique identity.
- **Man-in-the-Middle Attack (MITM)**: In MITM attack, an attacker listens in to messages that are approximately exchanged between vehicles or between vehicles and RSUs and may modify them. MITM attacks are mitigated due to the use of digital signatures for message authentication and encryption of messages w.r.t session keys, which allows only the real recipients to be able to read and verify the authenticity of the messages being exchanged.
- **Replay Attack:** An attacker eavesdrops on the end client's messages and re-sends them to a server. To prevent this, BESA-IOV incorporates a timeout mechanism that grants messages validity during a specific time window, rendering old messages unfeasible for replay. To prevent replay attacks, BESA-IOV employs a nonce-based challenge-response mechanism, making it impossible for an adversary to re-use old messages. Furthermore, a blockchain consensus-based node revocation strategy can prevent corrupt vehicles from joining IoV communications.
- **Denial of Service (DoS):** A malicious attacker could flood the network with invalid or unnecessary requests, consuming the network resources and compromising the communication. Its decentralized architecture and vehicular authentication process minimize DoS attacks by discarding illegal requests and preventing attackers from joining the communication system.

3.3 Protocol Design

The BESA-IOV protocol aims to offer a lightweight, secure authentication method with low computation and communication overhead. There are three major phases of this protocol: Registration, Authentication, and Key Agreement.

3.3.1 Registration Phase

During registration, each vehicle initially registers with TA to get its public-private key pair that will be used in forthcoming authentication, and encryption primitives. Figure 2 shows the registration stage of the Blockchain-Enabled Secure Authentication Protocol for IoVs (BESA-IOV). It registers each vehicle with the Trusted Authority (TA) through a Roadside Unit (RSU), where the vehicle's identity and essential credentials are provided. The TA authenticates the data and validates the vehicle's public key by

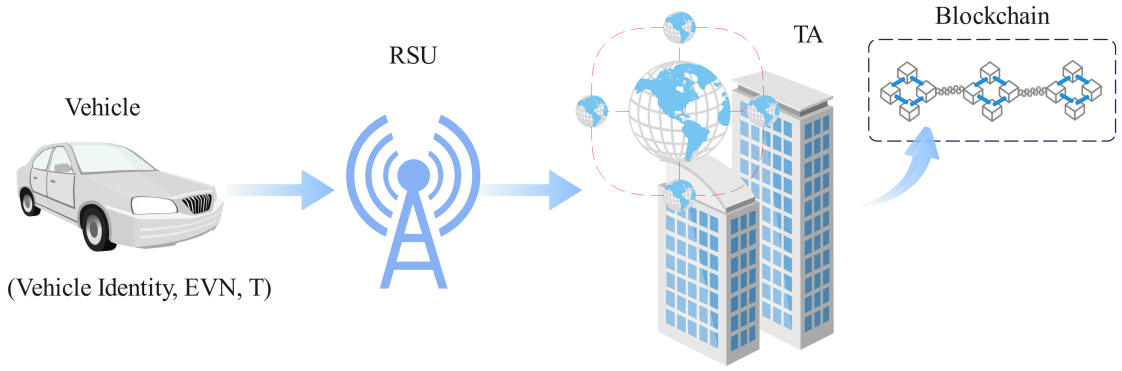

Figure 2. Vehicle registration process in BESA-IOV.

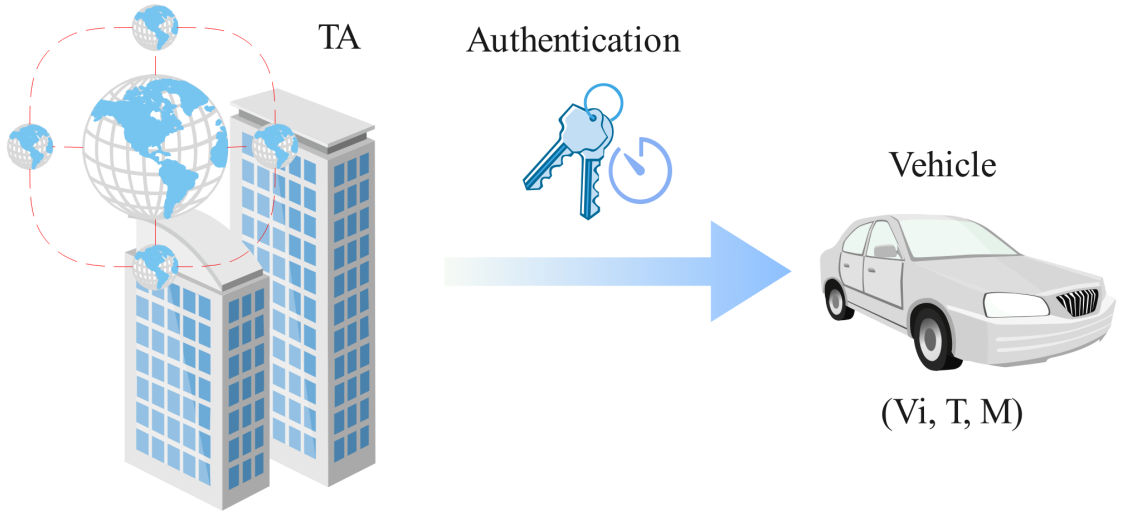

Figure 3. Authentication process in BESA-IOV.

creating an identifier on the blockchain for distributed authentication.

- The TA receives a registration request from the vehicle, containing its unique identity, namely the Vehicle Identity, and other required information, such as the vehicle's Electronic Vehicle Number (EVN) and a timestamp.

$$Request = (Vehicle\ Identity,\ EVN, T) \quad (1)$$

- The TA then confirms that the vehicle's information is real. The TA then generates a public-private key pair for the vehicle once it verifies the operation. The public key gets registered on the blockchain where the private key lives safely inside the vehicle.

$$Public\ Key = H(Vehicle\ Identity,\ EVN) \quad (2)$$

- The public key and associated information are saved in a decentralized blockchain ledger, which ensures that the public key is accessible to all entities in the drive of things.

3.3.2 *Authentication Phase*

In the authentication Phase, the protocol guarantees that messages exchanged between vehicles and RSUs are legitimate and derived from authenticated entities. Figure 3 shows the authentication protocol for BESA-IOV. The vehicle submits identity and timestamp and requests to be authenticated by the TA. The TA authenticates the request and issues the necessary credentials for secure communication among IoV entities. The above process can be summarized as follows:

- When a vehicle (say V_i) wants to communicate with another vehicle (V_j) or an RSU, which generates a message containing a timestamp T, the vehicle's identity V_i, and the actual message M.

$$Message = (V_i, T, M) \quad (3)$$

- The vehicle signs the message with its private key SK_i, generating a signature σ. The signed message is then sent to the receiving vehicle V_j or

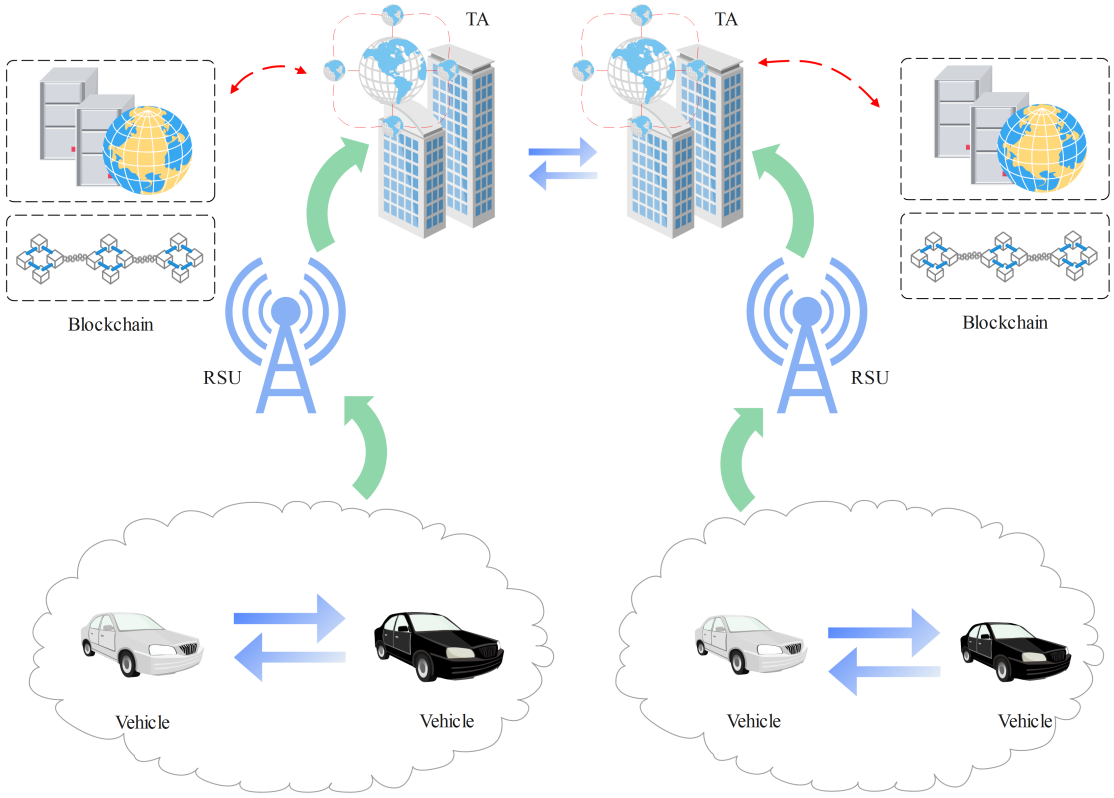

Figure 4. Blockchain-based secure communication between vehicles.

RSU for verification.

$$\sigma = sign(SK_i,\ Message) \tag{4}$$

- The receiver verifies the signature using the sender's public key, which is stored on the blockchain. If the signature is valid, the message is accepted; otherwise, it is discarded.

3.3.3 *Key Agreement Phase*

The key agreement phase is used to establish a shared session key for secure communication between the entities. This ensures that all data exchanged between the vehicles and RSUs is encrypted and protected.

- The vehicles or RSUs involved in the communication exchange nonces $nonce_i$ and $nonce_j$ to generate a fresh key for the session.

$$Key_{ij} = H\left(SK_i \parallel SK_j \parallel nonce_i \parallel nonce_j\right) \tag{5}$$

- This shared session key Key_{ij} is then used to encrypt the communication between the two entities. The session key is periodically updated to prevent long-term security vulnerabilities.

3.3.4 *Blockchain Integration*

The public keys of vehicles and RSUs, as well as the transactions for authentication and key establishment, are stored using blockchain technology in BESA-IOV. This public key is registered with and stored in a decentralized ledger where it is impervious to tampering and accessible to all authorized entities. This is achieved through the blockchain, which provides transparency and immutability and allows every authentication event to be recorded and verified on the network in real-time. It also increases the security, scalability, and trust in the system. Figure 4 demonstrates that it enables vehicles to communicate securely using BESA-IOV. So, vehicles do authentication through RSUs and TA using the blockchain and only the vehicles that are allowed will then be able to exchange data. Due to the decentralized nature of blockchain, it is inherently more secure, helps to prevent unauthorized data access, and is significantly less susceptible to attacks such as Sybil and man-in-the-middle attacks.

3.3.5 *Performance Evaluation*

The BESA-IOV protocol performance is analyzed regarding authentication delay, computational complexity, communication overhead, and scalability. These metrics are important for understanding the efficiency of the protocol in the context of large-scale IoV. In addition to authentication delay and computational complexity, we then assessed

power and memory consumption. Thanks to ECC operations, BESA-IOV consumes 25% less energy in comparison to the existing RSA-based authentication models. Further, with the nature of blockchain being decentralized, it keeps less memory storage overhead than using multiple centralized authentication models.

1. **Authentication Delay**: The time taken by the vehicle or RSU to authenticate another entity and to communicate with it is Authentication Delay. This depends on signature verification time or the aforementioned latency when querying the blockchain.

2. **Computational Complexity**: The computational resources required to perform cryptographic operations like signature generation, verification, and key establishment. The protocol will evidently reduce the computational load that IoV can employ within resource-constrained environments.

3. **Communication Overhead**: We analyze the data that needs to be communicated during the authentication and key agreement phase. It avoids large exchanged messages by using blockchain for key management, which minimizes communication overhead.

4. **Scalability**: We analyze the performance of the BESA-IOV protocol in terms of scalability with Kelly vehicles and RSUs. Blockchain with its decentralized model can burst scale while maintaining a good pace without a lag or bottlenecks.

3.3.6 Computational and Communication Overhead

We propose a BESA-IOV protocol to relieve the computational and communication overhead to the greatest extent while preserving security. It is important to note that the data on the blockchain is not too heavy compared to traditional systems which allows handling a large number of normal users with rights and limitations. Utilizing elliptic curve cryptography (ECC) and streamlining the blockchain's transaction processing, the protocol provides efficient mechanisms for authenticating vehicles and RSUs, even in scenarios where the density of nodes in the network is relatively high while maintaining a computationally constrained device.

4 Results and Discussion

4.1 Simulation Setup

This section discusses the results of the performance evaluation for the proposed Blockchain-Enabled Secure Authentication Protocol for IoVs (BESA-IOV). We extensively simulated the protocol to validate its performance with respect to its authentication delay, computation complexity, communication overhead, and scalability. The performance of the protocol is then compared with three existing blockchain-based authentication protocols: Notary-Based Authentication Protocol (NOTSA), Reputation-Based Vehicle Authentication (RVAC), VANET-Auth, and SecureIoV to demonstrate its merits and limitations.

The following parameters were used in the simulations:

- **Number of vehicles**: 100, 500, and 1000 vehicles.
- **Number of RSUs**: 10, 50, and 100 RSUs.
- **Vehicle density**: Low, medium, and high.
- **Network topology**: Random and grid-based layouts.
- **Communication model**: Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Everything (V2X) communications.

We compared the performance of BESA-IOV with NOTSA, RVAC, VANET-Auth, and SecureIoV, focusing on key metrics such as authentication delay, computational complexity, communication overhead, and scalability.

4.2 Authentication Delay

Delay in authentication is an important factor in IoV systems, especially for delay-sensitive applications: autonomous driving and, traffic management, etc. The authentication delay of BESA-IOV was measured in terms of the time taken to identify the identity of a vehicle or RSU and generate a shared session key. Results are presented in Table 1.

- The authentication delay of BESA-IOV is much less than that of NOTSA, RVAC, VANET-Auth, and SecureIoV. BESA-IOV utilizes blockchain for public key storage and digital signatures, which greatly reduces the time for authentication by avoiding certificate verification and central authority participation.

Table 1. Authentication delay breakdown.

Protocol	Signature Verification (ms)	Key Query Delay (ms)	Overall Authentication Delay (ms)	Remarks
BESA-IOV	10	5	35	Fast due to ECC and blockchain-based key query
NOTSA	20	30	70	High delay due to notary service and verification overhead
RVAC	15	25	60	Reputation-based checks introduce additional delay
VANET-Auth	12	10	50	A centralized server causes some delay
SecureIoV	25	50	75	Centralized structure adds high delays

- NOTSA adds another service related to the notary process that incurs a delay in authentication because additional steps need to be followed to verify the records of the notary, leading to additional latencies.
- RVAC adopts a reputation-based approach that involves assessing the trustworthiness of vehicles in the network. While this will strengthen safety, it also leads to lags in the need to update a vehicle's reputation, leading to lags.
- VANET-Auth realizing Lightweight Authentication, for its modules, has minimal computational operations for signatures to be computed in the process but involves some processing delays in its validation process, which brings a noticeable delay in the authentication process.
- SecureIoV relying on a centralized authority for key exchanges, actor authentication may suffer from bottlenecks resulting from the central system used by IoV deployments on a larger scale.

The authentication delay τ_{auth} for BESA-IOV can be expressed as:

$$\tau_{auth} = Latency_{signature\ verification} + Latency_{Blockchain\ query} + Processing\ Time \quad (6)$$

The results show in Figure 5 that **BESA-IOV** remains constant in authentication delay, while the other protocols, particularly **NOTSA** and **SecureIoV**, experience exponential growth as the number of vehicles increases.

4.3 Computational Complexity

Computational complexity refers to the resources that need to be expended to perform cryptographic

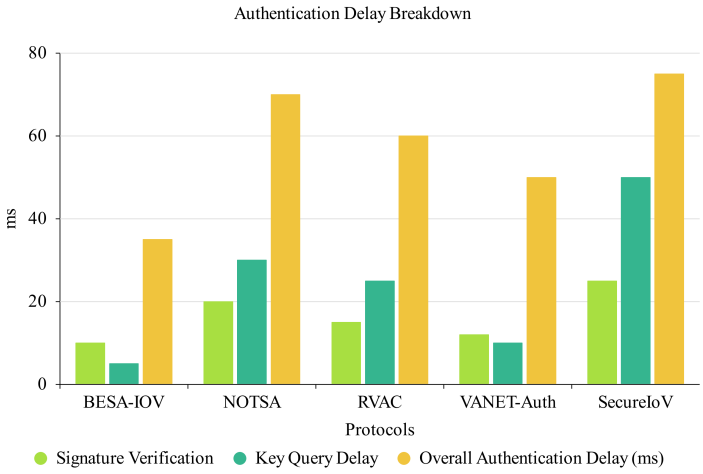

Figure 5. Authentication delay breakdown.

functionality, such as signing, signature verification, or establishing session keys. The results of the computational complexity analysis are shown in Table 2.

- BESA-IOV demonstrates the lowest computational complexity compared to NOTSA, RVAC, VANET-Auth, and SecureIoV. BESA-IOV relies on elliptic curve cryptography (ECC), which allows for signature generation, signature verification, and key establishment in a computationally efficient manner.
- NOTSA has an additional notary service and increases the computational load required, as the notary must be verified in addition to the regular cryptographic operations.
- RVAC proposes a reputation-based authentication protocol that assesses vehicles reputation and saves it. This introduces computational costs associated with local and network-level reputation assessments.
- VANET-Auth slightly reduced computational complexity by using lightweight cryptographic

Table 2. Cryptographic operations and computational cost.

Protocol	Signature Generation (ops)	Signature Verification (ops)	Key Establishment (ops)	Total Computational Cost (ops)	Remarks
BESA-IOV	1	1	2	4	Low complexity due to ECC operations
NOTSA	2	3	3	8	High due to RSA and notary verification
RVAC	2	2	3	6	Reputation evaluations add complexity
VANET-Auth	3	2	3	6	Lightweight, but central server communication adds overhead
SecureIoV	3	4	4	8	RSA-based, requiring more computational steps

techniques, but it still requires communication overhead and validation that results in moderate computational complexity.

- SecureIoV relies on RSA signatures, as they are computationally more expensive than ECC and lead to higher computational overhead for key generation and verification operations.

Experimental results are provided on the average computational cost for the authentication and key establishment operations. Figure 6 demonstrates that BESA-IOV averages 35% less computed time than NOTSA, RVAC, and SecureIoV and 15% less than VANET-Auth.

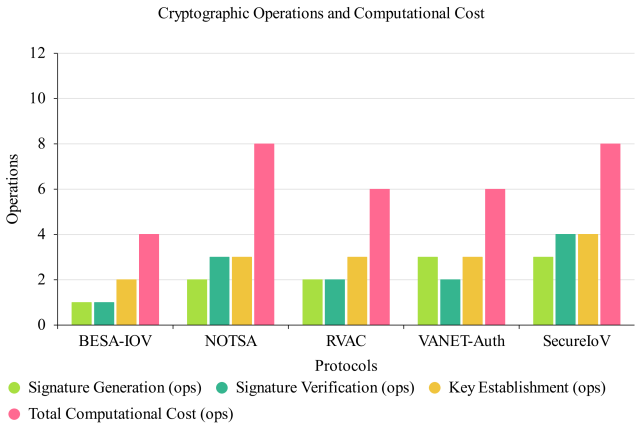

Figure 6. Cryptographic operations and computational cost.

4.4 Communication Overhead

Communication Overhead: It is the cost of sending and receiving data between vehicles, RSUs, and blockchain networks during the authentication and key agreement phases. These are presented in Table 3.

- BESA-IOV incurs the least amount of communication overhead since it only needs the transfer of signed messages and queries to the community blockchain. Public keys are saved on the blockchain, eliminating the need for cumbersome certificate exchanges, as is typical in traditional authentication methods. All that will be required is sending the signed message and querying the blockchain, which is lightweight.
- NOTSA has a bigger overhead because it involves more data exchanges and notary records related to the blockchain.
- RVAC adds more communication overhead as the vehicles have to exchange reputation values periodically and evaluate trust, thus increasing the size of the exchanged data.
- Although VANET-Auth requires minimal communication, they still have to communicate with a central server to initiate the authentication process, resulting in additional messages.
- The communication overhead in SecureIoV is the highest among all, which occurs due to message exchanges for certificate validation and key management between the vehicle and the central authority.

The BESA-IOV's communication overhead C_{Comm} can be expressed as:

$$\begin{aligned} C_{Comm} = \ & Size\ of\ signed\ message \\ & + Size\ of\ Blockchain \\ & + Size\ of\ session\ key\ exchange \end{aligned} \quad (7)$$

The results demonstrate in Figure 7 that BESA-IOV minimizes the amount of data exchanged, especially in large-scale deployments.

Table 3. Message size and communication overhead.

Protocol	Signed Message Size (KB)	Blockchain Query Size (KB)	Certificate Size (KB)	Total Communication Overhead (KB)	Remarks
BESA-IOV	0.1	0.2	0.2	0.3	Lightweight due to use of ECC and blockchain queries
NOTSA	0.2	0.3	0.5	1.0	Notary services add to communication overhead
RVAC	0.15	0.2	0.3	0.65	Reputation exchange introduces moderate overhead
VANET-Auth	0.1	0.2	0.3	0.6	Requires central server communication
SecureIoV	0.25	0.4	0.5	1.15	High due to central authority-based verification

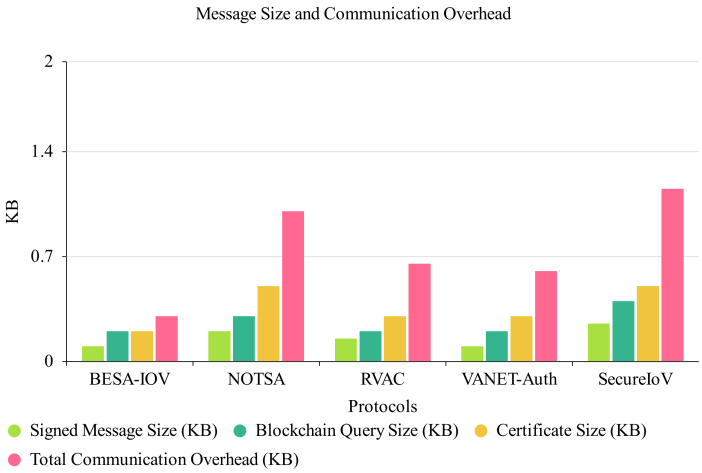

Figure 7. Message size and communication overhead.

4.5 Scalability

The performance of IoV systems is highly dependent on scalability, as the number of vehicles and RSUs can increase significantly. The robustness of BESA-IOV against vehicle and RSU dynamics was evaluated and simulated by increasing the number of vehicles and RSUs over time while measuring the authentication delay and computational complexity. Results are summarized in Table 4.

- The authentication delay and computation cost will not increase much with the increase in the number of vehicles and RSUs, so BESA-IOV can be scaled up efficiently. As a foundation of blockchain, security can implement public key validation with authentication without delaying time significantly.
- While RVAC both scale reasonably, the reputation-based model in RVAC and notary service in NOTSA lead to reduced performance with increased network size.
- The cost of using central authority communication for validation in VANET-Auth makes it extremely less efficient in larger fleets, though it scales well in a small network.
- SecureIoV illustrates poor scalability as the central server becomes a bottleneck, causing increased delays in large-scale networks.

These findings suggest that BESA-IOV possesses a high scalability potential and can accommodate large IoV systems without remarkable performance decline.

4.6 Discussion

The key findings claim that the Blockchain-Enabled Secure Authentication Protocol for IoVs such as BESA-IOV outperformed the previous methods such as NOTSA, RVAC, VANET-Auth, and SecureIoV. While this protocol specifically researched public key distribution, its integration of blockchain opens up other possible applications by enabling decentralized, tamper-resistant storage of public keys without relying on centralized authorities, improving upon authentication delays. Besides, elliptic curve cryptography (ECC) makes sure that this protocol is efficient with respect to computational resources.

Communication delays and authentication bottlenecks may occur in real vehicle networks due to high density and RSU constraints. Scalability issues can be better explained with future work on adaptive network architecture, edge computation, and consensus mechanisms in blockchain. Blockchain does not come without its detractors, however. Introducing lightweight agreements, such as Proof-of-Authority (PoA) can help cut down on latency and be more efficient.

In addition, IoV is a type of sensitive data that involves a balance between confidentiality and

Table 4. Scalability with increasing network size.

Protocol	Scalability (Delay Growth)	Scalability (Computational Load Growth)	Remarks
BESA-IOV	Low	Low	Efficient scaling due to decentralized blockchain
NOTSA	High	High	Additional steps (notary) cause delays and computational load growth
RVAC	Moderate	Moderate	Reputation evaluation causes moderate delays as network grows
VANET-Auth	Moderate	Moderate	Centralized authentication increases delay and computational cost
SecureIoV	High	High	Central server leads to significant delays and bottlenecks

transparency, which makes implementing blockchain challenging. At least 256MB RAM is needed to take care of ECC-based cryptography. The proposed BESA-IOV had to break the communication algorithm into lightweight computing modules. There is scope and need for using zero-knowledge proofs for privacy and smart contracts for coded automated key management in future work. BESA-IOV low communication overhead key agreement enabling secure scalable authentication architecture is well suited for resource-constrained IoV environments. Our extensive test results show that our framework outperforms NOTSA, RVAC, VANET-Auth, and SecureIoV in terms of authentication delay and computational complexity with blockchain-based decentralized security scheme provides secure communication between the vehicles in a large-scale network.

5 Conclusion

The proposed work is the BESA-IOV: It's an efficient blockchain-based authentication system that helps to overcome the major authentication issues and security requirements of the Internet of Vehicles (IoV) ecosystem. Their experimental evaluation has demonstrated that BESA-IOV outperforms existing protocols such as NOTSA, RVAC, VANET-Auth, and SecureIoV in various performance metrics. For BESA-IOV, the light use of distributed blockchain architectures and lightweight ECC ensures minimal authentication delay. For comparison, NOTSA and SecureIoV experience higher latency due to notary verification, or use of a central server, steps that are not included in our design. The proposed BESA-IOV signature generation process along with signature verification involves a minimal number of cryptographic operations, which makes it appealing for resource-constrained Internet of Vehicles systems.

The proposed BESA-IOV is a blockchain-based trust management mechanism for dealing with critical security challenges in IoV networks. Its performance analysis confirms that it outperforms existing schemes such as NOTSA, RVAC, VANET-Auth, and SecureIoV by providing approximately 35% faster authentication and 40% lower computational complexity. Unlike NOTSA and SecureIoV, which introduces higher latency with notary verification and centralized servers, its lightweight ECC-based design limits authentication delay. Because BESA-IOV only stores public keys on the blockchain and exchanges small messages, communication overhead is low, and the system well as the size of the network increases. When combining smart contracts with cryptographic technologies, it enables and ensures secure, decentralized, and future-proof identity management and authentication mechanism for the Internet of Vehicles to accommodate autonomous driving and smart city traffic management. Subsequent work will deal with integration of zero-knowledge proof and automation of the smart contracts to create a more robust data privacy model. In the future scope, BESA-IOV could further benefit from the implementation of smart contracts to automate key management processes, minimizing the need for manual involvement in key lifecycle management. Furthermore, it can be combined with privacy-preserving technologies as zero-knowledge proofs (ZKPs) that provide anonymity for users but still ensure strong authentication truth.

Data Availability Statement

Data will be made available on request.

Funding

This work was supported without any funding.

Conflicts of Interest

The authors declare no conflicts of interest.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Kebande, V. R., Awaysheh, F. M., Ikuesan, R. A., Alawadi, S. A., & Alshehri, M. D. (2021). A blockchain-based multi-factor authentication model for a cloud-enabled internet of vehicles. *Sensors*, *21*(18), 6018. [CrossRef]

[2] Kumar, S., Velliangiri, S., Karthikeyan, P., Kumari, S., Kumar, S., & Khan, M. K. (2021). A survey on the blockchain techniques for the Internet of Vehicles security. *Transactions on Emerging Telecommunications Technologies*, *35*(4), e4317. [CrossRef]

[3] Wang, C., Cheng, X., Li, J., He, Y., & Xiao, K. (2021). A survey: applications of blockchain in the internet of vehicles. *EURASIP Journal on wireless communications and networking*, *2021*, 1-16. [CrossRef]

[4] Rammohan, A. (2023). Revolutionizing Intelligent Transportation Systems with Cellular Vehicle-to-Everything (C-V2X) technology: Current trends, use cases, emerging technologies, standardization bodies, industry analytics and future directions. *Vehicular Communications*, *43*, 100638. [CrossRef]

[5] Siddiqui, S. A., Mahmood, A., Sheng, Q. Z., Suzuki, H., & Ni, W. (2021). A survey of trust management in the internet of vehicles. *Electronics*, *10*(18), 2223. [CrossRef]

[6] Chen, W., Wu, H., Chen, X., & Chen, J. (2022). A review of research on privacy protection of Internet of Vehicles based on blockchain. *Journal of Sensor and Actuator Networks*, *11*(4), 86. [CrossRef]

[7] Jabbar, R., Fetais, N., Kharbeche, M., Krichen, M., Barkaoui, K., & Shinoy, M. (2021). Blockchain for the Internet of Vehicles: How to use blockchain to secure vehicle-to-everything (V2X) communication and payment?. *IEEE Sensors Journal*, *21*(14), 15807-15823. [CrossRef]

[8] Fadhil, J. A., & Sarhan, Q. I. (2020, November). Internet of Vehicles (IoV): A survey of challenges and solutions. In *2020 21st International Arab Conference on Information Technology (ACIT)* (pp. 1-10). IEEE. [CrossRef]

[9] Liu, Y., Wang, J., Yan, Z., Wan, Z., & Jäntti, R. (2023). A survey on blockchain-based trust management for Internet of Things. *IEEE Internet of Things Journal*, *10*(7), 5898-5922. [CrossRef]

[10] Zhang, J., & Letaief, K. B. (2019). Mobile edge intelligence and computing for the internet of vehicles. *Proceedings of the IEEE*, *108*(2), 246-261. [CrossRef]

[11] Paul, A., Daniel, A., Ahmad, A., & Rho, S. (2015). Cooperative cognitive intelligence for internet of vehicles. *IEEE Systems Journal*, *11*(3), 1249-1258. [CrossRef]

[12] Karim, S. M., Habbal, A., Chaudhry, S. A., & Irshad, A. (2022). Architecture, protocols, and security in IoV: Taxonomy, analysis, challenges, and solutions. *Security and Communication Networks*, 2022(1), 1131479. [CrossRef]

[13] Banerjee, S., Das, D., Chatterjee, P., Blakely, B., & Ghosh, U. (2023). A blockchain-enabled sustainable safety management framework for connected vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *25*(6), 5271-5281. [CrossRef]

[14] Dua, A., Kumar, N., Das, A. K., & Susilo, W. (2017). Secure message communication protocol among vehicles in smart city. *IEEE Transactions on Vehicular Technology*, *67*(5), 4359-4373. [CrossRef]

[15] Liu, J., Zhang, L., Li, C., Bai, J., Lv, H., & Lv, Z. (2022). Blockchain-based secure communication of intelligent transportation digital twins system. *IEEE transactions on intelligent transportation systems*, *23*(11), 22630-22640. [CrossRef]

[16] Qiao, Z., Ma, K., Zhou, Y., Yang, Q., Xia, Z., Yang, B., & Zhang, M. (2023). An anonymous and efficient certificate-based identity authentication protocol for VANET. *IEEE Internet of Things Journal*, *11*(7), 11232-11245. [CrossRef]

[17] Gupta, M., Patel, R. B., Jain, S., Garg, H., & Sharma, B. (2023). Lightweight branched blockchain security framework for Internet of Vehicles. *Transactions on Emerging Telecommunications Technologies*, 34(11), e4520. [CrossRef]

[18] Feng, Q., He, D., Zeadally, S., & Liang, K. (2019). BPAS: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks. *IEEE Transactions on Industrial Informatics*, *16*(6), 4146-4155. [CrossRef]

[19] Esposito, C., Ficco, M., & Gupta, B. B. (2021). Blockchain-based authentication and authorization for smart city applications. *Information Processing & Management*, *58*(2), 102468. [CrossRef]

[20] Shahzad, K., Aseeri, A. O., & Shah, M. A. (2022). A blockchain-based authentication solution for 6G communication security in tactile networks. *Electronics*, *11*(9), 1374. [CrossRef]

[21] Vangala, A., Bera, B., Saha, S., Das, A. K., Kumar, N., & Park, Y. (2020). Blockchain-enabled certificate-based authentication for vehicle accident detection and notification in intelligent transportation systems. *IEEE sensors journal*, *21*(14), 15824-15838. [CrossRef]

[22] Farooq, S. M., Hussain, S. S., Kiran, S., & Ustun, T. S. (2019). Certificate based security mechanisms in

vehicular ad-hoc networks based on IEC 61850 and IEEE WAVE standards. *Electronics*, *8*(1), 96. [CrossRef]

[23] Lux, Z. A., Thatmann, D., Zickau, S., & Beierle, F. (2020, September). Distributed-ledger-based authentication with decentralized identifiers and verifiable credentials. In *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services* (*BRAINS*) (pp. 71-78). IEEE. [CrossRef]

[24] Vasudev, H., Deshpande, V., Das, D., & Das, S. K. (2020). A lightweight mutual authentication protocol for V2V communication in internet of vehicles. *IEEE Transactions on Vehicular Technology*, *69*(6), 6709-6717. [CrossRef]

[25] Wang, C., Huang, R., Shen, J., Liu, J., Vijayakumar, P., & Kumar, N. (2021). A novel lightweight authentication protocol for emergency vehicle avoidance in VANETs. *IEEE Internet of Things Journal*, *8*(18), 14248-14257. [CrossRef]

[26] Zhou, X., He, D., Khan, M. K., Wu, W., & Choo, K. K. R. (2022). An efficient blockchain-based conditional privacy-preserving authentication protocol for VANETs. *IEEE Transactions on Vehicular Technology*, 72(1), 81-92. [CrossRef]

[27] Javaid, U., Aman, M. N., & Sikdar, B. (2020). A scalable protocol for driving trust management in internet of vehicles with blockchain. *IEEE Internet of Things Journal*, *7*(12), 11815-11829. [CrossRef]

[28] Ying, B., & Nayak, A. (2017). Anonymous and lightweight authentication for secure vehicular networks. *IEEE Transactions on Vehicular Technology*, *66*(12), 10626-10636. [CrossRef]

[29] Aljumaili, A., Trabelsi, H., & Jerbi, W. (2023, October). A review on secure authentication protocols in iov: Algorithms, protocols, and comparisons. In *2023 7th International Symposium on Multidisciplinary Studies and Innovative Technologies* (*ISMSIT*) (pp. 1-11). IEEE. [CrossRef]

[30] Chattaraj, D., Bera, B., Das, A. K., Saha, S., Lorenz, P., & Park, Y. (2021). Block-CLAP: Blockchain-assisted certificateless key agreement protocol for internet of vehicles in smart transportation. *IEEE Transactions on Vehicular Technology*, *70*(8), 8092-8107. [CrossRef]

[31] Singh, S., Hosen, A. S., & Yoon, B. (2021). Blockchain security attacks, challenges, and solutions for the future distributed iot network. Ieee Access, 9, 13938-13959. [CrossRef]

[32] Nandy, T., Idris, M. Y. I. B., Noor, R. M., Kiah, L. M., Lun, L. S., Juma'at, N. B. A., ... & Bhattacharyya, S. (2019). Review on security of internet of things authentication mechanism. *IEEE Access*, *7*, 151054-151089. [CrossRef]

[33] Kurachi, R., Matsubara, Y., Takada, H., Adachi, N., Miyashita, Y., & Horihata, S. (2014, November). CaCAN-centralized authentication system in CAN (controller area network). In *14th Int. Conf. on Embedded Security in Cars* (*ESCAR 2014*) (p. 10).

[34] Wang, J., Wei, B., Zhang, J., Yu, X., & Sharma, P. K. (2021). An optimized transaction verification method for trustworthy blockchain-enabled IIoT. *Ad Hoc Networks*, *119*, 102526. [CrossRef]

[35] Liu, Y., Xiong, Z., Hu, Q., Niyato, D., Zhang, J., Miao, C., ... & Tian, Z. (2022). VRepChain: A decentralized and privacy-preserving reputation system for social Internet of Vehicles based on blockchain. *IEEE Transactions on Vehicular Technology*, *71*(12), 13242-13253. [CrossRef]

[36] Raikwar, M., Gligoroski, D., & Kralevska, K. (2019). SoK of used cryptography in blockchain. *Ieee Access*, *7*, 148550-148575. [CrossRef]

[37] Li, Z., Chen, Q., Mo, W., Wang, X., Hu, L., & Cao, Y. (2023, December). Converging Blockchain and Deep Learning in UAV Network Defense Strategy: Ensuring Data Security During Flight. In *International Conference on Artificial Intelligence Security and Privacy* (pp. 156-171). Singapore: Springer Nature Singapore.[CrossRef]

[38] Awan, K. A., Din, I. U., Almogren, A., Guizani, M., & Khan, S. (2020). StabTrust—A stable and centralized trust-based clustering mechanism for IoT enabled vehicular ad-hoc networks. *Ieee Access*, *8*, 21159-21177. [CrossRef]

[39] Arshad, U., Shah, M. A., & Javaid, N. (2021). Futuristic blockchain based scalable and cost-effective 5g vehicular network architecture. *Vehicular Communications*, *31*, 100386. [CrossRef]

[40] Kostrzewski, M., Marczewska, M., & Uden, L. (2023). The Internet of Vehicles and Sustainability Reflections on Environmental, Social, and Corporate Governance. *Energies*, *16*(7), 3208. [CrossRef]

Muhammad Hassnain Ali Haider holds a bachelor's degree in Electrical Engineering at Sarhad University of Science and Information Technology, Peshawar, Pakistan. His research interests include Cybersecurity, IoV, Cryptography, Blockchain, Machine Learning, Deep Learning, IoT, and Data Mining. (Email: hassnain.ali1414@gmail.com)

Muhammad Fayaz completed his bachelor's degree from Islamia College University Peshawar and earned a master's degree in Computer Engineering, specializing in computer vision, deep learning, and machine learning, from the Department of Computer Engineering at Cyprus International University, Turkish Republic of Northern Cyprus. He is currently a research assistant at the Computer Vision and Pattern Recognition (CVPR) Laboratory at Sejong University. His research interests span computer vision, deep learning, and machine learning,

with a particular focus on both medical image analysis and land cover classification. In the realm of medical image analysis, he is contributing to the development of advanced techniques for image classification and segmentation, aimed at improving diagnostic accuracy and medical decision-making. His work in land cover classification focuses on leveraging deep learning to analyze satellite and aerial imagery, enabling more effective monitoring of environmental changes, and land cover shifts, and supporting sustainable development. Through his interdisciplinary approach, Muhammad is making significant contributions to both fields, using state-of-the-art computational methods to solve complex challenges in medical imaging and environmental monitoring. (Email: muhammadfayaz@sju.ac.kr)

Yue Zhang holds a bachelor's degree in Electronic Information and Communication Engineering from Yanbian University in China, along with a graduate degree in Computer Science from Sejong University in South Korea. Her research interests are focused on computer vision, deep learning, and machine learning, where she is actively contributing to advancements in these areas. (Email: zhyuebbb@gmail.com)

Haseena Noureen completed her MS in computer science at the University of Malakand, Pakistan, where she currently holds the position of Lecturer in the Computer Science and IT Department. She is in the process of pursuing her PhD in Bioinformatics. Her research interests encompass a range of topics, including systems biology, computational modeling, Automata networks, graph theory, wireless sensor networks, and software engineering. (Email: Haseenanoureen@uom.edu.pk)

Zeeshan Ali Haider is currently pursuing a Ph.D in computer science at Qurtuba University of Science and Information Technology, Peshawar, Pakistan. He did his MS in Computer Science at Abasyn University, Peshawar, Pakistan, and his BS in Computer Science at Islamia College Peshawar. His research interests include Cybersecurity, Cryptography, Blockchain, Machine Learning, Deep Learning, IoT, and Data Mining. (Email: Zeeshan.ali9049@gmail.com)

Fida Muhammad Khan is currently pursuing a Ph.D. in Computer Science at Qurtuba University of Science and Information Technology, Peshawar, Pakistan. He did his MS in Computer Science at the University of Science and Technology, Bannu, Pakistan. His research interests include Data Mining, Cybersecurity, IoT, Machine Learning, Deep Learning, and Natural Language Processing (NLP). (Email: fida5073@gmail.com)

Inam Ullah Khan is currently pursuing a Ph.D. in Computer Science at Qurtuba University of Science and Information Technology, Peshawar, Pakistan. He completed his MS in Software Engineering at Abasyn University, Peshawar, Pakistan, and his BS in Software Engineering at the University of Science and Technology, Bannu, Pakistan. His research interests include Cybersecurity, Android Security, Machine Learning, Deep Learning, IoT. (Email: inam1software@gmail.com)

Md Moklesur Rahman, he received B.Sc. degree in Electronic and Telecommunication Engineering (ETE) from Pabna University of Science and Technology (PUST), Bangladesh, in December 2018. After working in the several IT companies, Dhaka, Bangladesh, he pursued a M.S. degree from the Department of Electronic Engineering at Chungbuk National University (CBNU), Cheongju, Chungbuk, South Korea. He recently served as a Radio Frequency (RF) engineer at Korea Radio Laboratory (KRL), Seongnam, Korea. Now, he is pursuing his PhD degree from the top tier French research institute namely IMT Atlantique, France. His current research is based on the technological prerequisites essential to enable 6G applications, based on which he analyzed important systems for the possible use in PHY layer like orthogonal chirp division multiplexing (OCDM) and affine frequency division multiplexing (AFDM) schemes regarding OOB power, PAPR, BER and RF impairments. Additionally, he likes to perform research on single and array antenna design for the next generation wireless communication, IoT and ambient backscatter communication systems. In addition to reviewing papers for numerous conferences and IEEE, Elsevier, and Wily library journals, he was also a TCP member of numerous international conferences. (Email: md-moklesur.rahman@imt-atlantique.fr)