Research Article

Lightweight Authenticated Privacy-Preserving Secure Framework for the Internet of Vehicles

Mona Jamjoom 1, Hussein Abulkasim 2, and Safia Abbas 1

1Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia
2Faculty of Science, New Valley University, El-Kharga 72511, Egypt

Correspondence should be addressed to Hussein Abulkasim; hussein@scinv.au.edu.eg

Received 28 June 2022; Accepted 12 August 2022; Published 9 September 2022

Academic Editor: Irshad Azeem

Copyright © 2022 Mona Jamjoom et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The integration of the Internet of things and dynamic vehicles has become unavoidable in advanced transportation systems. The vehicles communicate wirelessly with other vehicles, cloud servers, and roadside units via open communication channels. The openness of the above-mentioned entities and their communication tools introduces new difficulties, such as data privacy, vulnerabilities, data integrity, and scalability. To enhance data privacy and ensure security, a lightweight authenticated privacy-preserving secure framework is presented in the Internet of vehicles deployment. The proposed scheme can achieve confidentiality, privacy, authenticity, integrity, anonymity, and perfect forward secrecy based on blockchain technology, elliptic curve cryptography, and a one-way hash function. The proposed framework is secure against well-known cyberattacks, including replay attacks, man-in-the-middle attacks, traffic analysis attacks, and DDoS attacks. The security analysis shows the robustness of the proposed scheme. Finally, the results demonstrate that the proposed framework is efficient and feasible in practice.

1. Introduction

The relevance of transportation in our everyday lives is apparent. In the future years, it is expected that the number of automobiles on the roadway will increase to 2 billion or even more [1]. As a result, we are seeing an increase in traffic jams, pollution, accidents, congestion, and other issues. The World Health Organization (WHO) has produced research estimating that 1.4 million people died in traffic accidents in 2018 [2, 3]. Vehicle ad hoc networks (VANETs) are the basis of the smarter cities concept and Intelligent Transportation Systems (ITSs) to increase transportation effectiveness and protection [4–6]. The Internet of Things (IoT) is a recent technology that has expanded to include billions of smart gadgets that are prepared to communicate to the Network [7]. Remote gadgets, smart objects, and wired and wirelessly networking have all been made possible by novel technology. The IoT connects every electrical, mechanical, and computational equipment. The notion of the Internet of Vehicles (IoV) is brought to life via vehicular ad hoc networks (VANETs) interconnected to IoT [8, 9]. The Network of VANET is an IoT implementation aiming to minimize urban transportation accidents and increase traffic management [10]. Operationalization, controllability, high creditability, and manageability effectiveness are the major characteristics of IoV [11]. VANETs are regarded as subcategories of MANETs (Mobile Ad Hoc Networks) [12]. Vehicles can communicate with numerous different vehicles and roadside units via dedicated short-range communication (DSRC) radiofrequency within the VANET umbrella. Two kinds of communications are developed in VANET specifically. It is in among vehicle-to-infrastructure (V2I) communication and vehicle-to-vehicle (V2V) communication, for starters. Smart automobiles and Road Side Units (RSU) are the major nodes of VANETs, which communicate with one another to transmit protection, infotainment, and safety data.

With the recent growth of the IoV, a large number of vehicles are required to join this big IoV network, yet the
amount of traffic to be managed and evaluated is massive. Similarly, bottlenecks become a problem as traffic loads on integrated structures grow [13, 14]. The central servers might be the bottleneck of the entire structure, in addition to the costly and intricate development methods. If the connection fails, the architecture as a whole may be broken. Furthermore, ensuring compatibility and consistency between frameworks is difficult for different providers. Vehicles on the roadway can build self-organized networks using the IoV. It provides multiple benefits, such as an in-built warning system that warns drivers of accidents so that they can decide quickly based on the provided roadside information. More sophisticated information can be possibly shared between vehicles and improve the safety and accuracy of auto-piloted vehicles. However, in the absence of effective security and privacy measurement, an adversary can easily gather the transmitted data via networks that typically contain the private data of vehicle users. In addition to privacy concerns, data integrity or data authenticity is an important security topic in IoV. It might cause a tragedy if an adversary can generate fake messages to misguide a human driver or an auto-pilot AI to make the wrong decisions. Those adversaries might attack the networks solely because of terrorism. They might also attempt to gain certain benefits from providing false information to other vehicles, such as attracting traffic to pass by their shops or competing parking lots. Those opponents could target the Internet for no other reason than terrorists. They may also try to obtain advantages by giving incorrect knowledge to other vehicles, including luring traffic to their stores or competitive parked spaces.

Accessibility regulation mechanisms have been used to interconnected vehicles in an attempt to ensure that the designated places or particular kinds of vehicles are recognized during the message distribution processes, as shown in Figure 1. To ensure message secrecy and fine-grained accessibility management, previous systems used cipher text-policy attribute-based encrypting (CP ABE) [15]. As a result, prior to continued transmitting, the message’s security must be confirmed [16]. For example, a hostile attacker could alter the congested position in the distributed message. Identity-based signature (IBS) has been used to accomplish message validation in IoT and minimize the key administration overhead of trusted authority (TA) by ensuring the validity of messages [17]. A motorist on either side might be reluctant to expose his trip routes, which could most likely be done by tracing the message provided by the OBU, since it might expose the consumer’s personal knowledge. As a result, in a cloud-assisted IoV, the security of the motorists must be carefully secured [18]. Furthermore, this could result in a new problem. Whenever a deliberately behaving car starts a scuffle, this might be trying to avoid being investigated. As a result, data conservation in interconnected vehicles must be conditioned [19], which implies that the actual identification of the vehicle must be hidden from RSUs as well as other vehicles, but the trusted authority might obtain the genuine identification of every vehicle if required. Enormous anonymously key-dependent protocols [20] and group signature-based protocols [21] are two current approaches that have been presented to accomplish this. Furthermore, because OBU’s must hold anonymously key pairings, the initial technique has several drawbacks, and the time required for validation in the second method increases as the number of revoked OBU’s increases. As a result, these two techniques are not appropriate for cloud-assisted IoV.

The rest of this paper is formalized as follows: Section 2 represents the related work, and Section 3 designates the proposed method for Lightweight Authenticated Privacy-Preserving Secure Framework for the IoV and designates in detail the workflow of the framework. Section 4 describes the experiments with results and comparison graphics with existing works and its discussion. Finally, Section 5 concludes the study.

2. Related Work

In Reference [22], the IoT is a promising field in which vast amounts of data and knowledge are continuously gathered, transmitted, and archived. Whereas this data and information are used for beneficial in wirelessly IoT, there are significant concerns that attackers will try to profit from the advantages of these novel technologies. Systems are especially vulnerable to numerous assaults in such a resource-constrained situation. Confidentiality and privacy of data are extremely important to IoT systems, and they should not be vulnerable to hacking. The absence of satisfactory privacy-preserving measures makes it impossible for end consumers to accept IoT wirelessly and embrace associated apps, which have become key barriers to the adoption and popularisation of wireless IoT. In this document, they will go over some of the most common wireless IoT implementation situations and the safety and private threat prototypes that go along with them. After that, they give a quick summary of wireless IoT privacy-preserving techniques. They also highlight new developments in privacy-preserving methods in wireless IoT depending on the categorization of implementation contexts. At last, they explore unresolved difficulties and potential data analysis possibilities for various wireless IoT implementation situations.

In Reference [23], the IoVs offer exciting possibilities for vehicle-to-everything (V2X) implementations, with authenticating serving as the foundation for establishing a secure vehicular framework and supporting sophisticated implementations. Current authenticating techniques, on the other hand, rely heavily on centralised services, which raise safety and confidentiality concerns. In this research, they present CyberChain, a CyberTwin (CT)-enabled blockchain system for verification that reduces both transmission and memory costs while preserving vehicular security. They divorce the consensus procedure from the real world by constructing a blockchain network in cyberspace, lowering the cost of blockchain operations. The Privacy-Preserving Parallel Pedersen Commitment (4PC) technique protects vehicle security while also speeding up the authenticating procedure. To improve CyberChain’s operating effectiveness, they suggest a Diffused Practical Byzantine Fault Tolerance (DPBFT) methodology for reaching cyberspace
agreements which could decrease decision time. Simulations and qualitative approaches are used to assess the suggested blockchain architecture and its related procedures. The findings of the assessment show that the suggested blockchain-based architecture enhances authenticating effectiveness in terms of authenticating latencies, confidentiality, memory expenditure, as well as communication overhead.

In Reference [24], the notion of the Social Internet of Things (SIoT) could be defined as the combination of current social networking and the IoT, which is infiltrating many sectors’ everyday operations. Smart networks are a promising SIoT implementation that is both prices efficient and ecologically benign. Furthermore, the bad side of intelligent networks is safety and confidentiality concerns. The purpose of this study is to address safety and confidentiality concerns in vehicle-to-grid (V2G) systems in order to encourage the wider deployment of V2G networking for smarter grids. As a result of this desire, they present a strong key agreement system in this work that could establish mutually authenticating without revealing users’ true identification. In resource-constrained contexts, effectiveness is often a crucial problem. The suggested approach is particularly effective when contrasted to pairing-based approaches because it only uses hash algorithms and bitwise exclusive-OR (XOR) procedures. In particular, they provide a formalized safety framework for their privacy-preserving key agreements technique for V2G systems. This approach’s rigorous safety assessment reveals that the suggested protocols are secure. Furthermore, an unofficial safety assessment shows that their approach could withstand a variety of assaults.

In Reference [19], developing intelligent and effective transportation networks for modern metropolitan regions has been considered a top priority for countries with rapidly growing metropolitan regions. The advancement of smart vehicles with various detectors capable of forming a temporary vehicular ad hoc network (VANET) or a vehicular sensor network (VSN) automatically is a novel concept. Drivers in a VSN could easily communicate vital or emergency traffic knowledge and execute driving considerations using wireless-enabled roadside unit (RSU) networks. They establish a novel identity-based (ID-based) signature depending on the elliptic curve cryptosystem (ECC) to sustain protected conversation and driver confidentiality for vehicles in a VSN and then use it to suggest new conditioned privacy preservation authenticating framework predicated on the discovered ID-based signature. This technique ensures that messages sent among vehicles as well as RSUs are securely authenticated. This study indicates that the suggested technique performs higher in regards to time consumption than current pseudo-ID-based authenticating systems for VSN.

3. Proposed Methodology

As illustrated in Figure 2, we assume a VANET architecture with different authorities structured hierarchically. Worldwide trust authorities (TAs) fix roadside units (RSUs) at the roadside, onboard units (OBUs), as well as a certificate authority (CA) mounted on mobile vehicles, make up the network structure. The CA is a globally recognized certificate authority that manages the device’s trusted organizations. It creates the global secret keys and the worldwide public keys, as well as sets up the network. Every TA relates to road authorities and serves as a registering and certifying agency for OBUs and RSUs. There are numerous TAs that separate city roadways into multiple domains using various decomposing techniques. Several graph-based approaches have already been used in intelligence networks and multimedia. They could be utilized to improve picture classification by acting as geometrical picture descriptions. Furthermore, these approaches could be employed as super pixel imaging high-order potential descriptions. Graph-based descriptions could also be utilized as generic picture aesthetically descriptions to help with cropping, image rankings, and photo retargeting.

RSUs link to the TA via a connected network, while OBUs connect via a wireless channel using a secured broadcaster, such as the transport layer security (TLS) protocols. RSUs act as gateways, receiving consumer
demands and delivering messages to the appropriate OBU's. Certain RSUs might be mounted on traffic signal poles at crucial intersections, as well as these RSUs could regulate the traffic indicators. RSU is assumed to be honest but curious, implying that it can be allowed to perform simulations authorized by the vehicles. It does not distort or skip calculations, although it might attempt to understand more regarding the messages. Vehicles equipped with OBU's broadcast traffic-related condition data to other VANET vehicles. We presume the vehicles are equipped with a variety of onboard equipment, such as onboard radar, GPS, and wireless transceivers. They also have tamper-resistant components for storing sensitive information, including equipment identifiers (EIDs) and cryptography keys. The application of attribute-based cryptography improves the effectiveness of secured communications across numerous vehicles significantly. The effectiveness is related to the characteristics' ability to limit information accessibility depending on distinct vehicle responsibilities. In the framework, properties are divided into three categories: (a) vehicle ownership; (b) event category: accidents, fires, bomb threats, and so on; and (c) event properties. Aspects could also be classed as dynamical or stable, based on how commonly they fluctuate. Car categories (e.g., fire engines, commercial vehicles, police cars, general civilian vehicles, and ambulances), as well as connections, are among the static properties. Parameters could also be changeable based on onroad circumstances (e.g., timestamp and location). Every static characteristic has its own private key, which is generated by the global certificate authority (CA). The local trustworthy authority (TA) will provide the dynamic characteristics and associated private key scan.

3.1. Design and Implementation of Blockchain-Based IoV

3.1.1. Data Categorization on the Blockchain. The importance of the information that must be distributed via the blockchain cannot be overstated. They would be categorized into a range of blockchains based on the objectives for which they would be used. It is not recommended that various blockchains interact with one another. The information is divided into the succeeding classifications:

(i) Data-1: information collected by roadside structures about driving patterns, speeding, and other factors.

(ii) Data-2: information from the vehicle's interior mechanics, air pressure, electrical, temperatures, and other sensors.

(iii) Data-3: private video, audio, as well as various data from users, including in recorders, videos, and so on.

(iv) Data-4: information about vehicle coverage.

![Framework for the proposed method.](image-url)
3.1.2. IoV-Blockchain Specifications. Researchers have been paying close notice to “blockchain” since they anticipate it could provide huge possibilities and improvements to the industry. Furthermore, research on the combination of IoV with blockchain technologies is still in its earlier stages. The succeeding is a summary of the requirement for blockchain technologies in the IoV:

Big information containers: upcoming IoV information might contain a variety of sensor information from the car, sensory information from driving behaviour information beyond the vehicle, and human-computer interaction information, among other things. This would also contain information from e-commerce transactions, including refueling, auto insurance, electrical vehicle recharging, and even car-to-car experience exchange, travel images, as well as other activities. Given a large number of vehicles on the highway, the number of information generated would be enormous, and both centralised and distributed collection must be completely utilized:

(i) Comprehensive decentralisation and real backup: blockchain technologies could be used to create transmitted cloud information centers that store information on numerous chosen nodes in a certain region and distribute it smartly to distributed nodes.

(ii) Facilitating resource utilisation: blockchain technologies may facilitate on-demand capacity utilisation by executing an on-demand resource methodology using intelligent agreements to perform the specified activity.

(iii) Selective confidentiality: every client maintains their individual keys, and every information block node only keeps encrypted chunks of user information. Therefore, the key to part of the information must be accessible to the regulating agency, including the government’s vehicle managing department, according to legal requirements. As a result, complete confidentiality could be maintained without the use of third data accessibility and management.

(iv) Service reliability advancement: we could enable traceability of resources utilising blockchain technologies, allowing consumers and service suppliers to accurately validate service level contracts.

(v) Lower transaction prices: blockchain storing expenses would be substantially lowered because of the mix of distributed and centralised memory techniques, and transfer expenses would be greatly decreased because of the usage of intelligent agreements in operations.

3.1.3. IoV Design. The succeeding design considerations might be addressed while designing a high-efficiency, secured, centralised, and dispersed scalable IoV to satisfy the ultimate objective of novel service demands.

Invulnerability: although certain nodes collapse, the computation would proceed on many other nodes.

Quick to set up: current networking infrastructure could be utilized to the maximum extent feasible, with the option of installing additional nodes.

Flexibility: the networking infrastructure must be capable of adjusting to altering surroundings and increasing its utilisation to satisfy the rising requirements of customers.

Scalability: it necessitates the systems’ capacity to insert systems and regulate the tremendous information explosion.

Safety: a key purpose of the IoVs architecture is to secure the vehicular network’s connections and information privacy.

High accessibility and defect tolerance: the IoVs must be simple to utilize and dependable.

3.1.4. Blockchain Transmitting in the IoVs. It is difficult to implement blockchain techniques in implementations because of the rapid speeds of cars, rapid fluctuations in speed, and error-prone wirelessly transmitting lines. As a result, adopting appropriate measures to ensure proper transmissions is crucial. Unlike standard blockchain implementations, IoV blockchain technologies should take into account the vehicle’s movement, the repetition of the physically positioning of roadside network components, the restricted communications range, and the low communications link reliability.

Assuming the vehicle produces novel information at consistent durations and therefore is available to send to the networks. The vehicle would select to utilize the roadside network for information transfer because there are more roadside connections that are to be utilized as nodes of certain blockchains. Transmission failures are caused by poor transmitting performance. The transmission resumes at the roadside device after a brief period of randomized backoff. If numerous retransmissions fail and the number of retransmissions reaches a certain threshold, the cellular system, including 4G, may be used to transmit the data. We presume that the car is unable to transmit information to the
roadside device because the accessible channel duration is shorter than the information transmitting period.

The existing block in a typical blockchain includes the hashing values of the previous blocks, and the block is disseminated concurrently by the P2P multineighbour nodes and merged with the period in the component. There are fewer neighbour nodes in the vehicle networks, and the roadside networks’ status as neighbour nodes changes automatically as the vehicle moves. We create a blockchain with a “lag timestamp interval” to assure the data’s privacy. The accompanying is a description of their specifics: (1) the hash number of the preceding block is included in all information blocks transmitted by the IoV; (2) the block is not only validated by a single block with defined timing stamps but also by numerous blocks with timing stamps that are within a given limit. Data corruption generated by particular but also by numerous blocks with timing stamps that are fewer neighbour nodes in the vehicle networks, and the roadside networks’ status as neighbour nodes changes automatically as the vehicle moves. We create a blockchain with a “lag timestamp interval” to assure the data’s privacy. 

3.2. System Initialization. The traffic management organisation, which acts as a trusted authority (TA), chooses two huge protected prime statistics \( p_1 \) and \( p_2 \), where \(|p_1| = |p_2| = \kappa\), and then produces the altered Paillier cryptosystem’s public key \( pk = (n = p_1p_2, g = g^\kappa \mod n^2) \) as well as the private key \( sk = x \) using the security variable \( \kappa \). Then, TA divides the private keys \( x \) into three shares, \( x_0, x_1 \) and \( x_2 \), resulting in \( x = x_0 + x_1 + x_2 \), as well as the amount of \( h_1 = g^{x_0+x_1+x_2} \mod n^2 \). TA, on the other hand, maintains the secret share \( x_0 \) to himself. TA effectively provides the secret number \( x_1 \) to every RSU during the registering process; simultaneously, TA safely spreads the secret number \( x_2 \) to every vehicle throughout the registered process. TA picks \( k \) equal-length prime integers for a district with \( k \) segments: \((q_1, q_2, \ldots, q_k)\), wherein \(|q_1| = |q_2| = \ldots = |q_k| = \kappa_1\), and it meets the constraint that \( k \cdot \kappa_1 < \lceil n \rceil \). TA allocates a prime integer \( q_l \) to segments \( l \) with the segmented identification \((u_l, v_l)\). Then, TA calculates

\[
Q = \prod_{i=1}^{k} q_iQ_1 = \frac{Q}{q_1}, y_1 = \frac{1}{Q_1 \mod q_1} \alpha_1 = Q_1 \cdot y_1. \tag{1}
\]

TA also chooses a consistent number \( d \) with the value \(|d| = \kappa_1 - 2\). Meanwhile, it selects two secured cryptographic operations, \( H_{\phi}: \{0, 1\}^* \rightarrow \mathbb{Z}_n^* \), \( H: \{0, 1\}^* \rightarrow \{0, 1\}^{\kappa_1-2} \), to ensure that \(|H(\cdot) + d| < \kappa_1\). Lastly, TA makes the characteristics public: \( \text{params} = \{pk, h_1, H_{\phi}, H, q_l: l = 1, 2 \ldots , k\} \).

3.3. Security and Privacy Requirements. The following are the applicable safety and confidentiality standards as described in this segment:

Authentication: A VC’s cloud members must always be legitimated in the framework. Just an authenticated organisation can access the VC as a virtual member, thanks to this provision. A cloud user, on the other side, should be a legal entity in the network. Whenever a cloud consumer transmits messages to one or more VCs, his or her identification must be verified [25, 26].

Messaging data protection: data transferred to a VC by a cloud user might include sensitive information. Message privacy ensures that the information from the cloud users can only be seen by the cloud members that make up the VC.

Conditional privacy: an attacker must be unable to discover the genuine identification of a messaging sender and differentiate between two messages sent by a similar sender to be considered private. Confidentiality is frequently conditional in the VC world (i.e., the security of a car should not be invaded). Malicious cars, on the other hand, might occur in the VC. For example, a cloud member (vehicle) might depart a VC without informing other cloud members or transmit a cloud user a false outcome. As a result, authorities must be capable of disclosing malicious participants’ identities.

Location sensitive: cloud consumers’ information is delivered to a VC in the VC. Cloud consumers, in general, are unconcerned about where their information is handled. Furthermore, there are times when cloud consumers will
only wish to utilize trusted VCs to handle specific knowledge. In truth, VCs could have varying levels of trust. For example, a VC in a city center or within an organisation under video monitoring might be regarded as more reliable than a VC in a remote area. A cloud consumer can limit the location of his or her information to be analyzed based on the amount of confidence necessary. We should point out that if a locality is not specified, a group of parked automobiles in unsupervised and unsecured parking lots in a remote area can form a VC and pretend to be in a secured parking lot [27].

3.4. Delay in Authentication and Protection from Hostile Attacks

3.4.1. Conspiracy Attack. The assault means that a malicious CRV could work together with many vehicles in a local area to get access to a new zone using an illegal identification, such as id\textsubscript{att}, and then communicate with other cars using malicious transactions, such as TX\textsubscript{att}.S. Furthermore, because the identification transactions TX\textsubscript{att} have a diffusion component, CTs in other zones could now obtain the TX\textsubscript{att} and validate the accuracy of ic and ip. The final verification will fail if the malicious CRV is unable to regulate the majority of the vehicles in the fresh area. The identification id\textsubscript{att} will be regarded as incorrect in the current region in this situation. TX\textsubscript{att}S interactions would also be considered invalid and would not be appended to the ledger. That is to state, even while the conspiracy assault could defraud honest vehicles within a narrow radius, the assault would be eradicated along with TX\textsubscript{att} spread, and all malicious activities TX\textsubscript{att}S that happened during the assault would be invalidated as well.

3.4.2. Man-in-the-Middle Attack. The sort of assault is intercepting and stealing a message throughout the authenticating procedure in order to get the private knowledge of honest automobiles. Both the ic and ip in the suggested P4C method are Pedersen commitments, which hide the hidden characteristics Atr. Furthermore, the P4C employs a parallel validation technique that does not require an opening process. Though if the attacker receives the accessible points of the elliptic curves G and H, the associated characteristics Atr cannot be determined in polynomial speed.

3.4.3. Replay Attack. The assault relates to attackers who reuse or gather other people’s authorized data to achieve reauthentication. Every transaction in our suggested authenticating architecture is identified by a timestamp. During the consensus validation procedure, every CTs would compare the existing timing to the timestamp enclosed in TX\textsubscript{id}. The transaction TX\textsubscript{id} is legitimate if the difference among the existing time and the timestamp falls within a particular time period; alternatively, it is denied. Furthermore, the ip is created by referencing the most recent Atr value on the ledger. If the malicious CRV replicates a prior ic to the novel area, the authenticating procedure would be refused as well.

4. Experimental Results and Discussion

This article’s experimental setup consists of five servers, each with an Intel i7 3770 3.4 GHz processor and 16 gigabytes of storage. Experimentation on a blockchain-dependent IoV with five RCNs, designated as A ~ E, and multiple VCNs validated the suggested methodology. The five RCNs are in charge of reaching a consensus. A and D are Byzantine nodes, but B, C, E are valid nodes that fulfill $n \geq 2f + 1$. Every node has two neighbours in its field of vision. During every communication, a node searches for and updates its neighbours in its view, in turn, using the push-pull modes and the gossiping protocols. The existing blockchain’s duration was fixed to 10, and the knowledge used to reach a consensus was fixed to $h$. The LI of proper nodes was then calculated to be $h$, whereas the LI of Byzantine nodes might be any values. Every node’s unique data is shown in Table 1. Prior to reaching a consensus, it is believed that two appropriate RCNs F, G wish to join the networks, whereas nodes C desire to leave. The networking channel is recognized to accommodate a maximum of 10 nodes entering and exiting at the same time. As a result, the number of units entering or removing the networks stays within limits, and nodes can join and leave the system properly. At last, six nodes are engaged in the consensus process, including two Byzantine nodes. Since it was the first time a consensus was reached, the number of c is zero.

$$A = (b + c) \% N = (5 + 0) \% 6 = 5.$$  

The VCN nodes that produce the data for consensus-making would transmit it to node F, as per equation (2). Node F would release data and begin the consensus-making procedure after obtaining it. The UI would then be determined by every node depending on its individual LI.

4.1. Maintaining the Vehicles’ Privacy. The public keys of each of the vehicles are recognized, and their original identities, containing public keys, are safely saved in their

| Model | M1 | M2 |
|-------|----|----|
| Metrics | Ac | Pr | Re | F1s | Ac | Pr | Re | F1s |
| Normal | 0.954 | 0.996 | 1.012 | 1.095 | 0.98 | 1.037 | 1.088 | 1.062 |
| Attacks, flaws | 0.954 | 1.023 | 0.993 | 1.02 | 0.98 | 1.087 | 1.033 | 1.059 |
| Median | 0.954 | 0.9486 | 1.044 | 1.044 | 0.98 | 1.062 | 1.098 | 1.099 |

Table 1: Measures for evaluating the blockchain-based categorization technique for M1 and M2.
Table 2: Measures for evaluating the blockchain-based categorization technique for M3 and M4.

| Model          | M3       | M4       |
|----------------|----------|----------|
|                | Ac  | Pr | Re | F1s | Ac  | Pr | Re | F1s |
| Normal         | 1.084 | 1.062 | 1.012 | 1.085 | 1.066 | 1.047 | 1.003 | 1.077 |
| Attacks, flaws | 1.084 | 1.012 | 1.059 | 1.085 | 1.066 | 1.011 | 1.043 | 1.075 |
| Median         | 1.084 | 1.0856 | 1.084 | 1.085 | 1.066 | 1.0786 | 1.0766 | 1.076 |

Figure 4: Accuracy comparison.

Figure 5: Precision comparison.
LAC. LAC protects the true identities of the vehicles in this manner, and they are secured till enemies obtain the connection to the LAC. Furthermore, the identifying data is maintained in an encrypted form, ensuring that the vehicles’ privacy is protected. Furthermore, even if attackers have the public-private key combinations for a certain car, obtaining genuine identification is impossible.

4.1.1. Transaction Security, Confidentiality, and Integrity.

The senders’ sign every transaction in the suggested framework to assure the privacy, confidentially, and consistency of the data. The digitally signature technique utilized is RSA-1024, which has an 80 bit safety strength, meaning it takes a minimum of 282 procedures to crack the keys [28]. The hash number is used to validate each event to enhance the security of the operations.

4.1.2. Preventing Attacks.

The RSA-1024 digital signature technique is deemed secure till the attacker cracks the basic key [29]. As a result, the suggested technique effectively secures communications among automobiles and LAC. The physical identification is ensured by LAC, and the
blockchain is used to verify it. This configuration protects the network from unauthorized or impostor cars, as well as Sybil as well as other unidentified source assaults [30]. The suggested digital signature technique employs a hash value to verify the transaction’s authenticity; as a result, any alteration to the initial information is detected and denied. This characteristic protects the suggested technique from both reply and man-in-the-middle attacks [31]. Because no unauthorized cars may complete any transactions, VANET is immune to DDoS attacks. Becoming a member of a cluster needs both physical and public key validation.

4.2. Evaluation. After putting the datasets through both classification measures in this chapter. Accuracy (Ac), precision (Pr), recall (Re), and F1-score (F1s) are the four measures described here. True Positive, True Negative, False Positive, and False Negative are denoted as TP, TN, FP, and FN, correspondingly.

The assessment parameters, including all four algorithms of the lightweight authenticated classifiers, are listed in Tables 1 and 2. The effectiveness of all the stacking blockchain architectures is greater throughout all four criteria than the VANET approach, as can be seen in both tables. Furthermore, of all the stacking VANET structures evaluated, the 4-VANET prototype performed the highest. The blockchain classification appears to be operating higher than the other when it comes to classifying errors and assaults separately. In both tables, the finest findings of both classifiers are displayed in bold. Figures 4–7 show a comparison of the best average, precision, recall, and f1-score assessment parameters for each classification. As a result, a fine-grained categorization depending on the VANET classifiers appears to be a preferable strategy, as the efficiency is superior, and we could identify assaults and errors independently at a similar moment. This technique may help implementations that require the classification of assaults and errors into separate classifications.

5. Conclusion

In numerous assault circumstances, a privacy-preserving attack-resistant lightweight trusted framework is presented to improve IoVs security by quickly detecting dishonest networks and revoking their accreditation. Furthermore, to keep the trusted structure lightweight, fewer arithmetic functions, including such squared logarithm and complicated geometries, are utilized to minimize the model’s complexities. Safety, reputational, confidentiality, decentralisation, trust-based approaches, data sharing, and authentication are among the methods categorized in the articles gathered from the research. Current studies on blockchain-based ways to protect the IoV are examined, and their inadequacies in terms of the criteria are stated. Additionally, batch validation could greatly minimize the computing overhead of evaluating a bunch of alerting signals. This technique has undergone an experimental assessment and security assessment to ensure that it could meet the safety and effectiveness requirements of alerting messages distribution in cloud-assisted IoV.

Data Availability

All data generated or analyzed during this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the present study.

Acknowledgments

The authors acknowledge Princess Nourah Bint Abdulrahman University Researchers Supporting Project number (PNU-RSP2022R104), Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia.

References

[1] S. Latif, S. Mahfooz, B. Jan et al., “Multicriteria based next forwarder selection for data dissemination in vehicular ad hoc networks using analytical network process,” Mathematical Problems in Engineering, vol. 2017, Article ID 4671892, 18 pages, 2017.

[2] W. H. Organization, “Global status report on road safety 2018: summary,” World Health Organization, Tech. Rep., 2018.

[3] I. A. Rai, R. A. Shaikh, and S. R. Hassan, “A hybrid dual-mode trust management scheme for vehicular networks,” International Journal of Distributed Sensor Networks, vol. 16, no. 7, Article ID 155014772093937, 2020.

[4] N. Gupta, R. Manaswini, B. Saikrishna, F. Silva, and A. Teles, “Authentication-based secure data dissemination protocol and framework for 5g-enabled vanet,” Future Internet, vol. 12, no. 4, p. 63, 2020.

[5] F. Al-Turjman and J. P. Lemayian, “Intelligence, security, and vehicular sensor networks in internet of things (Iot)-enabled smart-cities: an overview,” Computers & Electrical Engineering, vol. 87, Article ID 106776, 2020.

[6] M. Balta and I. Oz, “A stage fuzzy-decision tree model for traffic signal optimization in urban city via a sdn based vanet architecture,” Future Generation Computer Systems, vol. 104, pp. 142–158, 2020.

[7] M. H. Junejo, A. A.-H. Ab Rahman, R. A. Shaikh et al., “A privacy-preserving attack-resistant trust model for internet of vehicles ad hoc networks,” Scientific Programming, vol. 2020, Article ID 8831611, 21 pages, 2020.

[8] R. Iqbal, T. A. Butt, M. Afzaal, and K. Salah, “Trust management in social internet of vehicles: factors, challenges, blockchain, and fog solutions,” International Journal of Distributed Sensor Networks, vol. 15, no. 1, Article ID 155014771982582, 2019.

[9] I. O. Sumra, “Applications of internet of vehicle (Iov): a survey,” Lahore Garrison University Research Journal of Computer Science and Information Technology, vol. 4, no. 2, pp. 59–70, 2020.

[10] G. Usha Devi and M. Priyan, “A survey on internet of vehicles: applications, technologies, challenges and opportunities,” International Journal of Advanced Intelligence Paradigms, vol. 12, no. 1/2, pp. 98–119, 2019.
[11] T. Halabi and M. Zulkernine, "Trust-based cooperative game model for secure collaboration in the internet of vehicles," in Proceedings of the ICC 2019-2019 IEEE International Conference on Communications (ICC), pp. 1–6, IEEE, Shanghai, China, May 2019.

[12] I. Memon and H. T. Mirza, "Madptm: mix zones and dynamic pseudonym trust management system for location privacy," International Journal of Communication Systems, vol. 31, no. 17, Article ID e3795, 2018.

[13] A. Mishra, N. Gupta, and B. B. Gupta, "Defense mechanisms against ddos attack based on entropy in sdn-cloud using pox controller," Telecommunication Systems, vol. 77, no. 1, pp. 47–62, 2021.

[14] M. B. Mollah, J. Zhao, D. Niyato et al., "Blockchain for the internet of vehicles towards intelligent transportation systems: a survey," IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4157–4185, 2021.

[15] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proceedings of the 2010 IEEE INFOCOM, pp. 1–9, IEEE, San Diego, CA, USA, March 2010.

[16] Q. Kang, X. Liu, Y. Yao, Z. Wang, and Y. Li, "Efficient authentication and access control of message dissemination over vehicular ad hoc network," Neurocomputing, vol. 181, pp. 132–138, 2016.

[17] S.-F. Tzeng, S.-J. Horng, T. Li, X. Wang, P.-H. Huang, and M. K. Khan, "Enhancing security and privacy for identity-based batch verification scheme in vanets," IEEE Transactions on Vehicular Technology, vol. 66, no. 4, pp. 3235–3248, 2017.

[18] J. Sun, C. Zhang, and Y. Fang, "An id-based framework achieving privacy and non-repudiation in vehicular ad hoc networks," in Proceedings of the MILCOM 2007- IEEE Military Communications Conference, pp. 1–7, IEEE, Orlando, FL, USA, October 2007.

[19] N.-W. Lo and J.-L. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 5, pp. 1319–1328, 2015.

[20] W. Li and H. Song, "Art: an attack-resistant trust management scheme for securing vehicular ad hoc networks," IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 4, pp. 960–969, 2016.

[21] S. S. Kaushik, "Review of different approaches for privacy scheme in vanets," International Journal of Advances in Engineering & Technology, vol. 5, no. 2, p. 356, 2013.

[22] S. Wang, J. Wang, and Z. Yu, "Privacy-preserving authentication in wireless iot: applications, approaches, and challenges," IEEE Wireless Communications, vol. 25, no. 6, pp. 60–67, 2018.

[23] H. Chai, S. Leng, J. He, K. Zhang, and B. Cheng, "Cyberchain: Cybertwin Empowered Blockchain for Lightweight and Privacy-Preserving Authentication in Internet of Vehicles," IEEE Transactions on Vehicular Technology, vol. 71, 2021.

[24] J. Shen, T. Zhou, F. Wei, X. Sun, and Y. Xiang, "Privacy-preserving and lightweight key agreement protocol for v2g in the social internet of things," IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2526–2536, 2018.

[25] A. M. Almuaideb and S. S. Algothami, " Efficient privacy-preserving and secure authentication for electric-vehicle-to-electric-vehicle-charging system based on ECQV," Journal of Sensor and Actuator Networks, vol. 11, no. 2, p. 28, 2022.

[26] S. A. Chaudhry, "Comments on "a secure, privacy-preserving, and lightweight authentication scheme for VANETS"," IEEE Sensors Journal, vol. 22, no. 13, pp. 13763–13766, 2022.

[27] S. Liu and Y. Zheng, "Efficient Privacy Protection Protocols for 5G Enabled Positioning in Industrial IoT," IEEE Internet of Things Journal, 2022.

[28] E. Barker and Q. Dang, "Nist special publication 800-57 part 1, revision 4," NIST, Tech. Rep, vol. 16, 2016.

[29] M. Al-Bassam, "Sepki: a smart contract-based pki and identity system," in Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, pp. 35–40, Abu Dhabi, United Arab Emirates, April 2017.

[30] A. I. Taloba, A. A. Sewisy, and Y. A. Dawood, "Accuracy enhancement scaling factor of viola-jones using genetic algorithms," in 2018 Proceedings of the 14th International Computer Engineering Conference (ICENCO), pp. 209–212, IEEE, Cairo, Egypt, December 2018.

[31] M. M. Abdelgawd, T. H. A. Soliman, A. I. Taloba, and M. F. Farghaly, "Arabic Aspect Based Sentiment Analysis Using Bidirectional Gru Based Models," Journal of King Saud University-Computer and Information Sciences, 2021.