Machine Learning for Human Intelligence
2025, Vol. 3, Issue 1

Research Article

Trust Management and Data Authentication in VANETs

Syed Fakhar Bilal[1,⋆] and Sana Basharat[2]

[1]Faculty of Information Technology, School of Software Engineering, Beijing University of Technology, Beijing, 100124, China.; Email: fakhar.bilal@bjut.edu.cn
[2]Department of Computer Science, University of Management and Technology, Lahore, Punjab, Pakistan.; Email: sana.basharattt@gmail.com
⋆Corresponding author: Syed Fakhar Bilal (fakhar.bilal@bjut.edu.cn)

Article History

Academic Editor:
Dr. Muhammad Nabeel Asghar
Submitted: December 19, 2024
Revised: February 17, 2025
Accepted: March 1, 2025

Keywords:
User migration, SNS, SSLA, User switching intentions, PPM Framework

Abstract

The Vehicular Ad Hoc Networks (VANETs) have grown in popularity due to its capacity to provide both safety and non-safety services that rely on communication between vehicles and diverse network entities. However, it is crucial to understand that when using these services, malevolent vehicles may take advantage of the situation by spreading misleading information around the network for their benefit. As a result, vehicles must be authenticated to communication with other vehicles and network entities. The pairing-free and digital signatures have historically been the most widely used signature methods for this purpose, but they can place a heavy computational burden on vehicles during the authentication process. The signing numerous vehicles at once is difficult because the pairing-free signature techniques are often created for single users. The huge key size of digital signatures can also cause them to operate more slowly. In contrast to traditional digital signatures and pairing-free signatures, we uses the Boneh-Gentry-Lynn-Shacham (BGLS) signature scheme for vehicle authentication. The BGLS signature method does not rely on computationally expensive bi-linear pairing or conventional signature schemes. The proposed model emphasizes effectiveness while providing crucial characteristics like immutability, pseudonymity, decentralization, and scalability.

1 Introduction

The transportation has developed an intelligent system called Intelligent Transport Systems (ITS) with increasing urbanization and the most recent advances in autonomous vehicles. As of late, the ITS has acquired a lot of consideration in research due to the sustainability of transportation infrastructures. The researchers are focusing toward accidents avoidance, mishaps and presented a few active electronics and PC-controlled instruments. The ITS presented the smart vehicles those are controlled remotely through voice commands using a communication gadget called an On-Board Unit (OBU). There are numerous new directing plans and models have been recommended lately to empowered ITS effectively in vehicles.

The widespread organization of ITS is a challenging and perplexing task [1]. The principal objective of ITS is to give protected, compelling and dependable transportation systems to the society. There are many reasons why specialists need autonomy in ITS such as efficiency of drivers, improvement in energy consumption for clean and green climate, and the most importantly security of all users. The challenging task of the ITS is to upgrade the traffic stream and give traffic a complete sense of

security [2]. The Vehicular Ad Hoc Networks (VANET) have arisen an another amazing innovation because of their use for applications in Intelligent Transportation Systems (ITS) [3] as reconnaissance systems and well-being cautions on the road. The VANET is a Mobile Ad Hoc Network (MANET) that depends on enrollment tools, On-Board Units (OBUs) and Road-Side Units (RSUs). The OBUs are radios introduced as transmitters for all vehicles whereas the RSUs have network devices on road site. The RSUs are used for infrastructure communication and contain the network gadgets for short-range communication (SRC) [4].

With all the advantages of VANETs, there are some crucial challenges introduced including authentication and privacy preservation. The authentication includes message authentication [5] and vehicle identity authentication [6]. Message authentication refers to the authentication of messages sent and received by vehicles in the network, whereas identity authentication refers to the authentication of a vehicle's identification. Vehicle identity authentication is important because a malicious vehicle may impersonate a legitimate vehicle and cause damage to the network. Since, the malicious vehicles can do a lot of damage in the network including detouring the vehicles unnecessarily, spreading false information, etc. It is essential to authenticate the vehicles before they can send and receive messages in the network. Every vehicle that joins the network needs to be authenticated by an RSU. In recent literature, many schemes have been proposed that provide identity authentication in VANETs. These schemes utilize digital signature schemes (DSS) [7], pairing free signature [8] and blockchain [9] base signature schemes. Although these schemes provide secure authentication but still the high computation costs affect the whole network performance. Many vehicles may be resource-constrained, so these solutions are not practical regarding cost and efficiency at the same time. Blockchain-based authentication solutions suffer scalability issues in such networks [10, 11].

A solution is needed that ensures identity authentication in VANETs while ensuring the computational cost and storage expenses. An efficient identity authentication should provide anonymity and an unmatched verification model. A model that does not require a separate entity for remote authentication of databases to reduce deployment and computational costs. In this paper, we propose a Boneh-Gentry-Lynn-Shacham (BGLS) signature scheme to ensure identity authentication in VANETs. It offers the most secure signature schemes of the most recent models. The BGLS signature scheme provides 112-bit and 128-bit key sizes to ensure authentication security. An IOTA ledger (a distributed ledger for the Internet of Things) was deployed to manage group keys and critical updating in these vehicle groups. An IOTA is a lightweight and the first ledger with micro-transactions without fees as well as offered secure data transfer which does not suffer any scalability issues as observed in blockchain-based security solutions. Moreover, IOTA is quantum-safe and does not need miners which makes it quantum-resistant, and secure even in the presence of a stable quantum computer. These strengths make IOTA a better option for a distributed ledger technology than blockchain.

According to the World Health Organization (WHO), approximately 1.3 million people die due to car accidents annually, while 20-50 million people get non-fatal injuries, and a lot of individuals get a disability as a result of these road mishaps. Hence, road accidents are expected to become the fifth major cause of death by the end of 2030 [12]. Many of these road accidents occur due to authentication and identification issues of vehicles, pedestrians, and obstacles. A lot of vehicles do not allow drivers to have sufficient reaction time due to speed limits. In the case of unauthenticated vehicles in the network, the chances of privacy breaches and maliciously diverting traffic grow. Malicious vehicles may enter the network using identity theft and reputation to spread incorrect information. It is essential to make sure that the authentication of vehicles transmits genuine information. For vehicles that pose security threats, the authentication certificates must be revoked so that they cannot communicate with other vehicles in the network. Such vehicles can cause accidents, injuries and in the worst case death. Multiple users' signatures on numerous (potentially distinct) messages are combined in BGLS aggregate signature techniques to ensure the authentication mechanism. The current chosen-key security strategy is inadequate to protect against the possibility that an attacker may believe it is sufficient to fake a signature implicating one user rather than a specific user [13]. In addition, a pairing-free signature scheme was used in [8], but this was valid only for a single user. Also, in [7], the Digital signatures were proposed, but the key size was too large which is not practical due to increasing the computational cost. To address the above issues, we use a BGLS signature scheme that can sign multiple users

simultaneously, and its key size is not too large. A model is proposed for the security of the VANET. The following are the main contributions of the proposed model:

1.1 Contribution

- We manage keys and certificates, which provide immutability and pseudonymity without posing computation or storage overhead on vehicles.
- We replaced the traditional signature scheme used for the authentication of vehicles in the literature with the new BGLS signature scheme which is lightweight and fast because of its key size for its signature scheme.
- Our findings demonstrate the great efficiency of our system in terms of computing cost, throughput, end-to-end latency, and time efficiency.

1.2 ORGANIZATION

The remaining sections of the paper are as follows:

- **Section 2** describes our study model and review recent literature, much of which has its roots in security and signature scheme.
- **Section 2.1** The following section describes the Research Model where we implement and simulate BGLS, evaluate its performance, and show the results in graphs.
- **Section 3** focuses on the experiments conducted to evaluate the proposed method.
- **Section 6** Finally, the research summarizes the main findings, contributions, and potential areas for future research.

1.3 PROBLEM STATEMENT

Offering a suitable authentication mechanism is one of the most important difficulties in ensuring secure and effective communication for Vehicular Ad hoc Networks (VANET). Most popular signature schemes include pairing free and Digital signatures, which cause computation overhead on vehicles. Pairing-free signature schemes are implemented for single users, so it's difficult to sign multiple vehicles simultaneously. A digital signature can slow the progress of vehicles because its crucial size is high. Also, not all vehicles have resources, as most are resource-constrained, so signature schemes such as Pairing-free and digital signature schemes do not perform efficiently (in terms of computation). Hence, a signature scheme is required that will overcome the above limitations.

2 Related Work

Most VANET schemes associate vehicles at the base of a hierarchy of two or three levels with those in the same region. When vehicles reach the area, they request group membership and are given registration by entities at one of the higher levels. Once verified, cars are granted the means of collective communication. These keys could be group keys, symmetric keys, or asymmetric keys. Roadside units must verify signed messages in VANETs in a relatively brief period. The certificates aggregate signature (CLAS) approach has been regarded as a solution to the challenges of restricted network bandwidth and processing capacity in VANETs. In this paper, Han et al. [14] present eCLAS, an optimal pairing-free CLAS for communication among vehicles and infrastructure. Individual signatures on separate communications across various vehicles can be combined into a single shorter signature using the aggregated signature. The demonstration of the method's applicability in the arbitrary oracle model comes from the adaptive selection message assault and the difficulty of solving the discrete logarithm issue on the elliptic curve. In V2V communications, the vehicles communicate information about their driving surroundings, including speed and position, regularly. Manivannan et al. [15] provided

an overview of safe authentication and privacy-protection systems. It provides insight into VANET authentication, privacy, and message delivery issues. This study investigates protocols depending on public cryptography, identity-based encryption, pseudonyms, and group signing.

VANET networks are available to the community, and automobiles are entering and departing rapidly. As a result of this feature, two high criteria for VANET security emerge: The accuracy of the data that vehicles in a VANET convey should be their responsibility, and message security assurance systems must be rapid. [8] describe an efficient, pairing-free signature technique for VANETs that resists signer identity fraud, notably internal attacks, without using a tamper-proof component. A literature review of the latest papers and techniques. This methodology classifies entities among three categories: RSUs, TA, and OBUs. The OBUs are verified by the TA while signing messages, preventing the vehicles from creating false identities. OBUs generate sign messages, including data from car telemetry and traffic, which are then forwarded to surrounding cars and the TA. Furthermore, while their technique handles the main common sort of TA-level insider threat, the prospect of a fraudulent TA inappropriately issuing keys to illegal cars is not addressed. There has been presented a successful Model for authentication that protects privacy (EPAM) in [16] to address the issue of greater latency in membership verification for users in VANET with secret identifying demands. It is a three-part strategy, with initiation coming first, chain construction coming second, and authentication coming third. The suggested method assumes that OBU is an entirely unmodifiable component, [17] with virtually no opportunity for unauthorized read/write operations.

OBUs, however, are impenetrable when used. A tamper-resistant OBU is resistant to unauthorized read operations, although they are still prone to data leakage through side channels. For example, if a secret key is frequently used to sign numerous messages, it might be simple to determine from a succession of side-channel time-series data breaches (such as data on power usage, device sound, etc.) exposed throughout signature process invocation, [18] the architecture of a modern blockchain in which message and node trustworthiness are recorded in the block as transactions. To boost scalability, researchers have also recommended creating a distinct blockchain for each region, depending on geographic position. Furthermore, they have advocated using edge servers to offload heavy computing workloads to minimize block creation delays. Because VANETs operate in untrusted contexts, it is exceedingly difficult for vehicles to verify the legitimacy of transmitted event messages. To solve the security challenges on VANET. [20] presented a straightforward conditional privacy-preserving authentication (RCPPA) method based on ring signatures. The vehicle in the suggested technique acquires a pseudonym through a root trusted authority (RTA). If the vehicle performs an unlawful act, only RTA can determine the car's true identity. A vehicle creates a ring signature to sign a message. The signature is checked by vehicles within the communication range to confirm that the message was transmitted by an allowed vehicle.

The ring signature offers cars complete secrecy, but the RTA uses a pseudonym supplied in the transmission to disclose the identity. The most significant feature of this system is that it facilitates only authorized cars, not intruders, to set up ring signatures without collaboration from neighboring vehicles. Some systems mandate that all communications be handled by RSUs, prohibiting direct vehicle communication. According to one example from [21], symmetric keys provided by RSUs are unique to each vehicle and can only be used by that vehicle to establish a connection with the RSU. The system experiences an increase in latency as a result of adding an additional communication step and necessitates that all communications be processed by RSUs before re-transmission. Additionally, broadcast messaging is not allowed because every car shares a distinct key with the RSU. In VANETs, broadcast messaging is desired, hence most methods make use of group signatures or group keys in some way. The simplest systems in this category produce a single, shared symmetric key that each group member uses to communicate with the others [22, 27]. Sadly, insider attacks are a serious threat to VANET systems when everyone generates identical signatures with the same key. If each vehicle has a unique key and no ID verification is performed, it is highly challenging to identify or attribute attacks in which a rogue vehicle injects insufficient data or poses as another vehicle. Instead of making the key pairs for the cars themselves, RSUs will authenticate the public keys for the cars, avoiding insider attacks from jeopardizing the private keys [28].

A vehicle signs messages after being authorized and having its public key confirmed. Subsequently,

other automobiles use collaborations to verify the authenticity of the inscriptions and authenticate the communication. The approach is quite efficient because it allows for batch verification. However, it does not offer rapid message sender tracing in the event of a disagreement or the ability to recognize attacks like Sybil or masquerade attacks. It is possible to trace, but it necessitates a database search and one pairing computation for each car listed in the database. Two strategies developed by [25] for pairing-free solutions that are more recent, similar to the [26] scheme concerning signature generation and verification. Contrary to the second design [29], the first scheme [30] does not call for TPDs. The tracing process, however, necessitates that there is no direct way to track down the sender of the message because Once a match is made, TA looks through a database of previously saved values and displays the sender's actual ID. finally, due to the hacking of the TAs. Governments and businesses are developing or already have developed their own standards for VANET security in addition to those suggested by academic literature. IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages (IEEE 1609.2) [31], and Intelligent Transport Systems (ITS); Security; ITS Communications Security Architecture and Security Management are two crucial English linguistic requirements. 2nd release [32].

These standards, which call for the usage of certificate hierarchies akin to public critical infrastructure (PKI) models, were initially developed before a substantial portion of academic security research concentrated on VANET. For the purpose of signing communications, In order to preserve some amount of anonymity, OBUs are given a wide range of pre-installed certificates or permission tickets that they can switch out at predetermined intervals. In [40], a secure authentication technique that protects privacy has been proposed. Based on the vehicle's real identity, TA assigns it an internal pseudo-identification (IPID). After choosing an encryption key, the vehicle enters it into IPID and TPD. The vehicle creates a public pseudo-identity (PPID) following TA authentication before signing the message. To authenticate the communication, the recipient checks the signature. The automobile frequently modifies the IPID and encryption key settings to prevent information from leaking. This system also provides non-forgery, unlinkability, and confidentiality, and it is protected from side-channel attacks. The end-to-end delay of the communications is not discussed in detail, though. Based on the reputation that has been demonstrated, A safe, reliable, and adaptable cooperative downloading technique employs a selection mechanism and ordered signatures [41]. The only vehicles selected as proxy vehicles in this will be those with the highest predicted downloading capacities. By offering authentication, message secrecy, privacy protection, and process authentication, this system offers robust security.

2.1 Proposed Model

2.2 VANETs

A predefined architecture is needed for communication in VANETs. In the network, the vehicle is the critical entity that transmits over the wireless medium with being OBU-equipped. The wireless is WAVE (wireless access in the vehicular environment). The data is exchanged between the vehicles and other infrastructure through the OBUs. AU (Application Unit) is another device used in coordination with the OBU to connect with other services [42] and for communication in the network. The other components in the architecture are:

1. Cell Phones (also referred to as pedestrians).
2. RSUs (roadside fixed devices).
3. Cell towers (providing services like 3G/4G/5G to VANETs)
4. UAV (Unmanned Air Vehicle), FANET component for the assistance of VANET system.
5. Servers of a different kind (Application, authentication, location).

2.3 VANET Features

Most of the characteristics of VANETs are inherited from MANETs, as VANET is its subclass. The VANETs have unique characteristics [43], thus having the following features:

- No energy constraints: The capacity of the battery to store energy for a more extended period has an extra facility of charging during driving. Thus, the energy constraint is removed that exists in other wireless networks.
- Rapid topology change: There is a frequent change in the topology due to the remarkably high speed of the vehicles. These changes quickly influence congestion applications and routing algorithms.
- Highly Computational: Less time-consuming and more efficient results are generated due to using modern and strong CPUs in the calculations.
- Insecure communication: Due to the nature of the wireless medium, the information exchanged in the process is a challenging task.
- Predictable mobility pattern: The movement of the vehicles is only on the roads and highways; thus, the mobility pattern is predictable.
- Safety: The ability of V2V (vehicle to vehicle) communication in VANETs made possible the awareness of the environment, thus increasing safety.
- Dynamic density: Due to constant changes in topology, there are spatial and temporal variations in the network's density.

2.4 VANET-Based Intelligent Transport System:

The point of the ITS is to upgrade the traffic stream and give traffic security. Vehicular Ad Hoc Networks (VANET) have arisen as another amazing innovation because of their applications in intelligent transportation systems (ITS), reconnaissance systems, and well-being cautions on the road. VANET is a MANET that depends on enrollment tools, onboard units, and roadside units (RSUs). The OBUs are radios introduced as transmitters for all vehicles in each vehicle, whereas the RSUs have network devices on the road. RSUs are used for infrastructure communication and contain the network gadgets for short-range communication (DSRC). We divided them dependent on the fundamental motivation behind VANET-based ITS: blockage evasion, crossing point control, crisis management, and accident-avoidance [44].

In the VANET Architecture, wireless access in vehicular environment (WAVE), a distant invention, is primarily used for vehicle and RSU communication. The primary obligation of VANETs is to deliver successful communication; fundamentally, the hubs require explicit highlights to procure data, coordinate, and, afterward, make choices dependent on all data gathered by utilizing cameras, sensors, GPS collectors, and unidirectional receiving wires. As of late, VANETs are acquiring much consideration in mobile and wireless technology for communication. It includes vigorous plans for the intelligent transportation system (ITS). MANETs and VANETs are very different regarding high hub versatility, problematic channel and network architecture, deadline time, driving conditions, less dependability, and organization discontinuity [45].

2.5 VANET Applications

The information is gathered and processed to know the environment around the vehicles better through the information collected from different sensors and GPS devices. The information is then spread out in the vicinity [46]. Researchers have suggested several VANET applications implemented under various projects. These applications can be divided into various categories: Safety Applications: The main aim is to make decisions, improve road safety, and warn drivers about emerging situations [47] to avoid accidents. Examples of safety applications are pre-crash sensing, traffic signal violation warnings, emergency brake lights, lane change warnings, and so on.

2.6 VANETs Communication model and Standards

Communication in VANET is V2V, V2I, and V2B. The VANET is utilized for short-range transmission among the versatile host vehicles, RSUs, and vehicles. RSU has been taken as one of the critical pieces of VANET because of the designation limit for conveyance habitats for consolidated tasks. Generally, the upkeep and establishment costs related to RSUs are amazingly high. An essential model of VANET is displayed. In like manner, due to different difficulties, for example, the arbitrary dissemination of RSUs and the significant level of responsibility, analysts have suggested the usage of left-hand vehicles as an augmentation of RSUs. These vehicles are responsible for dispensing occupations to RSUs and giving vehicles access appropriately [44]. The VANET typically consists of three levels: the top-level semi-trusted Road-Side Units (RSUs), middle-level TA and/or SP, and bottom-level vehicles with on-board units (OBUs) for processors. [48].

1. **TA/SP LEVEL:** A server or servers of the highest caliber, with a high degree of confidence Identity identification, access to informational or entertaining services, or combined may be offered at this level.

2. **RSU LEVEL:** For close proximity interaction with the OBUs, the majority of VANET systems contain an intermediate level of hardware nodes, which are often fixed devices put beside highways. Authorities install and manage these devices, but they are typically only partially trusted because of their exposure to the outside world and the potential for hardware manipulation. The demand for specialized relay hardware will probably decline as 5G networks spread.

3. **O**BU LEVEL: In a VANET, every vehicle has an OBU installed. These OBUs serve as the system's fundamental nodes. OBUs are more effective since cars may offer plenty of room and electricity, as shown in [49]. Additionally, versus numerous other IoT systems, a vehicle's relatively high cost implies that processing cost is less of a concern. OBUs should be regarded as untrusted since, like other consumer IoT devices, they are controlled by humans and susceptible to physical attacks[50].

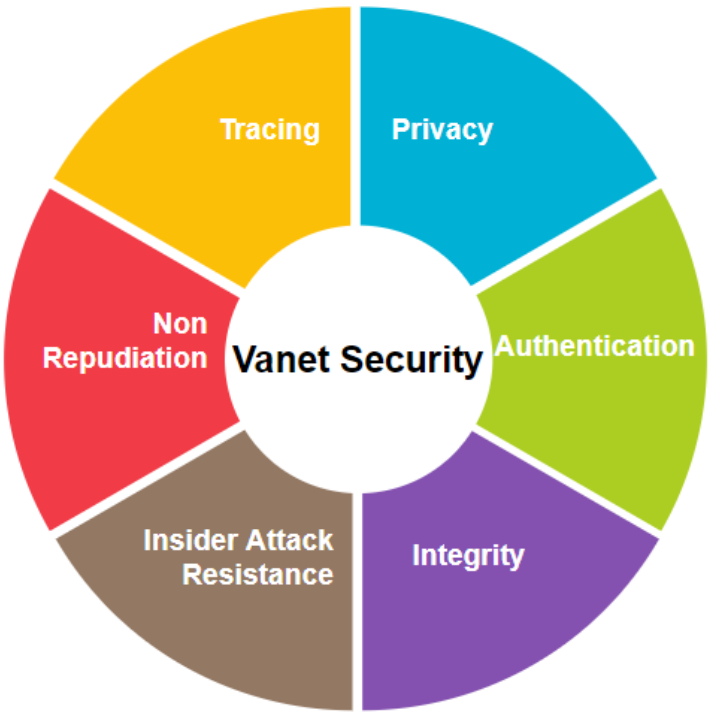

Figure 1: VANET Security

In this research, we introduce our proposed system model. We discuss the model proposed and the flow of tasks divided between different entities in our system. In order to secure identity authentication in VANETs, numerous approaches have been proposed. A lot of schemes have challenges associated with computation and storage resources. Because many vehicles are resource-constrained, it is essential to ensure that the authentication mechanisms are not computationally expensive. This research provides an identity authentication model based on IOTA that makes use of the BGLS signature technique. Multiple users' signatures on numerous (potentially distinct) messages are combined in BGLS aggregate signature techniques. Their current chosen-key security strategy is inadequate to protect against the possibility that an attacker may believe it is sufficient to fake a signature implicating one user rather than a specific user [13]. In addition, a free signature scheme was used in [8], but this was valid only for a single user. Also, in [7], Digital signatures were proposed, but the key size was too large, increasing the computational cost. To address the above issues, we use a BGLS signature scheme that can sign multiple users simultaneously, and its key size is not too large. In the following section, we will introduce our proposed scheme used in vanets.

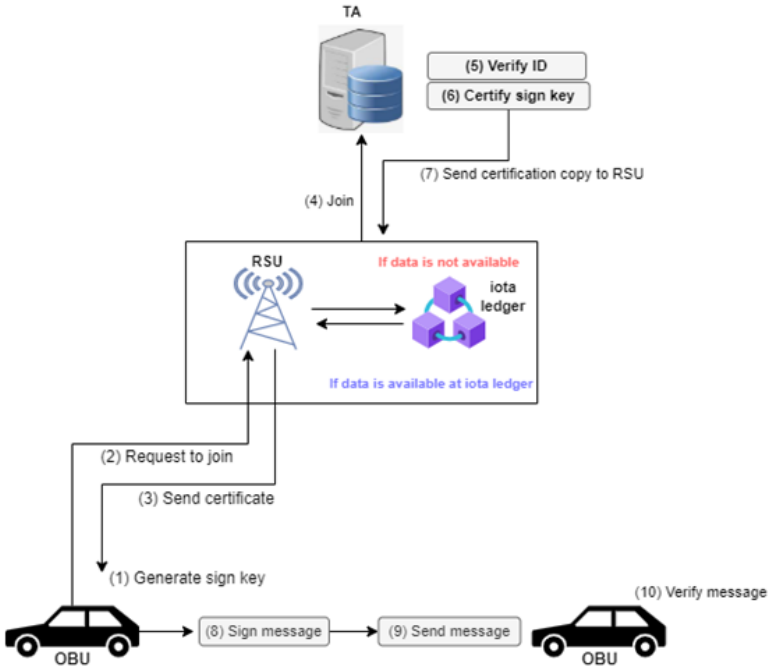

Figure 2: The proposed system Model

2.7 VANET SECURITY:

The great member mobility of VANETs when compared to other IoT systems stands out as being particularly noteworthy [50]. Due to its mobility, group membership changes more frequently than it does in other MANETs or other IoT applications. Group membership can fluctuate at highway speeds in heavily populated areas every 140 ms or more[51]. Members should not be trusted because wireless connections and group membership are both public information.

1. **INTEGRITY:** Secure communications systems, including VANETs, depend on message integrity to function properly. Systems need safeguards against both intentional and unintentional message corruption, or at the very least, the ability to identify it. Message integrity checks also make sure that message data isn't changed as it moves between nodes to create a legitimate message with a fraudulent message.

2. **AUTHENTICATION:** Message integrity by itself is insufficient to build secure VANETs, as is the case with the bulk of security applications. The system must also make sure that only parties with the necessary permissions can send messages to the system. Identity verification stops

Algorithm 1 BGLS Verification Algorithm

procedure BGLS Verification Algorithm

Input: pp: system public parameters.

Output: the signature of message M.

Process:

Step 1: M or M_1 .... M_n: the messages to be signed.

Step 2: ssk_u the secret signing key for V_i conducting the signature procedure

Step 3: **if** Single message M

1. Choose a random number r in Z_p^*

2. Compute: $\sigma = (\delta) = H_1\ (\mathrm{M})\ .\ z_2^{-r})^{\alpha}, r)$

end if

if Multiple messages $M_1 .... M_n$

1: Choose random numbers r_1, r_2, r_n

Compute $\sigma_i = (\delta_i = (H_1\ (M_i) \cdot z_2^{-r})^{\alpha}, r)$

Aggregate signature as follows:

Compute r = $r_1 + r_2 + r_n$

Compute $\delta = \delta_1 + \delta_2 + \delta_n$

Set $\sigma = (\delta, \mathrm{r})$

end if

end procedure

hackers from accessing the system with altered or fraudulent credentials. Message authentication prevents outside attackers from injecting fake data into the system.

3. **PRIVACY:** In the VANET, privacy refers to both safeguarding drivers' true identities, and personal identification, and prohibiting message linkage. Associating two or more messages with the same vehicle is referred to as message linkage. For instance, pseudo-IDs are widely used in systems to conceal the true identities of message senders [52].

4. **NON-REPUDIATION:** A vehicle cannot hide or deny that it was the source of the communication according to the non-repudiation property. In order to correctly identify hostile cars that try to inject false data or otherwise obstruct the VANET's operation, non-repudiation is necessary. For the purpose of detecting Sybil's attacks, it is very important. In a Sybil assault, a single vehicle poses as multiple vehicles, typically to trick the system into believing something

Algorithm 2 BGLS Verification Algorithm

procedure BGLS Verification Algorithm

Input: pp: system public parameters.

Output: True/False: the result of signature verification.

Process:

Step 1: M or M_1 .... M_n: received message

Step 2: σ the signature of received message M or M_1 ....M_n

Step 3: pvk_u: the public key of UAV_i used to conduct the signature procedure

Step 4: **if** Single message with the signature (M, σ)

1. check (δ, g_3) = (H_1 M z^2 , η.

2. **return** True if equation holds; False if the reverse.

end if

if Multiple messages M_1....M_n with the signature σ

Compute H = H_1 (M_1) $\cdot$ $H_1(M_2)$ $\cdot \cdot \cdot \cdot \cdot$ $H_1(M_n)$

Verify the aggregative signature with the following equation:

e (δ, g_3) = (H_1 M z^2 , η.

return True if equation holds; False if the reverse.

end if

end procedure

it is not. For instance, a Sybil attack may "out-vote" honest vehicles to simulate high traffic or cause a fraudulent accident report [53].

5. **INSIDER ATTACK RESISTANCE:** VANETs are utilized by the general public and have highly dynamic membership, making it easier for attackers to join the system. An attacker can freely join the system if they steal or counterfeit an identity certificate. The OBU-level entities must therefore be completely untrusted. Their behaviors need to be carefully watched. Attacks via compromised TAs or SPs have a different potential to take into account. In order to accept harmful vehicles into the system, compromised TAs might work with them. Attackers may use stolen keys to sign communications, start Sybil attacks, or target innocent automobiles, as depicted in igure 1.

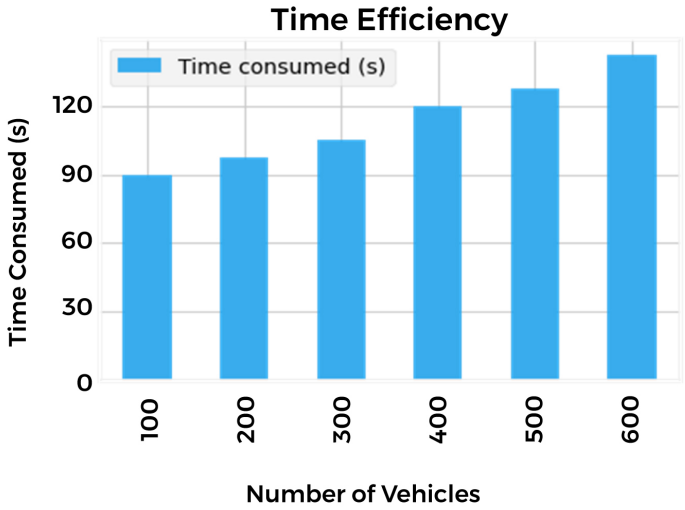

Figure 3: Time efficiency

2.8 System Model

The usual TA-RSU-OBU VANET hierarchy is used in the proposed scheme. We will now quickly review the functions.

2.9 TA Level

To authenticate automobiles that want to join the system, the TA makes use of a powerful central server linked to administrative databases. The TA is also in charge of verifying vehicle keys to make sure that vehicles are unable to sign messages under a false name and tracking down the genuine identities of message signers in the event of a disagreement.

2.10 RSU Level

RSUs are solely used as wireless messaging relays in the proposed configuration between the radio signals of the vehicles and a hard-wired link to the TA. They do not perform any other roles.

2.11 OBU Level

Every car has OBUs, which are tiny chips that allow for safe communication with other vehicles. When a vehicle requests to join the system, OBUs already have the certificates that have been duly signed and are necessary for vehicle authentication. Additionally, they produce, store, and communicate with the TA to certify their message signing keys, which is necessary to produce legitimate signatures. In this study, we use the BGLS signature technique to authenticate automobiles as they enter the network. These automobiles have been verified collectively. When cars group together, the corresponding RSU signs a group key for each group. These group keys are kept on the IOTA ledger depicted in Figure 2, together with each vehicle's public key and certificate.

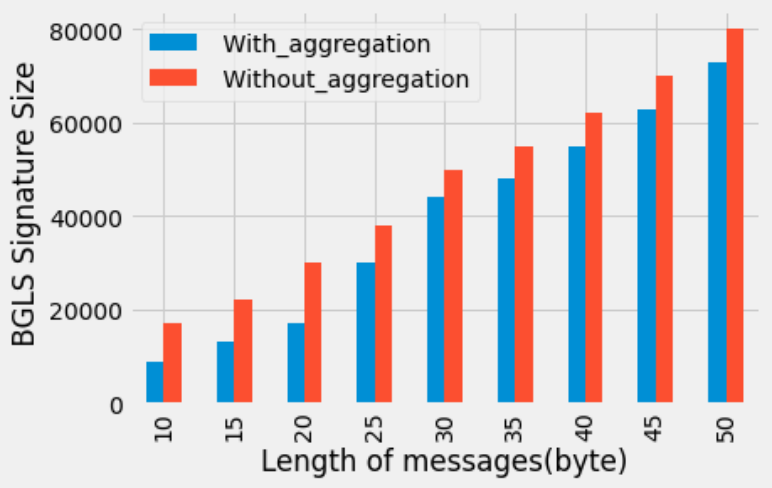

Figure 4: signature size

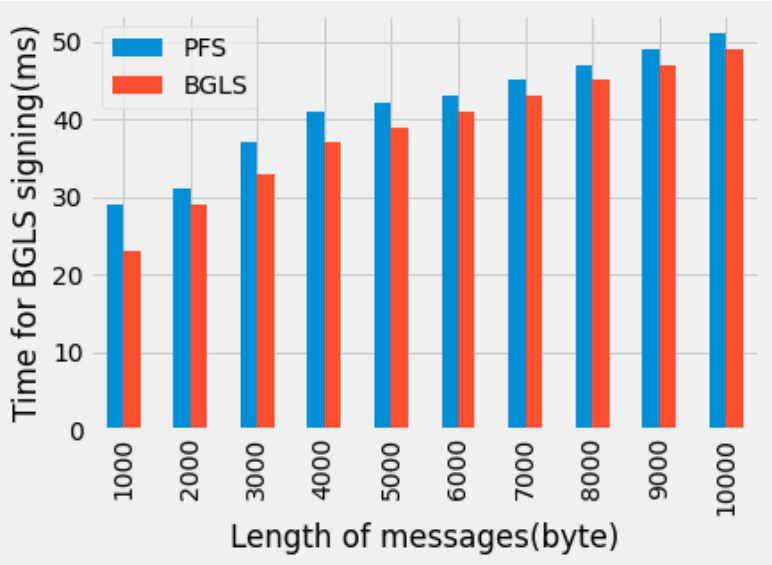

Figure 5: time for signing

2.12 System Setup

When a security parameter λ is entered, the TAs generate two groups of $G1$ with the same order q; $G1$ is a cyclically additive group, and $G2$ is a cyclically multiplicative group.A bilinear map is accessible $e : G1$ times $G1toG2$, and P is a $G1$. PKG chooses a random number $s \in Z_q^*$ and calculates $P_{pub} = sP$, where s is used for partial private key generation and is only known to PKG. TRA includes a random number $\alpha \in Z_q^*$ and calculates $T_{pub} = \alpha\ P$, where α is used for pseudo identity generation and is only known to PKG. TAs choose four cryptography hash functions: $H0 : [0,1]^* \rightarrow G1$, $H1 : [0,1]^* \rightarrow G1$, $H2 : [0,1]^* \rightarrow Z_q*$, and $H3 : [0,1]^* \rightarrow G1$. Then they publish $< q$, $G1$, $G2$, e, P, P_pub, T_pub, $H1$, $H2$, $H3$, $H4 >$ as the public system parameters.

2.13 Pseudonym generation

The vehicle should receive the pseudonyms before the VANET is included. The identity that uniquely identifies the vehicle cannot be used during communication to achieve anonymity. A V_i vehicle selects a random number $ki \in Z_q^*$ calculates the random number $PID_i, 1 = k_iP$, and then sends the car to TRA in a safe method $(RID_i, PID_i, 1)$. Following receipt $(RID_i, PID_i, 1)$, first, TRA verifies if RID_i is available in the local database and then calculates PID_i,2 = RID_i H0 (α PID_i, 1, V P_i) in which VP_i is the PID_i-period. Then a safe channel transfers the PID_i = (PID_i,1, PID_i,2, V P_i) to PKG.

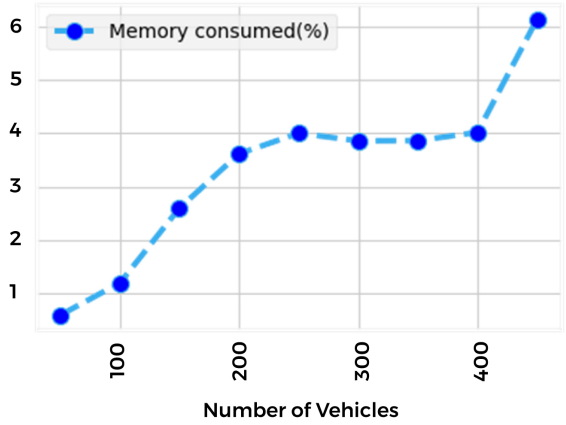

Figure 6: Energy consumption

2.14 Partial key generation

Given a PID_i pseudo identity, PKG calculates $= H_3(PID_i), psk_i = sQ_i$ and places psk_i as a private partial key. Then PKG (PID_i, psk_i) is transmitted to the truck. The PKG key pair (P_pub), α, is a partial private password. By evaluating if $e(psk_i, P) = e(Q_i, P_pub)$ equals or not, the car may verify precision. The store in the OBU the corresponding pseudonym and partial private key. In the plan and the alias and incomplete key age stage, we apply the pre-loading strategy [46] to use various brief period pen names for halfway private keys. After proper authentication between cars or TAs across a safe channel, the aliases are renewed on halfway private keys.

2.15 Vehicle key generation

The vehicle V_i determines the secret key vsk_i by selecting a random number $x_i inZ_q$ and calculating the vehicle public key $vpk_i = x_iP$. The message is authenticated and trustworthy to assure that conveyed by automobiles shall be endorsed. We divide the signing phase into 2 phases in our design. If the vehicle reaches an area under the inclusion of another RSU, it includes a preview, and the results are stored in the TPD. In the next step, the vehicle uses the results determined in the first phase to produce a signature when it has to sign a message.

1. In another RSU region a V_i vehicle first appears as $H_J = H_1(\ 1DR_j)$, $Sc_i = Pa_sk_i + vrk_i$ Hr_j and is saved in TPD. If V_i is subject to the inclusion of R_j, H_j and S_i should possibly be determined once. The vehicle should be recalculated when it leaves the current territory and enters another area.

2. At the point that a car V_i needs a message m_i, it's anything but a PID_i pseudonym, and it's used as the time stamp to choose the current time. Where do you give the new feature of the signposted message to the response? The number of $R_i = r_i$P is arbitrary and the $r_i = r_i$ is calculated. Then, ascertain $h_i = H2m_i$, PID_i, V_p k_i, IDR_J, $T_i = h_i + heyS_i$ at this moment. Ultimately, $i = (R_i,\ T_i)$ is the PID_i signature. Then, at that time, V_i sends RSU to close PID_i,m_i, vpk_i, t_i,i.

Figure 7: IOTA Transactions Interface

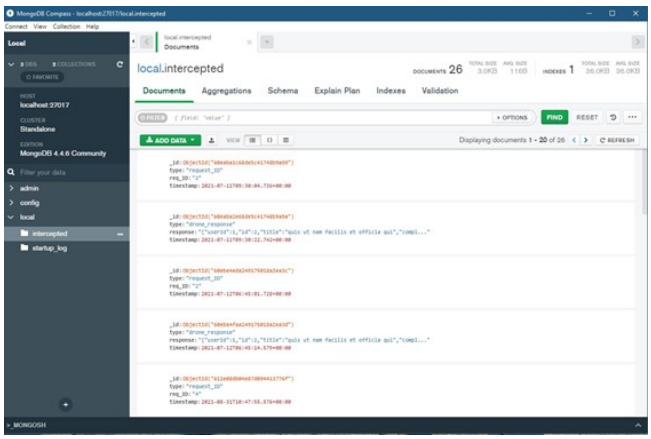

Figure 8: IOTA Transactions Storage in MongoDB

3 Results and Discussion

In this research, we evaluate the BGLS signature scheme.

4 Experimental settings

We implement BGLS in Python 3.8.10, on a RYZEN 5 4500 @2.3 GHz, 16 GB RAM and 512 GB SSD. We compare BGLS with [8] because this scheme is closely related. This scheme utilizes the IOTA ledger and BGLS to provide identity authentication. Also, we use omnet++ for the graphical representation of vehicle communication. Although this scheme ensures vehicular authentication, it suffers from

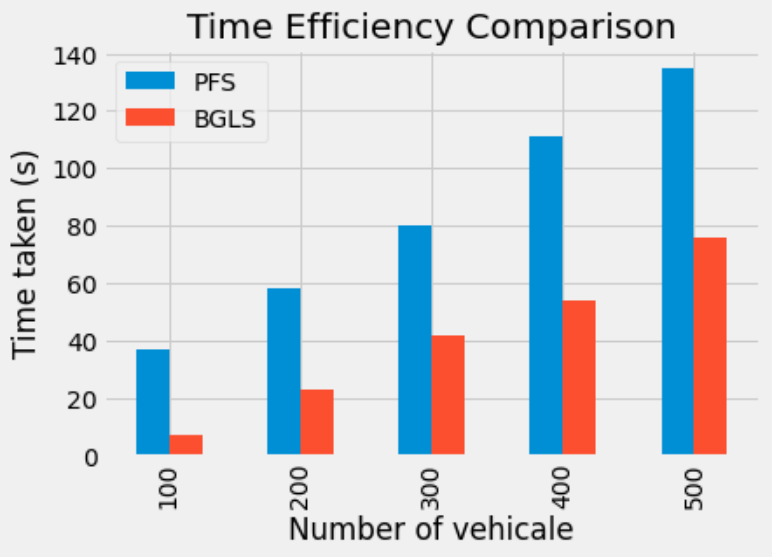

Figure 9: Time efficiency comparison

high computation and storage costs. In order to address these issues, we suggest a lightweight model for vehicles with limited resources. The computational ability of a vehicle's OBU is included in the Vehicular OBU Capability (VOCC) Dataset. This computer capacity includes RAM processing power, memory storage, node spacing, network transmission speed, and trust level. The dataset contains 4600 records that can be utilized in distributed computing paradigms including vehicular edge computing, vehicular fog computing, vehicular cloud computing and volunteer computing based on VANETs, which makes use of the processing power of moving automobiles. The computing method is better suited to vehicles with larger resources. We evaluate our scheme in terms of four parameters:

- Time efficiency
- Throughput
- Energy consumption
- computational cost

4.1 Time Efficiency

We evaluate the BGLS signature scheme in terms of the time it takes to run the code. We observe that BGLS is efficient in terms of processing time. The results for this experiment are given in Figure 3. On the x-axis, the processing time is shown in seconds, while the y-axis shows the network size. The minimum number of vehicles taken is 100, whereas the maximum number of vehicles is 500, as given in Figure 3, and from 100 to 500 vehicles, the time taken stays within 4.5 seconds. The Figure 5 shows that the processing time of BGLS does not grow linearly with the number of vehicles. The time recorded for different numbers of vehicles varies slightly. The difference is in milliseconds. However, the first decimal point stays the same. For example, the time taken to run the code for 100 number of vehicles is 4.5213 seconds, while the time recorded for 200 number of vehicles is 4.5248. Similarly, the time recorded for 300 number of vehicles is 4.5271. For 400 and 500 vehicles, the time taken is 4.5287 and 4.5291, respectively. Because VANETs have a dynamic structure and the vehicles keep entering and leaving the network constantly, the network size keeps changing. At one time during the day, traffic density may be low, whereas at other times, the traffic may be highly dense. Also, vehicles are highly mobile and do not stay in the network for an extended period. Vehicles are authenticated when they enter the network. This makes it essential to ensure that an authentication model proposed for VANETs is fast so that vehicles do not have to wait for the authentication process for a long time. Also, we check the time for BGLS signature size with aggregation and without aggregation shown in

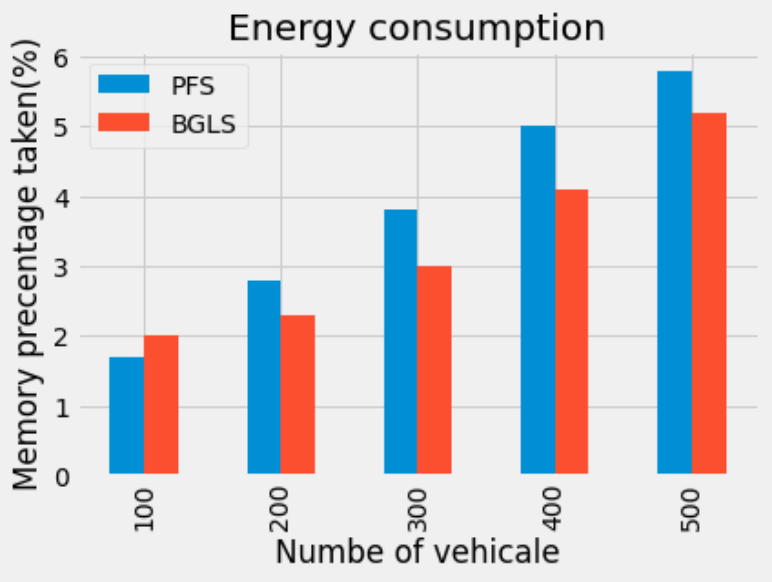

Figure 10: Energy consumption comparison

Figure 4 and Figure 5, respectively. It can be concluded that BGLS ensures time efficiency even when the network is extensive. Figure 3 shows that our scheme does not take longer than 4.5 seconds for any number of vehicles up to 500. This means BGLS does not pose a computation overhead even when the network is extensive. It can be said that BGLS is scalable in terms of time efficiency. The processing time does not increase with the growing size of the network.

4.2 Energy Consumption:

We evaluate our scheme in terms of the energy consumed by memory usage. In this experiment, we determine the memory percentage consumed by the code. The results of this experiment are shown in Figure 6 where the X-axis presented the number of vehicles and Y-axis percentage of memory consumed by BGLS. The minimum value taken for the x-axis is 1.85, and the maximum is 2.05. In Figure 6, for this experiment, the minimum value for energy consumption has been recorded to be 1.9415 %, and the highest value recorded is 1.956%. From 100 to 500 vehicles, the energy consumed by BGLS stays between 1.940% to 1.956%. We have observed in the time efficiency experiment that BGLS does not take long to authenticate the vehicles. Similarly, the energy consumption must also be low. We assume that the vehicles entering the network may be resource-constrained, which is why these vehicles may not be able to go through the authentication process if the authentication scheme requires a lot of resources. Our results for energy consumption in Figure 6 show that the growing number of vehicles does not lower the performance of BGLS. Energy consumption does not grow with a growing number of vehicles. At some point during the day, the traffic density may be high. To ensure large-scale authentication, it is essential to make sure that the authentication scheme does not require a large number of resources when the number of vehicles is increased. As our energy consumption graph stays straight and does not grow with the network size, it can be concluded that BGLS is scalable in energy consumption, i.e., it allows large-scale authentication without requiring a lot of resources. By looking at the results of this experiment, it can be concluded that when traffic is dense and the number of vehicles is high, BGLS does not require a higher number of resources.

4.3 IOTA Storage:

IOTA stores all the transactions in its database securely for long-term use. Figure 7 shows all the transactions stored in IOTA. The Figure 8 shows the MongoDB database where all the valid transactions are stored. The IOTA transfers transactions to the DB after the validation process. Only those transactions are stored which are validated to avoid any ambiguous data.

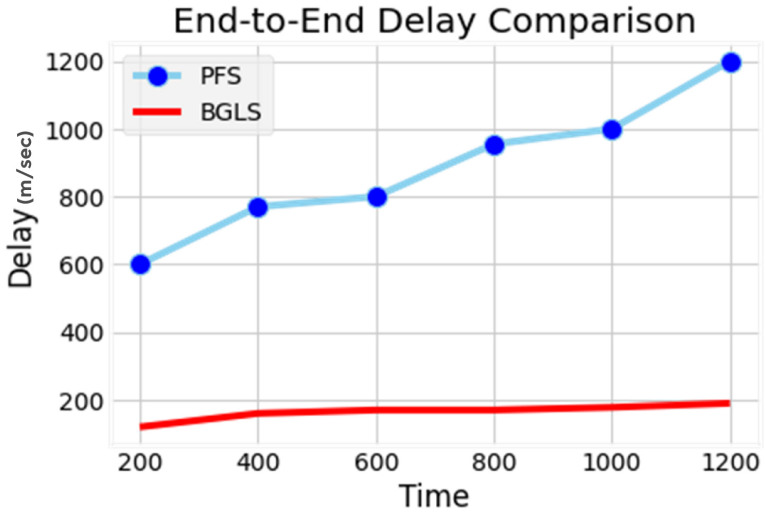

Figure 11: End-to-end delay comparison

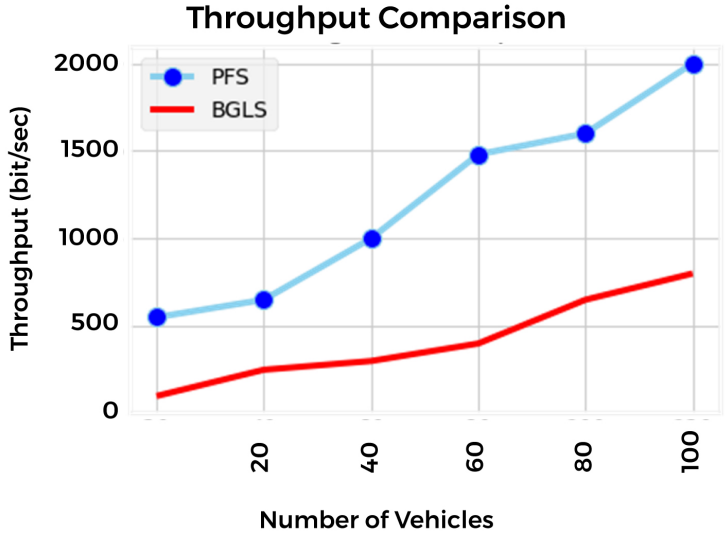

Figure 12: Throughput comparison

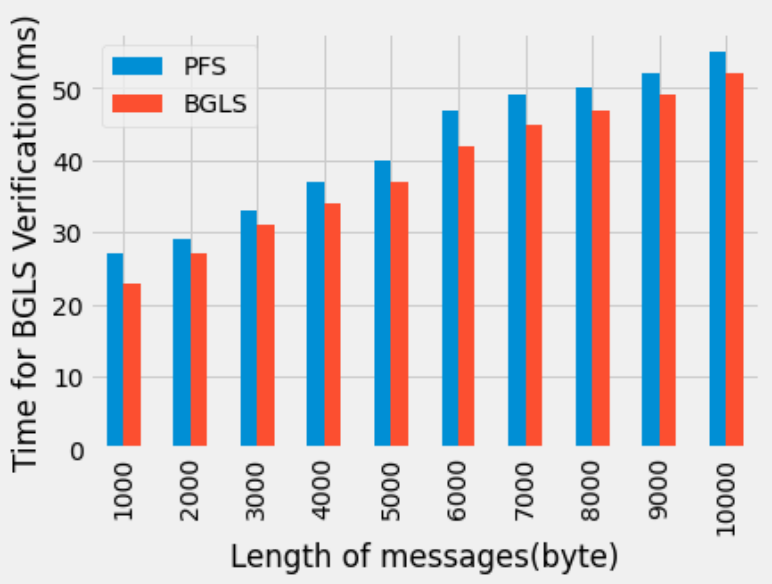

Figure 13: verification time

5 Comparison of Results

As stated earlier, we compare our results with [8]. This scheme works in the same network setting as BGLS.IOTA transaction interface and IOTA transaction storage in MongoDB are shown in Figure 7 and Figure 8, respectively.

5.1 Time Efficiency:

In this experiment, we evaluate our results regarding time efficiency and compare them with pairing free signatures [54]. In Figure 9, we compare our results for the same experiment with pairing free signature. It can be seen that the time taken by BGLS stays almost the same with different numbers of vehicles, which is not valid for pairing free signature. In the case of pairing free signature, the time taken keeps increasing with an increasing number of vehicles. We record the time taken in seconds. For 100 vehicles, the value recorded is 33 seconds, while the value recorded against 500 vehicles is above 120 seconds for pairing free signature. However, in the case of BGLS, the time taken for 100-500 vehicles stays below 5 seconds and does not grow with the growing network size. As seen in Section 1.1, blockchain suffers from scalability issues. In this experiment, we have observed that pairing free signature suffers from scalability problems, i.e., when traffic density is high, this scheme fails to perform efficiently. These two factors influence the performance of this scheme. Not only does the time taken for this scheme grow largely with growing network size, but it takes longer as compared to our scheme even when number of vehicles is minimal. The minimum number of vehicles that we consider in our results is 100. It can be concluded that BGLS is more scalable in terms of time efficiency as compared to pairing free signatures. The performance is not reduced when there are more automobiles on the road. IOTA ledger is lightweight, and it does not require miners or computationally expensive proof-of-work. This makes BGLS more efficient as compared to pairing free signatures.

5.2 Energy Consumption:

A comparison between the energy consumption of BGLS and pairing free signature is given in Figure 10. It is observed that BGLS utilizes a lower amount of energy as compared to pairing free signatures. The minimum value recorded for BGLS is 1.9416%, and the highest value is 1.956%. The energy consumed by BGLS does not exceed 1.9810% with any number of vehicles. The minimum value recorded for pairing free signature in the same setting is 1.65%, and the highest value is 6.12%. This shows that the energy consumed by pairing free signature is much higher than BGLS and keeps increasing with

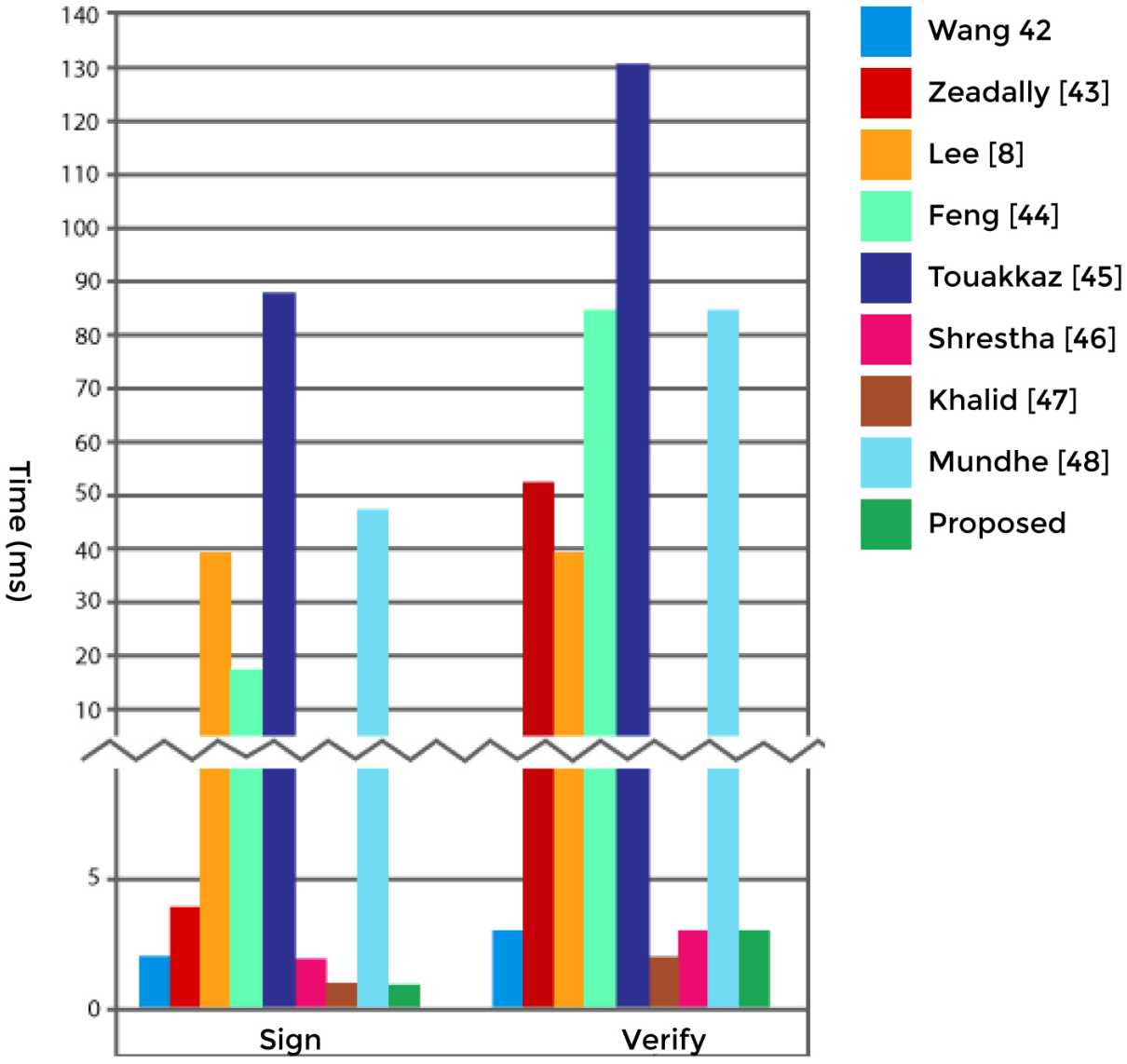

Figure 14: Performance comparison

increasing network size. VANETs require scalable systems because the network size keeps fluctuating throughout the day. For peak hours and urban areas, the model proposed in [8] is not scalable, requiring more resources. However, BGLS is scalable, i.e., it does not require more resources with a growing network size.

5.3 End-to-end Delay:

In this experiment, end-to-end delay is used to evaluate BGLS. When RSUs authenticate vehicles, they receive public and private key pairs. We compute end-to-end delay for this V21 communication. The results are given in Figure 11. Time is plotted on the X-axis, and end-to-end delay is shown on the y-axis in seconds. It is observed that BGLS is efficient in terms of end-to-end delay compared to pairing free signature. The smallest and largest values of end-to-end delay for pairing free signature are 587 and 1054, respectively, while the smallest and largest values in the case of BGLS are 100 and 213, respectively. This shows that BGLS has a lower end-to-end delay as compared to PFS. The formula below can be used to determine end-to-end delay: Transmission delay, Length, and size of data packet. $Ttrans = L/R$

5.4 Throughput:

We evaluate BGLS concerning the throughput achieved. The throughput in BGLS refers to the throughput of the communication going on between vehicles and RSUs when key pairs are assigned to vehicles. It is important to ensure higher throughput because vehicles keep entering and leaving the network at all times. Throughput results are given in Figure 12. We observe that BGLS has an optimal throughput. When compared with pairing free signatures, our scheme has higher throughput. In Figure 12, it can be seen throughput of BGLS increases with time and stays more than that of pairing free signature for all the values recorded. The formula below can be used to determine throughput: $T_r = I_n/F_v$ where: T_r = Throughput. I_n = Inventory (no. of vehicles signed per second).

5.5 BGLS Verification:

We observe that BGLS verification takes less time. Compared with pairing free signature, our scheme has a less verification time, as shown in Figure 13.

5.6 Computational Cost:

This section contrasts the size of messages with and without the suggested signature. Only the size of the signature component will be taken into account since it is assumed that the message content in all of the examined schemes is similar. For pairing-based schemes, this analysis employs G elements with a size of 128 bytes and pairing-free schemes with a size of 40 bytes [8]. Timestamps are 4 bytes long and Z p's elements are 20 bytes long. According to the research, the suggested scheme's signature length is comparable to that of existing pairing-free schemes, all of which are noticeably lower than pairing-based schemes' signature lengths. With only 20 bytes of additional signature length and without requiring the TPD necessary by two of the three pairing-free methods now in use, the proposed technique increases resistance against TA-level insider attacks caused by key material theft, as shown in Figure 14.

6 Conclusion and Future Work

In the most recent literature, numerous solutions have been put up to ensure the authentication of vehicles in VANETs. Most of these solutions utilize pairing free and digital signatures, which are computationally expensive. For vehicles that do not have enough computation resources, these schemes are impractical. For key management, many proposed solutions in recent literature utilize blockchain. Blockchain requires a mining process, which is computationally very expensive. Miners need to solve a puzzle that all network participants cannot solve. The proof-of-word that is used by blockchain is not practical for vehicles that do not have enough storage and computation resources. These factors

motivate this research. For resource-constrained vehicles, computationally expensive authentication mechanisms are not suitable, including blockchain, pairing free signature, digital signature scheme, and so on. As a result of identity authentication of vehicles in the network, vehicles are assigned a public and private key pair. Some vehicles may not have enough storage resources to store the keys and certificates. In this research, we propose BGLS, a lightweight identity authentication and critical management model. We utilize BGLS signature for identity authentication, which is lightweight and the fastest. To reduce the computations further, we use BGLS. As a result of identity authentication, vehicles are assigned public and private key pairs, along with certificates. To manage these keys and certificates, the IOTA ledger is used for key management. IOTA ledger is more lightweight as compared to blockchain. IOTA ledger does not require miners because adding a node on the ledger is not a computationally expensive task, which can easily be performed by resource-constrained vehicles. Because our focus is efficiency, we evaluate our scheme in terms of time efficiency, energy consumption, end-to-end delay, computation overhead, and throughput. It is observed that BGLS does not pose a computation or storage overhead on any entities in the system. The consumption of time and energy varies very slowly as the number of vehicles increases. We test BGLS with 100-500 number of vehicles. The graphs show that BGLS is efficient even when traffic is dense. We compare our results with a recent pairing free signature scheme and blockchain. It is observed that this scheme lacks efficiency when traffic is dense. Our results show that BGLS is efficient in energy consumption, time efficiency, end-to-end delay, and throughput compared to the model, which utilizes blockchain and traditional signature schemes. In the future, BGLS can be integrated with machine learning to learn authenticated vehicles' behavior. We have tested BGLS with 100-500 number of nodes. In the future, it can be tested with different numbers of vehicles, for example, from 10 to 10,000. For our future work, more appropriate and accurate authentication schemes, and more experiments would be executed to check the effectiveness of the scheme.

References

[1] Haydari, A., & Yilmaz, Y. (2020). Deep reinforcement learning for intelligent transportation systems: A survey. IEEE Transactions on Intelligent Transportation Systems.

[2] Aldegheishem, A., Yasmeen, H., Maryam, H., Shah, M. A., Mehmood, A., Alrajeh, N., Song, H. (2018). Smart road traffic accidents reduction strategy based on intelligent transportation systems (tars). Sensors, 18(7), 1983.

[3] Sheikh, M. S., Liang, J. (2019). A comprehensive survey on VANET security services in traffic management system. Wireless Communications and Mobile Computing, 2019.

[4] Baras, S., Saeed, I., Tabaza, H. A., Elhadef, M. (2017). VANETs-based intelligent transportation systems: An overview. Advances in Computer Science and Ubiquitous Computing, 265-273.

[5] Jie Cui et al. "An Efficient Message-Authentication Scheme Based on Edge Computing for Vehicular Ad Hoc Networks". In: IEEE Transactions on Intelligent Transportation Systems 20.5 (2019), pp. 1621–1632. issn: 15249050. doi: 10.1109/TITS.2018.2827460.

[6] Jian Kang et al. "Highly efficient randomized authentication in VANETs". In: Pervasive and Mobile Computing 44 (2018), pp. 31–44. issn: 15741192. doi: 10.1016/j.pmcj.2018.01.004.

[7] Kumar, S., Singh, V. (2021, March). A Review of Digital signature and hash function based approach for secure routing in VANET. In 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS) (pp. 1301-1305). IEEE.

[8] Funderburg, L. E., Ren, H., Lee, I. Y. (2021). Pairing-Free Signatures With Insider-Attack Resistance for Vehicular Ad-Hoc Networks(VANETs). IEEE Access, 9, 159587-159597.

[9] Jiao Liu et al. "Bua: A blockchain-based unlinkable authentication in vanets". In: ICC 2020-2020 IEEE International Conference on Communications (ICC). IEEE. 2020, pp. 1–6.

[10] Anamika Chauhan et al. "Blockchain and scalability". In: 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C). IEEE. 2018, pp. 122–128.

[11] Qiheng Zhou et al. "Solutions to scalability of blockchain: A survey". In: IEEE Access 8 (2020), pp. 16440–16455.

[12] https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries

[13] Lacharité, M. S. (2018). Security of BLS and BGLS signatures in a multi-user setting. Cryptography and Communications, 10(1), 41-58.

[14] Han, Y., Song, W., Zhou, Z., Wang, H., Yuan, B. (2021). eCLAS: An Efficient Pairing- Free Certificateless Aggregate Signature for Secure VANET Communication. IEEE Sys- tems Journal.

[15] Manivannan, D., Moni, S. S., Zeadally, S. (2020). Secure authentication and privacy- preserving techniques in Vehicular Ad-hoc NETworks (VANETs). Vehicular Communica- tions, 25, 100247.

[16] Feng, X., Shi, Q., Xie, Q., Liu, L. (2021). An Efficient Privacy-preserving Authentication Model based on blockchain for VANETs. Journal of Systems Architecture, 117, 102158.

[17] Bouakkaz, S., Semchedine, F. (2020). A certificateless ring signature scheme with batch verification for applications in VANET. Journal of Information Security and Applications, 55, 102669.

[18] Shrestha, R., Bajracharya, R., Shrestha, A. P., Nam, S. Y. (2020). A new type of blockchain for secure message exchange in VANET. Digital communications and net- works, 6(2), 177-186.

[19] Khalid, A., Iftikhar, M. S., Almogren, A., Khalid, R., Afzal, M. K., Javaid, N. (2021). A blockchain-based incentive provisioning scheme for traffic event validation and information storage in VANETs. Information Processing Management, 58(2), 102464.

[20] Mundhe, P., Yadav, V. K., Singh, A., Verma, S., Venkatesan, S. (2020). Ring signature-based conditional privacy-preserving authentication in VANETs. Wireless Personal Communications, 114(1), 853-881.

[21] Tsafack, E. G., Mbiantcha, M., Ateufack, G., Djuichou Nguemnang, S. F., Nana Yousseu, W., Atsamo, A. D., ... & Ben Besong, E. (2021). Antihypernociceptive and Neuroprotective Effects of the Aqueous and Methanol Stem-Bark Extracts of Nauclea pobeguinii (Rubiaceae) on STZ-Induced Diabetic Neuropathic Pain. Evidence-Based Complementary and Alternative Medicine, 2021.

[22] Lu, R., Lin, X., Liang, X., & Shen, X. (2018). A dynamic privacy-preserving key management scheme for location-based services in VANETs. IEEE Transactions on Intelligent Transportation Systems, 13(1), 127-139.

[23] Chauhan, K. K., Kumar, S., & Kumar, S. (2017, November). The design of a secure key management system in vehicular ad hoc networks. In 2017 conference on information and communication technology (CICT) (pp. 1-6). IEEE.

[24] Islam, S. H., Obaidat, M. S., Vijayakumar, P., Abdulhay, E., Li, F., & Reddy, M. K. C. (2018). A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs. Future Generation Computer Systems, 84, 216-227.

[25] Cui, J., Tao, X., Zhang, J., Xu, Y., & Zhong, H. (2018). HCPA-GKA: A hash function-based conditional privacy-preserving authentication and group-key agreement scheme for VANETs. Vehicular communications, 14, 15-25.

[26] Liu, L., Wang, Y., Zhang, J., & Yang, Q. (2019). A secure and efficient group key agreement scheme for VANET. Sensors, 19(3), 482.

[27] Paliwal, S., & Chandrakar, A. (2019). A conditional privacy preserving authentication and multi party group key establishment scheme for real-time application in VANETs. Cryptology ePrint Archive.

[28] Mansour, A., Malik, K. M., Alkaff, A., & Kanaan, H. (2020). ALMS: Asymmetric lightweight centralized group key management protocol for VANETs. IEEE Transactions on Intelligent Transportation Systems, 22(3), 1663-1678.

[29] He, D., Zeadally, S., Xu, B., & Huang, X. (2020). An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Transactions on Information Forensics and Security, 10(12), 2681-2691.

[30] Zhang, J., Zhong, H., Cui, J., Tian, M., Xu, Y., & Liu, L. (2020). Edge computing-based privacy-preserving authentication framework and protocol for 5G-enabled vehicular networks. IEEE Transactions on Vehicular Technology, 69(7), 7940-7954.

[31] Zhang, J., Cui, J., Zhong, H., Chen, Z., & Liu, L. (2019). PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks. IEEE Transactions on Dependable and Secure Computing, 18(2), 722-735.

[32] Kenney, J. B. (2017). Dedicated short-range communications (DSRC) standards in the United States. Proceedings of the IEEE, 99(7), 1162-1182.

[33] Cai, Y., Zhang, H., & Fang, Y. (2020). A conditional privacy protection scheme based on ring signcryption for vehicular ad hoc networks. IEEE Internet of Things Journal, 8(1), 647-656.

[34] Zhou, L., Su, C., & Yeh, K. H. (2019). A lightweight cryptographic protocol with certificateless signature for the Internet of Things. ACM Transactions on Embedded Computing Systems (TECS), 18(3), 1-10.

[35] Karati, A., Islam, S. H., & Biswas, G. P. (2018). A pairing-free and provably secure certificateless signature scheme. Information Sciences, 450, 378-391.

[36] Zhong, H., Han, S., Cui, J., Zhang, J., & Xu, Y. (2019). Privacy-preserving authentication scheme with full aggregation in VANET. Information Sciences, 476, 211-221.

[37] Yang, X., Chen, C., Ma, T., Li, Y., & Wang, C. (2018, October). An improved certificateless aggregate signature scheme for vehicular ad-hoc networks. In 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC) (pp. 2334-2338). IEEE.

[38] Yang, X., Chen, C., Ma, T., Li, Y., & Wang, C. (2018, October). An improved certificateless aggregate signature scheme for vehicular ad-hoc networks. In 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC) (pp. 2334-2338). IEEE.

[39] Cui, J., Zhang, J., Zhong, H., Shi, R., & Xu, Y. (2018). An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks. Information Sciences, 451, 1-15.

[40] J. Cui, W. Xu, Y. Han, J. Zhang, H. Zhong, Secure mutual authentication with privacy preservation in vehicular ad hoc networks, Veh. Commun. 21 (2020) 100200.

[41] Y. Zhang, L. Zhang, D. Ni, K.-K.R. Choo, B. Kang, Secure, robust and flexible cooperative downloading scheme for highway VANETs, IEEE Access 9 (2021) 5199–5211.

[42] Saxena, A. S., Bera, D., Goyal, V. (2019). Modeling location obfuscation for continuous query. Journal of information security and applications, 44, 130- 143.

[43] Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T., Shadbolt, N. (2018, May). Third party tracking in the mobile ecosystem. In Proceedings of the 10th ACM Conference on Web Science (pp. 23-31).

[44] Sheikh, M. S., & Liang, J. (2019). A comprehensive survey on VANET security services in traffic management system. Wireless Communications and Mobile Computing, 2019.

[45] Baras, S., Saeed, I., Tabaza, H. A., & Elhadef, M. (2017). VANETs-based intelligent transportation systems: An overview. Advances in Computer Science and Ubiquitous Computing, 265-273.

[46] Hussain, R., Kim, D., Son, J., Lee, J., Kerrache, C. A., Benslimane, A., & Oh, H. (2018). Secure and privacy-aware incentives-based witness service in social internet of vehicles clouds. IEEE Internet of Things Journal, 5(4), 2441-2448.

[47] Cui, J., Zhang, J., Zhong, H., Shi, R., Xu, Y. (2018). An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks. Information Sciences, 451, 1-15.

[48] Sheikh, M. S., Liang, J., & Wang, W. (2019). A survey of security services, attacks, and applications for vehicular ad hoc networks (vanets). Sensors, 19(16), 3589.

[49] Parkinson, S., Ward, P., Wilson, K., & Miller, J. (2017). Cyber threats facing autonomous and connected vehicles: Future challenges. IEEE transactions on intelligent transportation systems, 18(11), 2898-2915.

[50] Mejri, M. N., Ben-Othman, J., & Hamdi, M. (2018). Survey on VANET security challenges and possible cryptographic solutions. Vehicular Communications, 1(2), 53-66.

[51] Funderburg, L. E., & Lee, I. Y. (2021). Efficient short group signatures for conditional privacy in vehicular ad hoc networks via ID caching and timed revocation. IEEE Access, 9, 118065-118076.

[52] Douriez, M., Doraiswamy, H., Freire, J., & Silva, C. T. (2017, October). Anonymizing nyc taxi data: Does it matter? In 2017 IEEE international conference on data science and advanced analytics (DSAA) (pp. 140-148). IEEE.

[53] Funderburg, L. E., Ren, H., & Lee, I. Y. (2021). Pairing-Free Signatures with Insider-Attack Resistance for Vehicular Ad-Hoc Networks (VANETs). IEEE Access, 9, 159587-159597.

[54] Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated learning: Challenges, methods, and future directions. IEEE Signal Processing Magazine, 37(3), 50-60.