Proof of Pseudonym: Blockchain Based Privacy Preserving Protocol for Intelligent Transport System

S. JOHAR1, N. AHMAD2, A. DURRANI1 and G. ALI1
1Department of Computer Science, University of Peshawar (e-mail: sumaira.johar@uop.edu.pk; amad.durrani@uop.edu.pk; gauharstd@uop.edu.pk)
2College of Computer and Information Sciences, Prince Sultan University, Kingdom of Saudi Arabia. (email: nahmed@psu.edu.sa)
Corresponding author: S.Johar (e-mail: sumaira.johar@uop.edu.pk).

ABSTRACT Intelligent Transportation Systems is the future for safe and secure transportation. Vehicles in the ITS share basic safety information which can prompt the disclosure of the real identity of the vehicles. Thus, adversaries can misuse these safety messages. Pseudonyms are alias granted to vehicles by trusted authorities to conceal their original identities. To avoid linkability, various pseudonym generation and distribution protocols have been proposed. Such protocols pose overheads in the system as they are performed by Central Authorities. Therefore, re-utilizing the existing pseudonyms through shuffling is the most optimal mechanism for ITS. The Blockchain is a digital ledger and tamper-resistant record of transactions. It eliminates the need of central authority as well as provides anonymity of transactions resulting in more secure and privacy protected solution. To handle distribution optimization issue in the pseudonym shuffling process without a central authority, the blockchain is used with its distributed consensus. The shuffling results are logged in blocks as transactions. Pseudonym shuffle randomness is achieved via blockchain and it provides robustness in the structure. When one system fails, the rest would continue to work. The method also provide fully traceable record in case of certification revocation. The existing blockchain-based pseudonym shuffling mechanism uses traditional consensus algorithms to support the cryptography operation. This leads to overhead in terms of execution time and memory usage. This research proposes Proof of Pseudonym consensus protocol for the shuffling scheme to improve the efficiency of consensus as compared to Proof of Work, Proof of Kernel Work and, Proof of Elapsed Time in terms of time and memory. The execution time of Proof of Pseudonym is shorter than other algorithms. The security and privacy analysis revealed that our scheme achieves identity privacy, unlinkability, and non-repudiation properties. Threat analysis evaluates the proposed protocol in terms of both internal and external attacks.

INDEX TERMS Blockchain, Proof of Work, Proof of Kernel Work, Proof of Elapsed Time, Proof of Pseudonym.

I. INTRODUCTION

Blockchain (BC) is implemented in a distributed manner with tamper-proof and tamper-resistant digital records. Usually, blockchain does not require any central authority i.e. banks, government or companies [1]. They enable users’ communities to record their transactions within the shared ledger. The blockchain does not allow a change in the record once it is published. It can be used to record not only monetary transactions, [2] but also everything of value like bank transactions and business transactions etc [3]. In a centralized system, one authority is responsible for making changes to the records. The block in a blockchain is published via mutual agreement of the participants by the process of consensus mechanism. It is a mechanism achieved by a particular algorithm where users agree on a single source of truth (transaction value or asset etc.) even if some of the nodes fail.

Following are the main features of Blockchain.

1) Decentralized Computation:
Blockchain comprises distributed ledgers maintained by peer-to-peer networks [4]. Blockchain removes the role of the central entity by using consensus protocol to authenticate transactions [5].

2) Distributed ledger of Transactions:
Transactions are stored in a common ledger [6], [7]. The ledger is copied and maintained on each peer of
the blockchain networks. By timely replication, these copies are synchronized [8].

3) Transparency: Blockchain stores every transaction in a block. It is also available to all peers for verification.

4) Fault-Tolerant Network: Blockchain transactions are processed parallel by all the mining nodes as of peer-to-peer network quality [9]. If some of the nodes are faulty blockchain will continue to work.

5) Security: After validation, each block is added to the chain. Every block contains a hash of the preceding block [10]. Blockchain does not allow deleting or updating of a block as it performs recalculation of all the previous blocks’ hash.

Traditional transport system faces several issues that include air pollution, traffic congestion, and high accident rates. Due to such problems, researchers came up with the idea of integrating virtual technology with the traditional structure of transportation, hence named it as Intelligent Transport System (ITS). ITS is an evolving technology that has several applications like traffic management and congestion control. For example, if an accident has occurred somewhere on a road, vehicles can alert each other to avoid traffic jams [11]. Privacy and security are the vital right of each resident and must be incorporated into every system. Privacy ensures that the real identity of an individual/vehicle/node is not observed while security assures confidentiality, authentication, availability, and integrity of the messages. Vehicles share basic safety information regarding location, speed, and other personal information amongst each other.

To achieve privacy, fake names called pseudonyms are used in ITS networks. Pseudonyms should also be changed frequently according to new principles. Attacks may endanger privacy and security in ITSs. Vehicle status information, for example, direction, speed, and velocity are broadcasted sporadically through Cooperative Awareness Messages (CAM) and are operated to improve traffic safety and productivity. An intruder can utilize altered data and may track locations of vehicles [12], and can access user private data [13]. Certificate Authority (CA) is responsible for issuing certificates to each vehicle participating in ITS, for communication. If there is an occurrence of malicious activity by a vehicle, its certificate is revoked by CA. Vehicles need to be authenticated before they take part in the network in ITS. Research has been conducted to protect user’s and node’s privacy over different techniques but they are either through central authorities or they create extra overhead on the network. Work has been done to eliminate the use of trusted third parties and at the same time protect the user’s privacy by using blockchain technology. However, it suffers delays and overhead [16]. The literature explains some methods of using blockchain for achieving ITS privacy but the consensus mechanisms they use are not efficient in terms of time and resources. In ITS one cannot afford delays as the processes going are almost in real-time. The purpose of this research is to develop a pseudonym-based shuffle mechanism through private and hybrid blockchain techniques. To evaluate various consensus algorithms designed for ITS pseudonym shuffling and to design a hybrid consensus algorithm i.e. Proof of Pseudonym to tackle the shuffling mechanism efficiently as well as to enhance the security of Road Side Unit (RSU) in terms of protecting users privacy and not make it a single point of failure. Consensus used in blockchain-based pseudonym shuffling is PoW which takes heavy computational power of the resources. Another consensus is suggested for pseudonym management over blockchain but they need to be tested and compared.

A. RESEARCH CONTRIBUTIONS

The main contributions of the paper are as follows.

- Introducing a novel pseudonym management scheme for ITS.
- Comparing and testing the algorithms/consensus mechanisms suggested by other research studies for the pseudonym management scheme over the blockchain such as PoW, PoKW, and PoET.
- The above algorithms are discussed, shown diagrammatically, formally, and implemented in node.js.
- A novel Proof of Pseudonym is suggested for real-time scenario particularly for the Pseudonym shuffle scheme, however, the said proof can be used in general for VANETs/ITS blockchain applications.
- The scheme for pseudonym shuffle is further secured by introducing blockchain over the RSU.
- The scheme is analyzed and mitigated for security threats.

The rest of the paper is divided as follows. Section II discusses the related work. In section III we discuss the consensus algorithms suggested for the ITS pseudonym shuffling mechanism. Section IV provides our proposed architecture design. In section V we provide the results of the three consensus algorithms. In section VI we discuss the security analysis. Section VII provides the conclusion and future directions.

II. BACKGROUND AND RELATED WORK

M. Raya et al. focused on the privacy protection of the vehicle/user that it is necessary as the malicious vehicle may take advantage of the genuine identity of the vehicle/user. Pseudonyms can be used to protect the vehicle from malicious attacks [14]. It is suggested by D. Forster et al. that pseudonyms should be changed on a regular basis to avoid trace-ability [15]. In ITS, identity and location privacy is both required in order to prevent wrong use by malevolent ITSs. Pseudonym centered techniques discussed in [16] by F. Schaub et al. use cryptography for user identity protection. These techniques, however, generate high communication and computation overhead. The work suggested by Wang et al. [17] builds a reputation service where deceivers who generate false messages are identified. There should be two servers, one for reputations and the other for pseudonyms.
The server checks and computes vehicles’ reputations. However, this causes it to suffer extra overhead and results in delays in communication. The idea of pseudonyms as primary and secondary is discussed by U. Rajput et al. [18]. L. Zhang et al. discussed the primary pseudonym as a single point of attack because it is provided by the Certificate Authority (CA). Similarly, secondary pseudonyms are used for V2X messages communication and generated through RSUs. RSUs, however, are prone to side-channel attacks as they are located in the open infrastructure [19].

H. Li et al. suggested the blockchain-based VANET resolves the problem of centralization and develops trust between entities in the existing VANET. However, the efficiency of the privacy protection mechanism is always an open issue in VANET [20]. An architecture proposed by M. Wagner et al. [21] is used for safeguarding VANETs without dependence on RSUs. However, the protocols presented have scalability issues as it uses Proof-of-Work (PoW) and it has computational overhead. Consensus algorithms like proof of work and proof of stake (PoS) are facing various issues.

For example, proof of work consumes too much energy and electricity while proof of stake deals with the phenomenon that the rich become richer as discussed by Z. Zheng et al. [22]. PoS protocols can experience from the nothing-at-stake problem, where validator nodes validate contradictory copies of the blockchain because there is insignificant expense to doing so, and a lesser chance of dropping out on rewards by validating a block on the wrong chain. If this continues, it can permit double-spending. The data privacy techniques suggested by T. Salman et al mostly depend on complex cryptographic algorithms; therefore, they are inefficient and hard to measure with large applications [23]. Research is being conducted to reduce the complexity and enhance the efficiency of these cryptographic techniques. The issues related to trust and privacy of VANETs are addressed by Z. Lu et al. [24]. Blockchain-based Anonymous Reputation System (BARS) is suggested for preventing the distribution of counterfeit messages from authentic vehicles by A. Lei et al. [25]. This system keeps the identity of the vehicle protected. Public key of the vehicle acts as a pseudonym to provide anonymous communication and to prevent linkability between a public key and real identity. An algorithm for reputation management is designed to avoid distribution of the forged messages while the vehicles get incentives to reveal the misbehavior of other vehicles.

In his research, Ao Lei [25] proposed a certificate revocation scheme for Vehicular Communication Systems (VCS) via blockchain which prevents insider attacks. This scheme reduces the overhead of broadcast messages and Certificate Revocation List (CRL) size. In this Blockchain structure, the PKI distributes the CRL and keeps track of the ownership of pseudonym sets in an efficient manner. Limitations of this research are: further investigation needs to be done for the efficient blockchain consensus algorithms and further evaluation of the privacy, security, and accountability. Privacy and authentication of users addressed by D. Zheng et al. [26] are two important VANET problems. It is important to avoid internal vehicles from spreading forged messages whereas at the same time preserving vehicles’ privacy against tracking attacks. Third important point is to remove dependency on third parties. BC for VANETs is introduced in cloud servers. No information linkable to real identity is included in the transactions. PKI as a central authority is prone to attacks. The system proposed by L. Benarous et al. is a scheme comprising of two Blockchains [27]. In a permissionless blockchain, certified pseudonyms are saved, and the revoked pseudonyms are spared in a public and permissioned blockchain. The first one is accessed by the RSUs with read rights and overseen by the enrolled vehicles. The second blockchain is supervised by the vehicles with read-only rights and the RSUs (having write access rights). RSU is responsible for managing pseudonyms over RSUs and vehicles computational and storage resources by using blockchain technology. The shortcoming of this paper is the complexity of implementation. The problem defined by K. Shi et al. [28] is that both the vehicles’ and users’ privacy can be disclosed, and communication routines of users are easily evaluated by adversaries. The shared multimedia data are more prone to be tampered with or altered. A blockchain-based privacy-preserving scheme is proposed for data sharing of multimedia in Vehicular Social networks. The use of cryptography measures is used to cover the real identity of RSUs and vehicles. Blockchain is also used to protect data from tampering and forging by malicious users and to safeguard consistent data sources. Users use pseudonym identities to communicate during multimedia data sharing. The experiments and security studies prove that the proposed scheme by K. Shi et al. achieves data integrity, verification, privacy protection, and efficiency. Shortcomings of this research are that the damage attackers can cause to the RSU should be paid more attention and work should be done for the security and performance of RSU. RSU can be curious to know the actual identity of the vehicle and to know the communication routines of the vehicles. Advanced privacy protection should be achieved i.e. location privacy. Pseudonym management is done by PKI which is a central authority and central system that is highly prone to attacks, has low scalability, and is highly unstable. Different locations require a different number of pseudonyms. Therefore, this becomes an issue of how to distribute the pseudonyms according to traffic. Pseudonym shuffle carried out by RSU is suggested but it creates a burden on RSU as RSU has less storage capacity in general. A consortium blockchain technology is deployed by J. Cui et al. [29] to achieve anonymous and traceable vehicle-to-vehicle (V2V) data sharing, to prevent second-hand sharing of data effectively. The combination of Blockchain and 5G
used to share data without relying on RSUs. The consensus protocol is based on a public blockchain network. There are two reasons for using blockchain technology in this context: scalability and immutability.

The working flow of Proof of Work (PoW) is the first consensus protocol used by a public blockchain network. All the nodes need to solve a cryptographic puzzle to validate transactions and add them to the blockchain. Therefore, consensus algorithms provide trust and reliability among unknown peers in a distributed environment. Consensus mechanism ensures that every new block added to the blockchain is the only truth which is agreed upon by all the blockchain nodes.

The blockchain consensus protocol comprises a number of specific aims that include coming to an agreement, cooperation, collaboration, mandatory participation of each node in the consensus process, and equal rights to every node. Hence, a consensus algorithm targets finding a common agreement that is a win for the whole network. The purpose of discussing the following consensus mechanisms is to compare and analyze with our own consensus Proof of Pseudonym.

A. PROOF OF WORK

Proof of work is the first consensus protocol used by a public blockchain. All the nodes need to solve a cryptographic puzzle by brute force. The node which wins the puzzle is rewarded and all the other nodes’ computations are wasted. The consensus is achieved as 51% of power [34]. PoW provides security to the network in terms of transactions but there are also some issues in PoW: It is a time-consuming protocol as it involves solving a puzzle. It takes heavy computation power of the resources. PoW is prone to 51% attack. In other words, if the eavesdropper takes over 51% of the network’s control then it can harm the network. Transaction confirmation can take up to 10 to 60 minutes, therefore the transactions are not instant as it takes time to mine the transactions and commit them to the blockchain. Hence, for real-time scenarios, it is not a suitable protocol. Figure 1 shows the basic working of PoW. The Proof of Work algorithm has no clear implementation details given in literature. Therefore based on theoretical details we implement proof of work 1. It was noticed that the algorithm was taking considerable time so changes are made to the algorithm so that it takes less time to solve a puzzle. This is the reason we give idea to researchers of both implementations. Algorithm 1 takes a whole string and we change the string manually to see how much time the whole string (puzzle) takes for guessing. Algorithm 2 takes a hash of data, timestamp, and nonce. We set a difficulty i.e. leading zeros over this hash and then we start the guessing and monitor the time it takes with different difficulty levels. We set the guessing characters for both the algorithms in order to provide the search set for the puzzle to find the string (puzzle) in the given set.

B. PROOF OF KERNEL WORK

Proof of Kernel Work (PoKW) is an energy consumption consensus that also leads to centralized mining by means of rewarding structures. Therefore, it appears desirable to preserve the benefits of PoW while also holding its energy consumption and justifying, if not excluding, centralized mining. The PoKW [35] eliminates some of the network nodes for the mining race and randomly chooses nodes (the
Algorithm 1 Proof_of_Work_1 Consensus

1: Inputs:
   a. P: It refers to the puzzle
   b. St: It refers to a puzzle string
   c. Length: It refer to the length of puzzle string
2: Begin Procedure
3: Step 1. St = n (No of Strings)
   P = 1 (Initialization)
4: Step 2. for (St = 1; St <= n; St ++)
5: if
   (P = St[i])
6: return (P)
7: else
8: return (St)
9: End Procedure
10: Output:
11: Return Puzzle Status

Algorithm 2 Proof_of_Work_2 Consensus

1: Inputs: h: Hash d: Difficulty n0: Nonce P: Puzzle
2: Output: Yes, No
3: Begin Procedure
4: Step 1:
5: P = h* d * n0 (difficulty level)
6: Character ch = ABC. . . . . . Zabc. . . .z0123. . .9#
7: Step 2.
8: for (St = 1; St <= n; St ++)
9: do
10: {
11: return (P)
12: }
13: while
14: {
15: St[i] = ch;
16: }
17: else
18: return (St)
19: End Procedure
20: Output:
21: Return Puzzle Status

C. PROOF OF ELAPSED TIME

In Proof of Elapsed Time (PoET), each node is allocated a randomized timer object from a trusted code. The node having the shortest timer when expires, node wakes up, propagates a signed certificate to show this node is the block leader [36]. The timer is given randomly so that the malicious user does not try to continuously obtain the shortest timer [37]. PoET is good in terms of winning block time duration but it has some disadvantages: It requires dedicated hardware having intel SGX. It also suffers Sybil attacks as an adversary gets a hold on the nodes with the help of forging multiple nodes’ identities. PoET is also prone to Denial of Service (DoS) attacks in which the adversary floods the network with requests. The working of PoET is given in Algorithm 3 followed by Figure 3 which we implemented in node.js and its running time complexity. In this algorithm, the client nodes generate random time ts without any threshold value and the node’s time is compared with each other. The node with the smallest time is the winner of the block.

IV. ARCHITECTURE DESIGN

The proposed architecture consists of the following core components i.e. RSU, PM, vehicles, PM cloud, BC.
Algorithm 3 Proof of Elapsed Time Consensus

1: Inputs:
   a. Nn: Total number of client nodes
   b. Nc: Client node (Available objects)
2: Begin Procedure
3: Step-1.
4: \( t = \text{time}\_\text{slot} \)
5: Step-2.
6: \( ts = \text{Computer node (smallest time)} \)
7: \( ts = 1 \) (initialized by 1)
8: Step-3.
9: \( \text{for } (ts <= Nn; ts++) \)
10: \( \text{if } (ts < t) \)
11: \( ts = \text{current time} \)
12: \( \text{else} \)
13: \( ts \neq \text{current time} \)
14: \( \text{continue} \)
15: \( \text{return } (ts) \)
16: End Procedure
17: Output: Return smallest_time of Nc

2) PM
Privacy Managers are devices introduced that come after PKI in the hierarchy. The purpose of Privacy Manager is to improve robustness in the system and act as a miner of the blockchain.

3) PM CLOUD
Cloud is used by PMs to manage blockchain among Privacy Managers.

4) BLOCKCHAIN (BC)
Blockchain in our scheme is used to record the pseudonym shuffling results in the form of transactions. The transactions contain the timestamp and the key pairs of the sender and receiver PMs along with the data encrypted with the receiver public key and signed by the sender/source private key.

5) VEHICLES
Vehicles are the main component of the ITS environment where the privacy of the vehicle or its owner is important.

A. FORMAL MODELING OF PROPOSED ARCHITECTURE
We formally model the proposed architecture and its vital components as follows.

1) Notations
The notations used in the proposed work are described in Table 1.

| Notation | Description |
|----------|-------------|
| \( v_i \) | \( i \)th vehicle in the ITS environment. |
| \( rsu_j \) | \( j \)th RSU. |
| \( cert_i \) | \( i \)th certificate of the vehicles. |
| \( PID_i \) | \( i \)th Pseudonym. |
| \( pk_i \) | Public Key. |
| \( sk_i \) | Secret Key. |
| \( V_n \) | All the Vehicles of the Network. |
| \( RSU_i \) | \( i \)th RSU. |

B. DEFINITIONS

1) Vehicle
\( V \supseteq \cup_{i=0}^{\infty} v_i, V \) is a superset of all the vehicles in the ITS environment.

2) RSU
\( RSU \supseteq \cup_{j=0}^{\infty} rsu_j, RSU \) is a superset of all the Road side units in the ITS environment.

3) Certificate Set
\( CERT \supseteq \cup_{i=0}^{\infty} cert_i, CERT \) is a superset of all the certificate. Certificate \( cert_i \) is the \( i \)th certificate.

FIGURE 3: Proof of Elapsed Time

1) RSU
Road Side Units are fixed infrastructure places geographically in an ITS network that communicate with vehicles and other RSUs. In our scheme, RSUs will distribute the pseudonyms according to the distributed algorithm and are placed third in the hierarchy.
4) Certificate to Vehicle Assignment
\[ C_{AV} \supseteq \cup_{i=0}^{\infty} j=0 \ P_{PKI} \xrightarrow{\text{cert}_j} v_i, \]
\[ C_{AV} \text{ contains all the assignment of certificates } \text{cert}_j \text{ to vehicles } v_i. \]

5) Pseudonymous IDs
\[ \mathcal{P}_{ID} \supseteq \cup_{i=0}^{\infty} j=0 \ P_{PID} \rightarrow v_i. \]
\[ \mathcal{P}_{ID} \text{ is super set of all the Pseudonymous IDs in a domain.} \]

6) PAV
\[ \mathcal{P}_{AV} \supseteq \cup_{i=0}^{\infty} j=0 \ P_{PKI} \rightarrow v_i. \]
\[ \mathcal{P}_{AV} \text{ contains all the assignment of Pseudonymous IDs } (P_{PID}) \text{ to vehicles } v_i. \]

7) PM
\[ \mathcal{P}_{PM} \supseteq \cup_{i=0}^{\infty} j=0 \ P_{RSU} \rightarrow v_i. \]
\[ \mathcal{P}_{PM} \text{ is a superset of all the Privacy Managers in the ITS environment.} \]

C. BLOCKCHAIN OVER PRIVACY MANAGER
This architecture reduces the cost of generating and pseudonym management for ITS. The architecture follows the traditional structure of VCS, where a central manager is Public Key Infrastructure (PKI) or a Certificate Authority (CA) is designed to maintain pseudonyms certificate centrally. PKI is at the top of the hierarchy. Privacy Managers (PMs) introduced comes after PKI to improve robustness in the system and act as miners of the blockchain. PM cloud is used to manage blockchain among Privacy Managers. Road Side Units (RSUs) will distribute the pseudonyms according to the distributed algorithm and they are placed third in the hierarchy as discussed in [38]. PKI is accessed only twice in the system. First, it provides the initial permanent identities and certificates to vehicles, and the second time it is accessed in case of malicious activity for certificate revocation [39]. The RSUs and PMs have devices that can communicate wirelessly over the wireless medium, using VCS communication standards (C-ITS [39] or DSRC [40]). RSUs act more as a communication bridge between vehicles (users) and service providers. Furthermore, vehicles are equipped with an On-Board Unit (OBU) which are computerized devices for the purpose of provisioning VCS standards. A PKI comprises of Certificate Authority (CA) and other third-party services. PKI is responsible for all the cryptographic credentials for pseudonyms such as pseudonym certificates, key pairs, and anonymous identities. PM manages certain areas under its security domain. PMs are supposed to support the PKI to manage the security domains and their cryptographic material that are placed beneath the PKI layer. This scheme proposes to install PMs geographically sparse. There is continuous communication between vehicles V2V and vehicles to infrastructure V2I. The infrastructure is RSU which collects safety-related messages from vehicles at regular intervals. The safety message contains the current status of the vehicle which includes the position, orientation, speed, and direction along with pseudonyms and time stamps. Vehicles contain a set of pseudonyms to utilize during diverse time durations in VANETs. Pseudonyms need to be used for a short time period and shift to new one often in lieu of achieving privacy. The vehicles do not exchange pseudonyms with each other but they get their updated sets from the sets given to them by RSUs.

The significance of the proposed work is providing an optimal solution for pseudonym management via an efficient consensus mechanism for pseudonym shuffling. External attackers and curious RSUs cannot take an advantage of data kept in BC as the transactions at RSU are anonymous. The scheme provides pseudonym shuffling at zones where there is maximum traffic. For example, traffic signal stops roundabouts and car parks, etc. This scheme aims to improve the unpredictability of pseudonym mixtures. It also reduces the cost and effort of constantly generating new pseudonym certificates as it reuses the pseudonyms after shuffling them. The social advantage in terms of expedient travel, users are recommended to take part in the blockchain platform to share and improve traffic and navigation information. Through blockchain, traffic routes can be optimized and speed can be controlled, hence, reducing pollution of urban traffic.

Algorithm 4 explains the updated step wise procedure as discussed by [31]. Nomenclatures and symbols used in algorithms are listed in Table 1.

- PKI will be used for the initial registration of vehicles i.e it generates and broadcasts the permanent id, pk, sk and cert to manufacturers via a secure channel.
- Manufacturer will give the above credentials to vehicles.
- PKI then generates and broadcast pseudonyms, certificates, pk, and sk to PMs encrypted with the public key of PM and signature encrypted with the secret key of the PKI.
- PMs and RSU will broadcast the Pseudonyms to RSU and vehicles respectively.
- Vehicles will use the Pseudonym sets and returns the used or unused pseudonyms to RSU after its expiration date.
- Privacy Managers (PMs) will collect used pseudonyms sets in form of packages from RSUs. Further PMs upload the pseudonym sets to PM cloud.
- PMs would shuffle them in the cloud and would take the shuffled sets back according to the traffic need reported by RSUs.
- Each PM would perform mining on the sets they have collected from the cloud. The mining process will be carried out according to the proposed consensus mechanism Proof of Pseudonym.
- The winner PM’s sets of pseudonyms will be published into the block of blockchain and RSUs will then assign them to vehicles after it takes the sets from the PMs. The proposed architecture for pseudonym shuffling mechanism is depicted in Figure 4.

D. BLOCKCHAIN OVER ROAD SIDE UNIT
Each Privacy Manager (PM) manages a number of RSUs under its coverage area. RSU has a risk of a single point of
PM manage the blockchain locally among each other. The working flow is as follows:

1. **Initial Registration:**
   
   $pid_i, cert_i, pk_i, sk_i$

2. **Pseudonym Allotment:**
   
   $PID$ broadcast $pid_i$ to $RSU_i$

3. **Pseudonym Management:**
   
   $RSU_i$ broadcast $pid_i$ to $V_n$.

4. **Pseudonym Shuffling**
   
   $\{pid_i, cert_i, pk_i\}_{skpk(M), signature_{skp(k_I), toPM}}$

5. **PKI broadcast**

$\{pid_i, cert_i, pk_i\}_{skpk(M), signature_{skp(k_I), toPM}}$

6. **PKI broadcast**

$\{pid_i, cert_i, pk_i\}_{skpk(M), signature_{skp(k_I), toPM}}$

Failure as a number of vehicles are managed by the RSU, RSUs are vulnerable to insider and outsider attacks therefore there is a need to secure the data on RSU. RSU can be protected from attacks and from a single point of failure if decentralized; hence, we introduce the blockchain over RSUs. However, one may think of the overhead created by maintaining multiple blockchains since the environment is in real-time and vehicles need quick responses. The issue comes with using slow consensus methods. The efficient consensus mechanism that we designed i.e. Proof of Pseudonym resolves the issue by generating the winner of the blocks faster as compared to other well-known methods. RSUs under each PM manage the blockchain locally among each other. The working flow is as follows:

- In our scheme, we assume the RSUs contains three sorts of data: The vehicles status information of its coverage area, the shuffled sets that it gets from the PMs to further distribute among vehicles, and the used pseudonyms given by vehicles.
- To disseminate the announcement that RSUs received the shuffled pseudonym sets and to protect the sets against attacks, the information is protected in the blockchain.
- Each RSU participates in a consensus to reach an agreement. Since Proof of Pseudonym gives fast results, the blockchain is maintained efficiently.
- Similarly, when the RSU collects the used pseudonyms from the vehicles, it identifies them as a separate transaction in blockchain to inform other RSU about the sets being used.
- The used pseudonyms are collected along with vehicles’ status information and recorded as transactions with their credentials.
- RSUs runs the mining process again to publish a block in a blockchain to keep the record of used pseudonyms. Hence, forming a Blockchain of Blockchains. This is advantageous in a way that attackers cannot try to reuse the used pseudonyms sets of the vehicles. Algorithm 5 discusses the pseudonym distribution by RSU while maintaining the blockchain.
- The pseudonyms in the sets are tracked by the blockchain and any vehicle using the same used sets is identified and reported to PM which further proceeds to inform CA to revoke its certificate. Similarly, the blockchain keeps used pseudonym sets as transactions. As the data in blockchain are kept immutable, anonymous, encrypted, and transparent, the attackers cannot take advantage of data in BC at RSU. The proposed

**Algorithm 4** Pseudonym Shuffling

1. **Initialization:**

   $ pid_i, cert_i, pk_i, sk_i$

2. **Step 1:** PKI generate constant

3. **Step 2:** PKI send

   $ pid_i, cert_i, pk_i, sk_i$

   through secured channel to Manufacturer.

4. **Step 3:** Manufacturer issue

   $ pid_i, cert_i, pk_i, sk_i \leftarrow V_n$

5. **Step 4:** PKI generate pseudonym ids with cryptographic credentials

   $ pid_i, cert_i, pk_i, sk_i$

6. **PKI broadcast**

   $ \{ pid_i, cert_i, pk_i \}_{skpk(M), signature_{skp(k_I), toPM}}$

7. **Pseudonym Allotment:**

   $ PID$ broadcast $ pid_i$ to $ RSU_i$

8. **RSU** broadcast $ pid_i$ to $ V_n$

9. **Pseudonym Management:**

   **for** {$ y = 1 \; y \leq i \; y++$} **do**

10. $ PM_i$ counts the number of used (expired) pseudonyms i.e., $ PID \in \bigcup_{y=0}^{\infty} PID_i$ from $ RSU_i$.

11. **CPU** picks $ PID$ sets in $ PM$ cloud.

12. $ PM_i$ picks $ PID$ sets in $ PM$ cloud and relocate them to destination $ PM_i$.

13. **end for**

14. $ PM_i$ starts mining on the selected $ PID$ sets.

15. The block is broadcasted into the network by winner miner.

16. **for** {$ y = 1 \; y \leq i \; y++$} **do**

17. $ PM_i$ retrieves new pseudonyms

18. Repeat step 2 and 3

19. **end for**

20. Exit
scheme already maintains the blockchain as the main entity where the shuffling process takes place over the PMs in the cloud.

1) However, we keep the services of server optional in case of blockchain over RSU. There are two possibilities in this case. RSU can take the services from the cloud server for the Proof of Pseudonym i.e. percentage of nodes and nodes selection or,

2) RSU can eliminate the use of server but in that case, the code needs to be readjusted for randomization of the percentage for nodes selection. Figure 5 depicts blockchain over RSU.

![Blockchain over Road Side Unit](image)

**Algorithm 5** Pseudonym Distribution of RSUs via Blockchain

```plaintext
for \{y=1 \ y<=i; \ y++\} do
if \{RSU_i requests for new PID\} then
PM_i sends the PID to RSU_i.
end if
RSU_i records the PID as tx in BC and starts mining.
After the block is published RSU_i distributes the PID to V_n.
V_n returns PID to RSU_i after using.
RSU_i starts mining again for used PID_i
RSU_i sends the used PID_i to PM_i
end for
Exit
```

**E. PROOF OF PSEUDONYM**

Proof of Pseudonym working as client and cloud server is as follows.

1) The server detects as new nodes (clients) connect to the network. For example, N1, N2, N3,...Nn are the nodes connected to the server.

2) The Server randomly decides the percentage of miners among the participant nodes, not less than 50 percent. The percentage is set to 50 because the consensus agreement is more reliable if half or more of the network participates. The percentage is calculated by the following formula:

\[
\frac{(N1 + N2 + N3 + Nn)}{N_x*} = i\%\text{nodes}
\]

(Threshold value of percentage)

where Nx is the total number of nodes.

3) The server is also responsible for deciding which particular nodes among the percentage of nodes can proceed. For instance, we say the server chooses N2, N3, N5,...Ni, randomly predicts the nodes with their IP addresses. These nodes are informed about mining while other nodes are not informed about the elected miner nodes. Those will only receive a message that you are not selected for mining. This is to protect the miner nodes from any kind of vulnerability.

4) These miners will reach the consensus to publish a block of transactions into the blockchain. The time limit is also decided about the server for the nodes.

5) The nodes run the code for generating random short time.

6) The node with the shortest time is the winner of the race. Optionally, it can get incentives from the network. The proposed scheme runs over the PMs and RSUs so there is no need for incentive. However, the Proof of Pseudonym is not limited to pseudonym shuffling. This node’s block will be published into the blockchain network. In our scheme, the blockchain is maintained by PMs in the cloud. The server is also in the cloud for deciding the percentage of miners and nodes participating in the mining race as shown in Figure 6. We also describe the working of Proof of Pseudonym in Algorithm 6 where in step 1, the client C_{IP} wants to handshake with the server, Ser. If the handshake is established, then step 4 is performed, else step 5 is carried out where the server finishes the handshake with C_{IP}. In step 4, the server checks the number of nodes Nn and threshold percentage. If Nn is less than or equal to the threshold percentage, then it grants access according to a percentage threshold value set by the server randomly. If C_{IP} is granted access, the list is updated and step 2 is performed. In step 2, if the server grants access to C_{IP}, then step 3 is accomplished. However, if C_{IP} is selected for mining and time is generated for selected nodes, step 1 is performed otherwise step 4 is carried out. We also calculated the best, average, and worst time complexities of the three algorithms in Table 2.
V. RESULTS
The popular platform for blockchain development such as Hyperledger and Ethereum are not suitable for our proposed work due to their implementation of Proof of Stake (PoS) and Proof of Work (PoW) consensus algorithms. Moreover, their platform architecture does not support assumptions for developing customized consensus. The proposed architecture is implemented by developing a private blockchain in node.js and python platforms due to their rich support of libraries for the blockchain. To validate the algorithm emulation is performed by using mining rigs/GPU nodes. GPU RAM is 16 GB, processor: intel (R) Core (TM) i7- 9700K CPU 3.60 GHz 64 bit Operating System. We assume the constant specifications of the systems, as the proofs are meant to run on PMs and not vehicles with variable specifications.

The algorithms are analyzed according to their working. The PoW 1 solves a puzzle where the difficulty is chosen by the leading zeros. A higher number of leading zeros results in an increased difficulty level. The Figure 7 shows puzzle difficulty level on the x-axis and CPU time on the y-axis. The graph shows a clear rise in CPU time as the difficulty increases. The algorithm is executed 50 times for 10 different puzzles system. We encountered a long delay for the difficulty level with three leading zeros. The algorithm guesses the entire puzzle and the time taken by PoW 1 shows that a simple CPU is not suitable for solving a difficult puzzle. We also constructed a PoW 2 with difficulty (leading zeros) and a hash consisting of data, timestamp, and nonce where the guessing is based on the hash. We also show in Figure 8 the average pageable memory taken by the puzzles (nonces) in kilobytes in CPU. The graph shows that as the puzzle difficulty level increases, the memory is more occupied. Utilizing GPU can result in better time as compared to CPU. However, GPUs are expensive as compared to CPUs, hence, the resources used for PoW are expensive. Figure 9 and Figure 10 show the results of our second implementation of PoW which is improved as compared to the one implemented earlier. However, it still suffers delays.

Algorithm 6 Proof of Pseudonym Consensus

1: Inputs:
   a. $C_{IP}$: A client node that connects to server using its IP address.
   b. Ser: server node
   c. Port: Port number for connection
   d. Nt: Node threshold value used by server
   e. Nn: Number of Nodes
2: Begin Procedure
3: Step-1. if $C_{IP}$ requests Ser (handshaking)
4: goto Step-4
5: else
6: goto step-5
7: Step-2. if $C_{IP}$ request granted Ser
8: goto step 3
9: else
10: goto step 4
11: Step-3.
   a. $C_{IP}$ is selected for mining
   b. ts = $C_{IP}$ (Generate time for clients)
   c. Goto Step-1.
12: Step-4.
   a. Server checks the Nn and Nt values
   b. if Nn <= Nt
   c. Nn = Access granted and list updated
13: Step-5. $C_{IP}$ Ser (Finish handshaking)
14: End Procedure
15: Output: Either $C_{IP}$ is selected for mining or not.

PoKW is the delegated version of PoW which is why displaying its graph is not mandatory. We assume the time taken by the puzzle in the network is not suitable for ITS applications as the vehicles need fast responses especially when it comes to privacy achievement. The removal of or minimizing the number of leading zeros makes the puzzle easy to guess, hence more prone to a 51% attack.
Figure 11 shows the results of PoET with 10 nodes and their randomly generated times. The said proof is tested for 100 and 200 nodes but the graph can be shown clearly for not more than 10 nodes. The graph shows that nodes produce time randomly with each node receiving the chance of generating the shortest time, hence winning the race block publishing into the blockchain. Hence we conclude that this algorithm is efficient as compared to PoW and PoKW in terms of transaction winning time. The CPU time in PoET is directly proportional to the number of nodes. This means that the overall time of winning the block is proportional to the number of nodes. For example if five nodes takes two seconds in deciding that node 2 has the shortest time and is the winner, twenty nodes will take more time to decide the winner node.

The time taken by Proof of Pseudonym is calculated and then we compare PoW and Proof of Pseudonym according to the formula:
\[ tB = nT \cdot tV + 2 \cdot tP + t_{\text{prep}} + t_{\text{MN}}. \]

\( tB \) is the total time of the block, \( nT \) denotes the number of transactions, \( tV \) is the total time of transaction verification where \( tV \) depends on \( nT \), \( tP \) is the network cable propagation time, \( t_{\text{prep}} \) is the block preparation time, and \( tM \) is the mining average time where mining time \( tM \) is changed with the average time taken by PoW 2 and Proof of Pseudonym. We assume PoW 2 as the time for the winning node which is less than PoW 1. Therefore we compare our Proof of Pseudonym with the minimum average time taken by PoW 2. We take constant time for \( tV \), \( tP \), and \( t_{\text{prep}} \) with as negligible values as possible while we change \( nT \) for 100 to 1000 as the transactions generated in off hours are 100 while in peak hours may exceed 1000 as discussed in previous works. The negligible constant times taken in the given formula are not realistic as transaction preparation and block preparation take
according to formula 2 in Figure 12. We elect 20 nodes for each shuffle consensus and we can analyze that all the nodes get a chance for generating the shortest random time and winning the race. We can see and compare the results of Proof of Pseudonym with both the implementations of PoW and PoET. Random selection is better at minimizing the consensus time. The comparison of Proof of Pseudonym with PoW1 and PoW2 can be seen in Figure 13. In Figure 14 Proof of Pseudonym is compared with time cost of transactions calculated using PoW by [31]. We can see in Figure 14 that [31] has shown a graph where using PoW the time cost increases with number of transactions while Proof of Pseudonym is not relying on number of transactions rather random time is generated by elected nodes.

VI. SECURITY ANALYSIS

We identify pertinent attack vectors for blockchain-based pseudonym management systems in vehicular Adhoc networks and mitigation measures for such attacks. We divide this section according to the privacy and security threats to pseudonym management schemes, the internal and external attacks on RSUs, how they are prevented in the proposed scheme, and last but not least we discuss the threats to consensus protocols. We discussed i.e. PoW, PoET, PoKW, and how we overcome them in Proof of Pseudonym.

1) NO SINGLE POINT OF FAILURE:
The blockchain is distributed and the PMs and RSUs are all participating in the formation, maintenance, and updating of the blockchain of blockchains framework. Hence, no certifying authority is required and the single point of failure problem is removed. Additionally, the contributing nodes serve as multiple restoration and backup points.

2) THE IDENTITY PRIVACY:
Unlike the traditional PKI, in which each certificate is linked with the name of the public key holder. Our proposed framework does not save the identity of the owner in the blockchain. The generated pseudonyms are attached to the owner’s account initially and later they are reused by other vehicles, the system can decide when to change and allot new pseudonyms.

3) THE UNLINKABILITY: Unlinkability is the property that two messages sent by the same vehicle cannot be linked for long durations. In this proposed scheme, the pseudonyms given to the vehicles are not static. They keep changing when the system triggers. Hence, the messages sent by the same vehicle are unlinkable. The use of blockchain makes the transactions anonymous, hence unlinkability is achieved.

4) NON REPUDIATION:
The framework is aimed to preserve the privacy of vehicles, especially that the blockchain is fully distributed, non-repudiation is also another essential property for assurance. Therefore, we have guaranteed that the mischievous nodes are responsible and that they cannot deny their committed activities.
A. THREAT MODEL

The safety messages are broadcasted in the network and an adversary can track the location of vehicles via analyzing these safety messages. We focus on external and internal attacks. External attacks are further divided into Global Passive Adversary (GPA) and Local Passive Adversary (LPA). A Global Passive Adversary has inclusive access to a network of connected vehicles. An eavesdropper can leverage the broadcasted beacons messages and track a vehicle in a region where the eavesdropper is interested.

The Local Passive Adversary (LPA) is interested only in its transmission range region. It can also eavesdrop on the broadcasted beacons messages. Internal attacks have further two types: Internal Betrayal Adversary and Internal Tricking Adversary.

Internal Betrayal Adversary (IBA) is a compromised node that can give information about vehicles by spoofing safety messages to a local or global passive adversary. The attacker can then find out the real identity and location of the target vehicle.

Internal Tricking Adversary (ITA) uses pseudonyms of other vehicles to confuse the network and attack a node.

B. COUNTER MEASURES

We show how this study overcomes the attacks discussed above.

1) GLOBAL AND LOCAL PASSIVE ADVERSARY:

The most common type of attacks is Global Passive Adversary (GPA) and Local Passive Adversary (LPA) privacy attacks where the vehicle's beacon messages are passively snooped. The GPA and LPA might gain the location and timestamps of the leaving and joining of vehicles to map them. Works in [41], [42] state that they can predict the vehicles location-based data by brute-forcing beacon messages even if the vehicles change their pseudonyms often. Instead, this system allows vehicles to change the pseudonyms where there is maximum traffic in that zone. The GPA and LPA, hence cannot map the timestamps and locations of the vehicles as there is no entering or exiting of vehicles at mixed zones.

2) INTERNAL BETRAYAL ADVERSARY AND INTERNAL TRICKING ADVERSARY:

Internal betrayal adversary can obtain a vehicle's pseudonym to map it with the vehicle's real identity or it can pass it to the global adversary for manipulation. This attack is avoided in this scheme because the vehicles are not supposed to exchange pseudonyms among themselves, instead, they modify their sets with their own sets given by the RSU of their coverage area. Vehicles cannot evaluate the original source of the pseudonyms once it gets updated sets from the RSUs. The IBA cannot get any useful information from its vehicles or even if it tries to obtain the pseudonym sets. RSUs will identify the malicious activity as it records the transaction over a blockchain.

However, the ITA will try to use the pseudonyms already given to the vehicles in order to confuse the network. This study proposed a solution for this problem where this activity of using old pseudonyms is identified by the nearest RSU of the coverage area. The identified adversary is marked and other vehicles are informed about the attacker. In case the attacker leaves its RSU coverage area, the RSU of the new coverage area can figure it out as the blockchain is maintained among various RSUs under each PM.

3) SPOOFING ATTACK: The PMs can be spoofed for an attack where it can generate false blocks for pseudonym shuffles and can manipulate the permanent identity of the vehicles. The proof of pseudonym consensus requires that the nodes selected for mining are informed and other nodes are not informed. Therefore the possibility of an attack on a PM is very rare as the network has no knowledge about the PMs selected for mining. In case PM is compromised, the CA will discard it and the network will discard its pseudonyms.

C. ATTACKS ON RSU AND ITS COUNTER MEASURES

RSUs as a single point of authority for many vehicles suffer attacks. They can be compromised for mutual collaboration with an attacker or between each other. We discuss the possible attacks and their measures by our proposed system.

1) INTERNAL ATTACKS: RSU gives a set of pseudonyms to vehicles. It can allow an attacker to track the location of the vehicle via pseudonyms. There is also a possibility for an attacker to track vehicles between two RSUs in case both the RSUs are compromised. Curious or compromised RSU will try to analyze the communication habits between different real vehicles and the user’s real identity behind the vehicle to track the vehicle services. In our proposed system, the RSU contains pseudonym shuffled sets as well as the used pseudonym sets. First, the RSU contains pseudonyms that are shuffled. Therefore, curious RSU cannot take advantage even if it observes the communication habits and cannot reach to map the
original identity with the pseudonyms. Curious RSU cannot analyze the shuffled pseudonym sets as it is of no use. Secondly, the RSU contains used pseudonym sets, and blockchain transactions containing these used pseudonym sets are stored anonymously, hence this data is of no use to curious RSU as the transactions are unknown. The RSU has no prior knowledge about the pseudonyms coming from a particular vehicle.

2) EXTERNAL ATTACKS:
External attackers can attack RSU by stealing the data stored in RSU. An external attacker can have an access to shuffled sets and can manipulate it accordingly, may forge a large amount of communication data within RSU and may perform other illegal operations. Hence, RSUs are at risk. With blockchain over RSU the transactions and data are secured in a distributed ledger that is immutable. External attackers cannot have access to data, stored in RSU. However, if they by any means have access to RSU data it is of no use to them as the transactions are anonymous.

D. ATTACKS AND COUNTER MEASURES IN PROOF OF PSEUDONYM

Proof of Pseudonym prevents the possible attacks encountered in PoW, PoKW, and PoET. It prevents 51% attack as it does not involve computational resources. It is not hardware independent as we analyzed it on core i3 and core i7 systems. Proof of Pseudonym also prevents Sybil attacks as it chooses a certain number of nodes for consensus and not all. The selected nodes are not aware of each other about their selection for consensus, hence it prevents Sybil attack. As this algorithm does not involve solving a puzzle, an attacker cannot separately mine a private thread.

VII. CONCLUSION AND FUTURE DIRECTIONS

This paper proposes a scheme for pseudonym management in intelligent transport systems based on blockchain. The scheme suffers delays by using Proof of Work. Therefore, this paper proposes a novel consensus method Proof of Pseudonym which overcomes the delays suffered by Proof of Work and suggests two other methods that are Proof of Kernel Work and Proof of Elapsed Time. The results show that the proposed consensus achieves better results in terms of execution time, memory, and transaction processing time. The paper also suggests using blockchain on RSUs under each privacy manager, so as to protect RSUs from vulnerabilities. In the future, we plan to implement the blockchain over RSU and analyze the overhead as the mining process commences twice as per our assumption. Proof of Pseudonym over RSU blockchain needs to be updated for server services. It can be updated, so it chooses the percentage of nodes without relying on the server. The transactions of the block in RSU need further consideration. Additionally, the Proof of Pseudonym can be edited with the incentivization process if used in other scenarios of ITS.

ACKNOWLEDGMENT

The authors would like to acknowledge the support of Prince Sultan University for paying the Article Processing Charges (APC) of this publication. The author would like to thank Prince Sultan University for their support.

REFERENCES

[1] D. Yaga, P. Mell, N. Roby, and K. Scarfone, “Blockchain technology overview,” arXiv preprint arXiv: 1906.11078, 2019.
[2] A. Tapscott and D. Tapscott, “How blockchain is changing finance,” Harvard Business Review, vol. 1, no. 9, pp. 2-5, 2017.
[3] F. Rizal Batubara, J. Ubacht, and M. Janssen, “Unraveling transparency and accountability in blockchain,” Proceedings of the 20th Annual International Conference on Digital Government Research, pp. 204–213, 2019.
[4] M. Swan, “Blockchain thinking: The brain as a decentralized autonomous corporation [commentary],” IEEE Technology and Society Magazine, vol. 34, no. 4, pp. 41–52, 2015.
[5] A. Bahga and V. Madisetti, Blockchain applications: A hands-on approach. Artechouse Bahga and Vijay Madisetti, 2017.
[6] N. El Ioini and C. Pahl, “A review of distributed ledger technologies,” in OTM Confederated International Conferences “On the Move to Meaningful Internet Systems.” Springer, pp. 277–288, 2018.
[7] E. Anceaume, A. Gueliet, R. Ludinard, and B. Serricola, “Sycomore: a permissionless distributed ledger that self-adapts to transactions demand,” IEEE 17th International Symposium on Network Computing and Applications (NCA), pp. 1–8, 2018.
[8] A. Hughes, A. Park, J. Kietzmann, and C. Archer-Brown, “Beyond bitcoin: What blockchain and distributed ledger technologies mean for firms,” Business Horizons, vol. 62, no. 3, pp. 273–281, 2019.
[9] R. P. Wattenhofer, Distributed Ledger Technology: The Science of the Blockchain. Inverted Forest Publishing, 2017.
[10] G. Karame, “On the security and scalability of bitcoin’s blockchain,” Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, pp. 1861–1862, 2016.
[11] F. Sakiz and S. Sen, “A survey of attacks and detection mechanisms on intelligent transportation systems: Venets and iav,” Ad Hoc Networks, vol. 61, pp. 33–50, 2017.
[12] C. Ganan, J. L. Munoz, O. Esparza, J. Mata-D’az, and J. Alins, “Epa: An efficient and privacy-aware revocation mechanism for vehicular adhoc networks,” Pervasive and Mobile Computing, vol. 21, pp. 75–91, 2015.
[13] M. Gerlach and F. Guttler, “Privacy in venets using changing pseudonyms-ideal and real,” IEEE 65th Vehicular Technology Conference-VC2007-Spring, pp. 2521–2525, 2007.
[14] M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,” Journal of computer security, vol. 15, no. 1, pp. 39–68, 2007.
[15] D. Forster, F. Kargl, and H. L’ohr, “Puca: A pseudonym scheme with strong privacy guarantees for vehicular ad-hoc networks,” Ad Hoc Networks, vol. 37, pp. 122–132, 2016.
[16] F. Schaub, Z. Ma, and F. Kargl, “Privacy requirements in vehicular communication systems,” International Conference on Computational Science and Engineering, pp. 139–145, 2009.
[17] J. Wang, Y. Zhang, Y. Wang, and X. Gu, “RPRep: A robust and privacy-preserving reputation management scheme for pseudonym-enabled VANETS,” International Journal of Distributed Sensor Networks, vol. 12, no. 3, p. 6138251, 2016.
[18] U. Rajoput, F. Abbas, and H. Oh, “A hierarchical privacy preserving pseudonymous authentication protocol for VANET,” IEEE Access, vol. 4, no.5, pp. 7770-7784, 2016.
[19] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, “Distributed aggregate privacy-preserving authentication in VANETS,” IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 3, pp. 516-526, 2017.
[20] H. Li, L. Pei, D. Liao, G. Sun, and D. Xu, “Blockchain meets VANET: An architecture for identity and location privacy protection in VANET,” Peer-to-Peer Networking and Applications, vol. 12, no. 5, pp. 1178-1193, 2019.
[21] M. Wagner and B. McMillin, “Cyber-physical transactions: A method for securing VANETs with blockchains,” IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC), pp. 64-73, 2018.
[22] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An overview of blockchain technology: Architecture, consensus, and future trends,” IEEE international congress on big data (BigData congress), 2017, pp. 557-564.
A. Festag, “Cooperative intelligent transport systems standards in Europe,” IEEE Communications, vol. 7, no.3, pp. 117716-117726, 2019.

J. B. Kenney, “Dedicated short-range communications (dsrc) standards in VANETS,” ICT Express, vol. 4, no. 4, pp. 6252, 2021.

S. Bao, W. Hathal, H. Cruickshank, Z. Sun, P. Asuquo, H. Cruickshank, and et al., “A blockchain based certificate revocation scheme for vehicular communication systems,” Future Generation Computer Systems, vol. 110, no.9, pp. 892-903, 2020.

D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, “A traceable blockchain-based access authentication system with privacy preservation in VANETS,” IEEE Access, vol. 7, no.3, pp. 117716-117726, 2019.

L. Benarous, B. Kadri, and A. Bouridane, “Blockchain-Based Privacy-Aware Pseudonym Management Framework for Vehicular Networks,” Arabian Journal for Science and Engineering, no.2, pp. 1-17, 2020.

K. Shi, L. Zhu, C. Zhang, L. Xu, and F. Gao, “Blockchain-based multimedia sharing in vehicular social networks with privacy protection,” Multimedia Tools and Applications, no.1, pp. 1-21, 2020.

J. Cui, F. Ouyang, Z. Ying, L. Wei, and H. Zhong, “Secure and Efficient Data Sharing Among Vehicles Based on Consortium Blockchain,” IEEE Transactions on Intelligent Transportation Systems, no.2, 2021.

J. Ma, T. Li, J. Cui, Z. Ying, and J. Cheng, “Attribute-Based Secure Announcement Sharing among Vehicles Using Blockchain,” IEEE Internet of Things Journal, no., 2021.

S. Bao, Y. Cao, A. Lei, P. Asuquo, H. Cruickshank, Z. Sun, et al., “Pseudonym Management Through Blockchain: Cost-Efficient Privacy Preservation on Intelligent Transportation Systems,” IEEE Access, vol. 7, no.5, pp. 80390-80403, 2019.

N. Chaudhry and M. M. Yousaf, “Consensus algorithms in blockchain: comparative analysis, challenges and opportunities,” 12th International Conference on Open Source Systems and Technologies (ICOSST), IEEE, pp. 54–63, 2018.

Wahab and W. Mehmood, “Survey of consensus protocols,” arXiv preprint arXiv: 1810.03357, 2018.

F. Muratov, A. Lebedev, N. Iushkevich, B. Nasulina, and M. Takemiya, “Yac: Bft consensus algorithm for blockchain,” arXiv preprint arXiv: 1809.00554, 2018.

L.-N. Lundbaek, D. Janes Beutel, M. Huth, S. Jackson, L. Kirk, and R. Steiner, “Proof of kernel work: a democratic low-energy consensus for distributed access-control protocols”, Royal Society open science, vol. 5, no. 8, p. 180422, 2018.

S. Johar, N. Ahmad, W. Asher, H. Cruickshank, and A. Durrani, “Research and Applied Perspective to Blockchain Technology: A Comprehensive Survey,” Applied Sciences, vol. 11, no. 14, p. 6252, 2021.

M. Macdonald, L. Liu-Thorrold, and R. Julien, “The blockchain: a comparison of platforms and their uses beyond bitcoin”, Communications Magazine, no.1, pp. 858-880, 2018.

S. Bao, W. Hathal, H. Cruickshank, Z. Sun, P. Asuquo, and A. Lei, “A lightweight authentication and privacy-preserving scheme for vanets using tesla and bloom filters,” ICT Express, vol. 4, no. 4, pp. 221–227,2018.

J. B. Kenney, “Dedicated short-range communications (dsrc) standards in the united states,” Proceedings of the IEEE, vol. 99, no. 7, pp. 1162–1182, 2011.

A. Festag, “Cooperative intelligent transport systems standards in Europe,” IEEE Communications Magazine, vol. 52, no. 12, pp. 166–172, December 2014.

C.-Y. Chow and M. F. Mokbel, “Enabling private continuous queries for revealed user locations,” in International Symposium on Spatial and Temporal Databases, Springer, pp. 258–275, 2007.

X. Pan, J. Xu, and X. Meng, “Protecting location privacy against location-dependent attacks in mobile services,” IEEE Transactions on Knowledge and Data Engineering, vol. 24, no. 8, pp. 1506–1519, 2012.

S. Johar, N. Ahmad, W. Asher, H. Cruickshank, and A. Durrani, “Research and Applied Perspective to Blockchain Technology: A Comprehensive Survey,” Applied Sciences, vol. 11, no. 14, p. 6252, 2021.

M. Macdonald, L. Liu-Thorrold, and R. Julien, “The blockchain: a comparison of platforms and their uses beyond bitcoin”, Communications Magazine, no.1, pp. 858-880, 2018.

S. Bao, W. Hathal, H. Cruickshank, Z. Sun, P. Asuquo, and A. Lei, “A lightweight authentication and privacy-preserving scheme for vanets using tesla and bloom filters,” ICT Express, vol. 4, no. 4, pp. 221–227,2018.

J. B. Kenney, “Dedicated short-range communications (dsrc) standards in the united states,” Proceedings of the IEEE, vol. 99, no. 7, pp. 1162–1182, 2011.

A. Festag, “Cooperative intelligent transport systems standards in Europe,” IEEE Communications Magazine, vol. 52, no. 12, pp. 166–172, December 2014.

C.-Y. Chow and M. F. Mokbel, “Enabling private continuous queries for revealed user locations,” in International Symposium on Spatial and Temporal Databases, Springer, pp. 258–275, 2007.

X. Pan, J. Xu, and X. Meng, “Protecting location privacy against location-dependent attacks in mobile services,” IEEE Transactions on Knowledge and Data Engineering, vol. 24, no. 8, pp. 1506–1519, 2012.
G. ALI received his Ph.D. (Computer Science) degree from University of Peshawar, Pakistan in 2020. His research interests include Internet of Things, Access Control, Blockchain, Intelligent Transport System, Formal Verification, and Model Checking.