Computers, Materials & Continua
DOI: 10.32604/cmc.2022.031490
Article

Tech Science Press

Active Authentication Protocol for IoV Environment with Distributed Servers

Saravanan Manikandan[1], Mosiur Rahaman[1] and Yu-Lin Song[1,2,*]

[1]Department of Computer Science and Information Engineering, Asia University, Taichung, Taiwan
[2]Bioinformatics and Medical Engineering, Asia University, Taichung, Taiwan
*Corresponding Author: Yu-Lin Song. Email: d87222007@ntu.edu.tw

Received: 19 April 2022; Accepted: 12 June 2022

Abstract: The Internet of Vehicles (IoV) has evolved as an advancement over the conventional Vehicular Ad-hoc Networks (VANETs) in pursuing a more optimal intelligent transportation system that can provide various intelligent solutions and enable a variety of applications for vehicular traffic. Massive volumes of data are produced and communicated wirelessly among the different relayed entities in these vehicular networks, which might entice adversaries and endanger the system with a wide range of security attacks. To ensure the security of such a sensitive network, we proposed a distributed authentication mechanism for IoV based on blockchain technology as a distributed ledger with an ouroboros algorithm. Using timestamp and challenge-response mechanisms, the proposed authentication model can withstand several security attacks such as Man-in-Middle (MiM) attacks, Distributed Denial of Service (DDoS) attacks, server spoofing attacks and more. The proposed method also provides a solution for single-point failure, forward secrecy, revocability, etc. We exhibit the security of our proposed model by using formal (mathematical) analysis and informal analysis. We used Random Oracle Model to perform the mathematical analysis. In addition, we compared the communication cost, computation cost, and security of the proposed model with the related existing studies. We have verified the security of the model by using AVISPA tool simulation. The security analysis and computation analysis show that the proposed protocol is viable.

Keywords: IoV; message authentication; random oracle model; blockchain; distributed server; revocability

1 Introduction

In this decade, all the industries are influenced by high-tech innovations; the need for connected devices and automation devices is increasing day by day. The Internet of Things (IoT) is a crucial member of the invention that changes modern-day connected devices. The IoT facilitates a physical object to be intelligent by communicating with other devices. By 2025, forecasts suggest that more than 75 billion IoT-connected devices will be used. This count would be a nearly threefold increase from the IoT installed base in 2019 [1]. The cities are becoming smarter with the help of IoT like waste management, electricity supply, sanitization, efficient urban mobility, traffic management, etc. In the case of efficient urban mobility and traffic management, the IoV acts mail role. By using advanced networking technology like 5G and Cloud technologies, this system aims to achieve effective real-time communication among the Participant of the network. The IoV promises a system in which every vehicle on the street can communicate with each other, so it helps reduce accidents and increases the efficiency of fuel consumption and many more factors [2]. IoV Is a network of vehicles where the vehicle can communicate with each other and communicate with the Road-Side Units (RSU), pedestrian's handheld devices, traffic signals, and public network using Vehicle to Vehicle (V2 V), Vehicle to the Road (V2R), as well as a Vehicle to Infrastructure (V2I) connectivity. In the IoV system, the vehicles are the core nodes of the network, which have the storage and computation power to process the environmental data. The vehicles are powered by n number of sensors that help them learn about the environment. The drivers, passengers, and pedestrians are considered users of the system. Recommendation-based systems can also benefit from the profile of the user. The sensors used in the vehicles generate a large amount of data given as input to the local compute unit to analyze the environmental factors. The local storage of the vehicle is used to store such input data and analyze results of the environment. Such information about the location, speed, traffic, road condition, local weather, and other required data is shared between the network participants [3].

However, despite several advantages that IoV offers, it has some significant challenges and difficulties also to be solved. In the IoV communication model, sensitive information is transmitted between vehicles and infrastructure in the insecure communication medium. Suppose the sensitive messages of the legal user are leaked. In that case, a malicious attacker can use it to perform network attacks and give wrong information to the other devices, and it can cause a fatal accident. Another critical issue in the IoV is transmitting data in real-time without delay. So, the IoV needs a lightweight transmission, computation, and processing protocol that helps to perform real-time communication effectively. Therefore, the IoV required a secure and effective message authentication protocol to ensure the road safety of the vehicular network user [4,5]. The following are the main security requirements that a specific message authentication protocol should follow,

- Confidentiality. The message transmitted between the different entities of the network should be kept secret or private, only the legal participants of the network should be able to validate the message.
- Untraceability and anonymity. The user's real identity must be kept secret; it should not be revealed in any circumstance. Even if a small part of the transmission got leaked, the remaining should not be compromised.
- Mutual authentication. The protocol of the IoV should help a vehicle get mutually authenticated among the other entities of the network and obtain a meaningful message of communication.
- Withstand password guessing attack. The protocol for secure IoV should resist the password guessing attack where an intruder tries to think the driver password, even when the intruder got the transferred message or the smart card credentials.
- Withstand against insider attacks. The insider attack happens within the privileged account. The confidential or trusted user of the network who accesses sensitive information misuses this account access and acts as an adversary. A suitable design of IoV protocol should withstand this attack.
- Withstand against device theft attacks. An intruder can extract the credential from the stolen device or the vehicle. In a well-designed protocol, the information removed from the device should not be enough for the intruder to access that particular network.

- Revocability. If a vehicle's smart card is stolen or the vehicle is dumped, the identity should be removed from the Distributed Authentication Server (DAS) database before the adversary uses it. The IoV protocol should give the option, and it should provide a re-registration option for the lost smart card.

Other than the above attacks, the IoV protocol should withstand some popular attacks like a man-in-the-middle-attack, impersonation attack, denial-of-service attack, SQL injections, dictionary attack, etc. [6] Most of the recent time IoV authentication servers are using the centralized registration server architecture. The problem with centralized architecture is a single-point failure. The central node failure can cause the entire system to fail. The centralized architecture only can be vertically scalable [7–9]. Horizontal scalability will contradict the single central unit characteristic of the system. The bottleneck can appear when the traffic spikes, as the server can only have a limited number of open ports to listen to vehicles' connections. This server can suffer from a denial-of-service attack (DoS) or DDoS. The centralized server could attract hackers to perform DoS attacks; DDoS attacks commonly overpower their targets by sending a huge number of legal packets from multiple attack sites. Consequently, the target spends its key resources on processing the attack packets and cannot attend to its legitimate vehicles. DDoS traffic also creates heavy congestion in the Internet core during extensive attacks, disrupting communication between all Internet users whose packets cross congested the routers. It leads to system failure and causes a large-scale accident on the road. To avoid such a DDoS attack, the distributed architecture is one of the solutions [10,11]. The DAS has various advantages over the centralized server. In distributed servers, more nodes can be easily added, so scalability will be easy to handle. All the nodes in the distributed system are linked to each other. So, nodes can easily share data with other nodes. Failure of one node does not lead to the failure of the entire distributed system. Other nodes can still communicate with each other. Distributed server results in low latency. If a particular node is located closer to the user, the distributed system makes sure that the user system receives traffic from that nearby node. Blockchain technology has many advantages like trust, decentralized structure, improved security and privacy, reduced cost, visibility and traceability, speed, immutability, individual control of data, tokenization, etc. A lot of research is happening around the advantages of blockchain these days. In this proposed model, we used one of the advantages of the blockchain called decentralized structure and property of distributed ledger. The overall design of the authentication server is decentralized in the proposed model, so to hold the transactions of the DAS, we need a distributed ledger. The distributed ledger is used to store the request of the vehicles and keys of the transaction like session keys and security keys, as specified in Section 4. Compared to the customarily distributed ledgers, the blockchain ledger has the advantage of Proof-of-Work (PoW). In Blockchain, PoW is used to validate transactions. It is a system that requires some computationally heavy tasks to validate the Block and add it to the chain. This method ensures that the data added to a blockchain is not false or manipulated. So, the DAS becomes more secure and immutable [11]. To avoid such problems of centralized servers and to use the advantages of blockchain, the proposed model suggests a DAS for authentication in the IoV environment by using the blockchain as a distributed ledger for handling the transactions.

The contribution of the proposed model is summarized as follows.

- We have used the blockchain and distributed server architecture for authentication in IoV environment. Miners use the Ouroboros algorithm to assure the correctness of credentials of vehicles.
- We have formally analyzed the framework using the famous Random Oracle Model and performed the framework's informal security analyses.

- The proposed model has solved the problem of revocability and single-point failure in the IoV environment.
- The proposed model has higher efficiency in communication cost over other related studies.

The paper is organized as follows: we have discussed the system's background in Section 2. In Section 3, we have explained about the proposed system and its stages. Formal security analysis and Informal security analysis is discussed in the Section 4 and Section 5 respectively. In Section 6, we have discussed about the performance analysis of the proposed system. Finally, we have given the conclusion of the proposed system.

2 Related Work

In this section, we discussed the various research that happened in IoV authentication protocol in recent times. Li et al. [12] proposed authentication with privacy preservation and nonrepudiation for IoV environment. However, Dua et al. [13] analyzed the framework of Li et al. [12] and pointed out that their research framework could not withstand the session key disclosure attack. At the same time, it does not provide user anonymity and untracebility. Recently, some researchers have concentrated on the lightweight framework to reduce the complexity of transmission in real-time. The authors Ying et al. [14] presented a scheme for a secure and lightweight authentication method for IoV, whereas Chen et al. [15] found that the Ying et al. [14] work has the disadvantage of location leakage, password guessing attacks, repeat attack, and same time consumes considerable authentication time. Then Chen et al. [15] introduced a secure framework for authentication for IoV to resolve the drawbacks of Ying et al. [14] however, the method presented by Chen et al. [15] has the drawback of high storage cost due to the vast amount of data stored in the memory. Vasudev et al. [16] proposed a secure and efficient message authentication protocol for IoV environment; they claimed that their proposed method could withstand various security issues in IoV. However, Yu et al. [17] demonstrate that Vasudev et al. [16] cannot withstand critical security attacks such as a middle-man attack, mutual authentication, and impersonation. Then they [17] introduce a secure authentication protocol in a smart city environment for IoV. However, they [17] do not address the problem of single-point failure, revocability Problem, or denial-of-service attack in the IoV environment. The scheme of them [17] has a high computational cost comparatively. Therefore, we proposed a distributed server architecture for the authentication model for IoV environment to resolve their observed security problems.

3 System Background

This section describes the system background and the building blocks of the proposed method,

3.1 Primitives for Cryptography

The prominent Elliptic Curve algorithm for digital signature is used in this proposed method [18]. There are three processes act a main role in the digital signature, those processes are discussed follow,

- Key Generation: $keygen\ (1^p) \rightarrow (PuK, PrK)$: The $Keygen()$ function is used to generate a private key Puk, and its corresponding PuK with the constraint for security p.
- Digital Signature Generation: $Sig\,(PrK, m) \rightarrow S_j$: The $Sig()$ function is used to generate a digital signature value S_j of the message m by using the PrK.
- Verification: $Ver\left(PuK, S_j, m\right) \rightarrow b\epsilon\,\{0, 1\}$: The $Ver()$ function is used to verify whether the digital signature S_j is a correct value for the message m with the help of the public key PuK.

The Digital signature function must not be forgeable [19]. That's mean legal signature S_j should not be forged by any probabilistic polynomial-time adversary without the private key PrK [20].

3.2 Adversary Model

The following are the two main goals of adversary A_d in this model,

- The A_d can win the game of impersonating vehicle V_m, so it can get authenticate into the authentication server A_n.
- The A_d can win the game of impersonating the authentication server A_n, so it can get authenticate into the vehicle V_m.

Adversary A_d is a probabilistic polynomial time attacker, viable attacker is described as follow,

- The Adversary A_d can block, insert, alter, and eavesdrop the message which is transmitted between the nodes through the communication medium.so, it can control the medium between the vehicle and their authentication servers.
- The Adversary A_d can obtain the smartcard of the vehicle or the password of the vehicle. If the A_d has acquired the smartcard, then he/she can extricate the secret information from the smartcard. So, he/she has the potential to compute the password space $\left|D_{pw}\right|$.
- The A_d can be another legal user but malicious user in the distributed authentication server.

3.3 Threat Model

To assess the proposed framework, we explained the attack statements including the well-known "Dolev-Yao threat model (DYTM)". The abilities of a malicious adversary are as follows. Mentioning to the DYTM model, an adversary can modify, inject, reply, eavesdrop or delete the transmitted messages in a public network [10–12]. The adversary can rob the smart card of the legal driver and retrieve the confidential information saved in storage by using the power analysis attacks. After having the confidential information, the adversary may attempt potential attacks, including MiM attack, Repeat Attack, wrong credential access, impersonate attack, server spoofing attack, etc. The adversary has complete control over the network; the capability of the adversary are he knows all the public data of the protocol, he can start any number of parallel protocol sessions, he can encrypt/decrypt if he has the key, he can build and send messages, he can compose/decompose messages and so on.

3.4 Blockchain

Blockchain is a system that records information to make it difficult or impossible to modify, hack or cheat the system. It is necessarily a digital ledger to store duplicated transactions and distribute them across the whole network of a computer system on the blockchain. It contains an ordered chain of blocks [21]. These blocks have a specified number of transactions. Each block is connected to the previous block by referring to the previous block's hash. We suggested using a blockchain similar to the bitcoin in our proposed model, as shown in Fig. 1. It contains several blocks, timestamp, previous block hash value, and Merkle tree root. In our proposed model, the distributed authentication server are miners of the blockchain network, the miner of the blockchain network; the miner will issue the next block. Generally, if the miner wants to create a new node, he must complete some PoW [22], but PoW has always consumed high computational power to check the transaction and add those transactions into a new block. This method is expensive because it costs a lot of energy and money. To overcome this drawback, a new approach was introduced by Scott Nadal, and Sunny King called Proof of Stack (PoS) or Delegated Proof of Stack (DPoS) [9]. These methods select one of the miners randomly to achieve a new block. The PoS and DPoS are more effective methods compared to PoW. In our proposed model, we used the ouroboros model, which is the model of PoS [22], which is provable and secure. It is used as a consensus system to enter a new block of transactions in the blockchain network. Blockchains are found to consume exorbitant amount of energy because of the algorithm used in PoW. The ouroboros can manage thousands of transactions in seconds and reduce energy consumption compared to PoW. When a vehicle requests registration to the authentication server, the DAS node must check the vehicle information specified in Fig. 2. Following the successful verification, the blockchain node will enter the transaction into the blockchain network, and the entire nodes will create a new block through the Ouroboros algorithm. Whenever a vehicle wants to access the authentication system to get authorized in the network, the DAS will cross-check the transactions in the blockchain ledger and update the new access in the blockchain network. The architecture of the proposed method is illustrated in Fig. 1; using the Road-Side Unit (RSU), Infrastructure, and different sensors vehicle can communicate with the distributed authentication server.

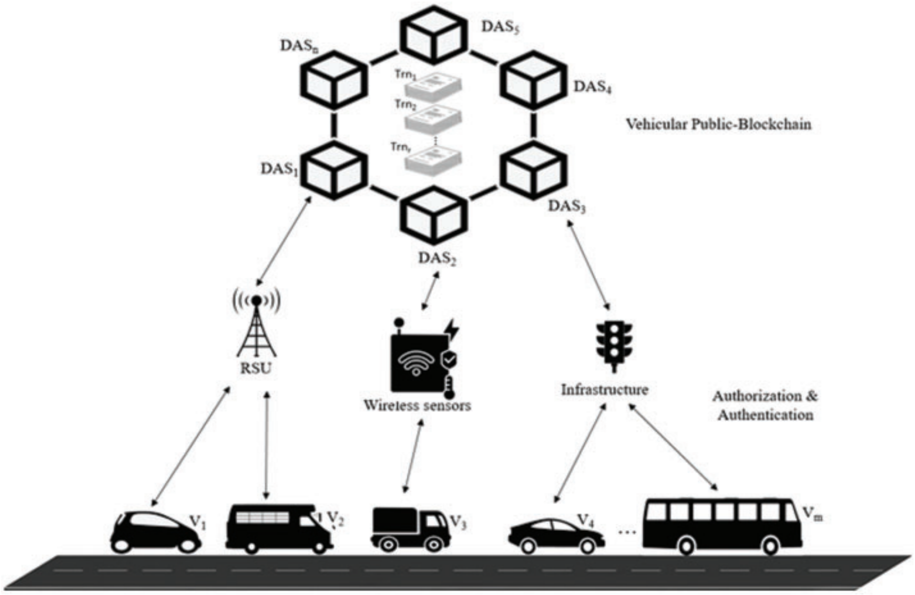


Figure 1: Blockchain based distributed authentication server architecture

4 Proposed System

The architecture of the proposed model is shown in Fig. 1. The V_1, V_2,...,V_m are vehicles that wanted to connect to the distributed authentication server. The infrastructure, RSU, and wireless sensors are mediums allow the vehicles to connect to the DAS through the public internet. The DAS is a distributed server for authentication which authorize the vehicle to take part in the network for communication, the DAS is backed by the blockchain ledger to store the transaction Trn_1, $Trn_2, \ldots,$ Trn_r of all the vehicles. The proposed system has 4 phases shown below. In Tab. 1. we have summarized the notations we used in the framework.

1. Low level formatting
2. Vehicle Enrollment
3. Two-way Authentication
4. Revocability

Table 1: Summary of notations

Notation	Explanation
A_n	nth Distributed authentication server
G	Generator of additive group A_g
b	Output bit length
h_m	Hash function
PuK	Public key
PrK	Private key
V_m	Vehicle m
R_{vm}	Random number generated by vehicle m
RVC_{vm}	Revocation status of vehicle m
S_{vm}	Digital signature vehicle V_m
TS	Time stamp
VID_m	Identity of vehicle m
PsW_m	Password of vehicle m
$u,\ r_i$	Random number
N_{vm}	New block in block chain
γ	Turing machine
Enr	enrolment requirements
id_{vm} *and* id_{An}	peer identities

4.1 Low Level Formatting

In the proposed system there are n-numbers of DAS for the simplicity it is represented as A_n. In this stage all nodes A_n concord with an additive group A_g with order P which is generated by the generator G and it's five hash functions h_m: $(0,1)^* \to (0,1)^b$, $h_2 : (0,1)^* \to \left(0 \ to \ 2^{10}\right)$, $h_4 : (0,1)^* \to Z_q^*$, where b is the bit output bit length and m = 0, 1, 3. Every node A_n will generate its own private key $PrK_{An} \in Z_q^*$ and a public key is calculated as $PuK_{An} = PrK_{An}.G$. We assume that the public key of each node will be known by all other nodes and vehicles then the node A_n stores the private key PrK_{An} in its memory and keep it as a secret and distribute the attributes $\{A_g, G, PuK_{An},\ h_0\ to\ h_4\}$ to all other nodes.

4.2 Vehicle Enrollment

When a vehicle V_m wants to access the authentication nodes, it needs to be enrolled with the Authentication nodes. Fig. 2 shows the process of vehicle enrollment, and it is narrated as follows in steps.

Step 1: A Vehicle V_m chooses the closest node A_n based on path loss and fading effect to enroll itself in the network and select its identity VID_m and a random number R_{vm} which is derived from the set Z_q^* and set the values for revocation parameter as zero, $RVC_{vm} = 0$. Moreover, evaluate the public key $PuK_{vm} = R_{vm} * G$, $S_{vm} = Sig\,(R_{vm}, VID_m \,||\, TS_1 || \, RVC_{vm})$ where TS is a timestamp. The V_m sends the message $\{TS_1, VID_m, Enr,\ PuK_{vm}, S_{vm}\}$ and its information (e.g., Reg number, chase number and unique digital sign) to A_n through a secure channel where $S_{v\,m}$ is a signature of vehicle V_m and Enr is the enrolment requirements.

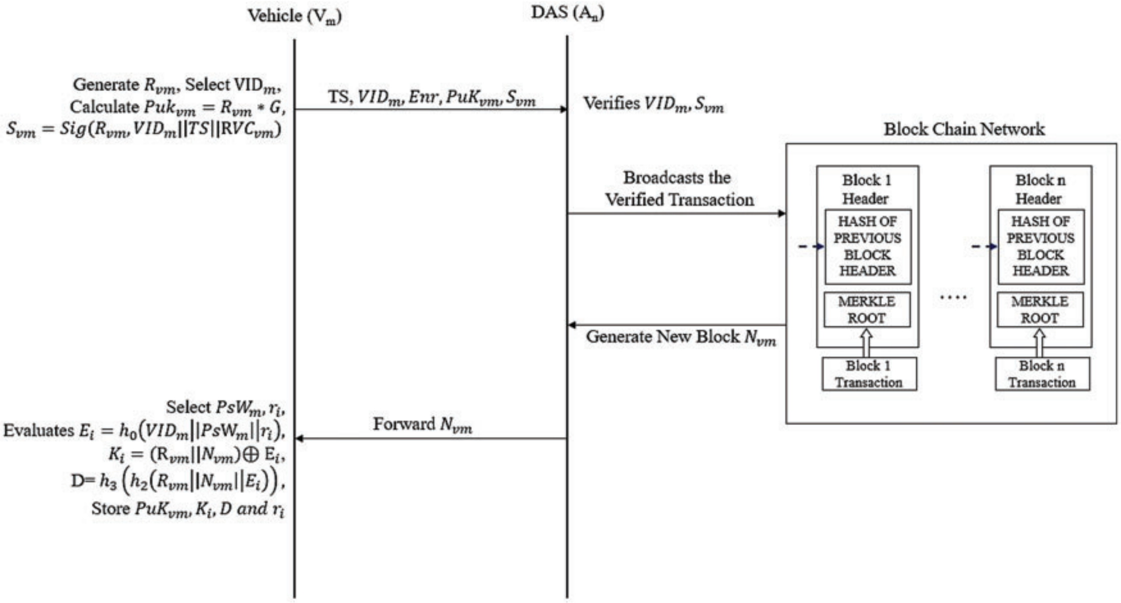

Vehicle (V_m)
DAS (A_n)
Generate R_{vm}, Select VID$_m$,
Calculate $Puk_{vm} = R_{vm} * G$,
$S_{vm} = Sig(R_{vm}, VID_m||TS||RVC_{vm})$
TS, $VID_m, Enr, PuK_{vm}, S_{vm}$
Verifies VID_m, S_{vm}
Block Chain Network
Broadcasts the Verified Transaction
Block 1 Header
HASH OF PREVIOUS BLOCK HEADER
MERKLE ROOT
Block 1 Transaction
Block n Header
HASH OF PREVIOUS BLOCK HEADER
MERKLE ROOT
Block n Transaction
Generate New Block N_{vm}
Forward N_{vm}
Select PsW_m, r_i,
Evaluates $E_i = h_0(VID_m||PsW_m||r_i)$,
$K_i = (R_{vm}||N_{vm}) \oplus E_i$,
D= $h_3\left(h_2(R_{vm}||N_{vm}||E_i)\right)$,
Store PuK_{vm}, K_i, D and r_i

Figure 2: Sequence diagram of vehicle enrollment phase

Step 2: After getting the message, A_n will check the authenticity of the vehicle details and the timestamp. Then A_n Assign the value of $RVC_{vm} = 0$ and verify the equation $Ver(PuK_{vm}, S_{vm}, VID_m \ ||TS_1|| RVC_{vm}) = 1$ or not. If the equation does not give the value 1, then the A_n will discard the enrollment request from the vehicle. Otherwise, the A_n will verify whether VID_m has been registered in the blockchain. If the vehicle transaction already available in the blockchain and $RVC_m = 0$ then the A_n will reject the request for enrolment. If not, A_n calculate $An_{vm} = sig\left(PrK_{An,}\ VID_m\ ||ID_{An}||\ PuK_{vm}\ ||RVC_{vm} = 0||\ TS_2\right)$ where TS_2 is the timestamp for the current transaction $\{VID_m,\ PuK_{vm},\ ID_{An},\ PuK_{An},\ RVC_{vm},\ TS_2,\ S_{vm}, An_{vm}\}$ will be broadcast to the blockchain network. Then the miner can generate a fresh block for vehicle V_m as N_{vm} by using the protocol called ouroboros. This protocol is a consensus algorithm for the distributed network [22]. Where, N_{vm} is the number of blocks in the blockchain. By using the secure channel, the N_{vm} is transmitted to V_m from A_n . Where, the signature An_{vm} represents that the node V_m has verified that the PuK_{vm} is belongs to the specific vehicle VID_m. The node V_m is responsible for this claim.

Step 3: Once the message is received by the vehicle V_m, then the vehicle V_m selects the password PsW_m and a random number r_i. After deciding those values, the V_m evaluates $E_i = h_0(VID_m|\,|PsW_m|\,|r_i)$, $K_i = (R_{vm}||N_{vm}) \oplus E_i,\ \ D = h_3\,(h_2\,(R_{vm}\ ||N_{vm}||\ E_i))$. Finally, the vehicle V_m stores $PuK_{vm},\ K_i, D$ and r_i in its local memory.

4.3 Two-way Authentication

If the vehicle wants to authenticate in the network, the vehicle needs to succuss the two-way authentication with the nodes. As shown in Fig. 3, the process of two-way authentication is explained as follows.

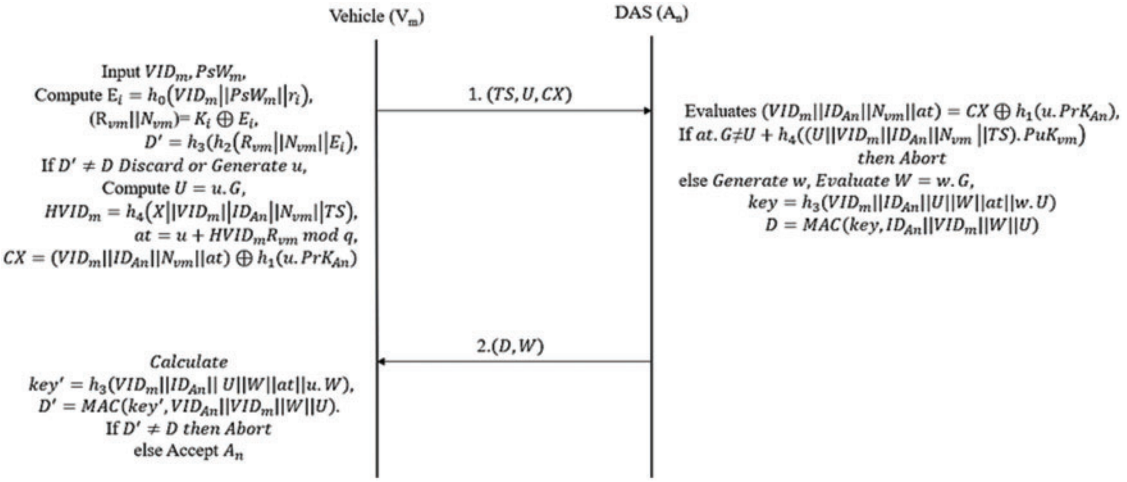

Vehicle (V_m)
DAS (A_n)
Input $VID_m, PsW_m,$
Compute $E_i = h_0(VID_m||PsW_m||r_i),$
$(R_{vm}||N_{vm}) = K_i \oplus E_i,$
$D' = h_3(h_2(R_{vm}||N_{vm}||E_i),$
If $D' \neq D$ Discard or Generate u,
Compute $U = u.G,$
$HVID_m = h_4(X||VID_m||ID_{An}||N_{vm}||TS),$
$at = u + HVID_m R_{vm} \bmod q,$
$CX = (VID_m||ID_{An}||N_{vm}||at) \oplus h_1(u.PrK_{An})$
1. (TS, U, CX)
Evaluates $(VID_m||ID_{An}||N_{vm}||at) = CX \oplus h_1(u.PrK_{An}),$
If $at.G \neq U + h_4((U||VID_m||ID_{An}||N_{vm}||TS).PuK_{vm})$
then Abort
else Generate w, Evaluate $W = w.G,$
$key = h_3(VID_m||ID_{An}||U||W||at||w.U)$
$D = MAC(key, ID_{An}||VID_m||W||U)$
2.(D, W)
Calculate
$key' = h_3(VID_m||ID_{An}||U||W||at||u.W),$
$D' = MAC(key', VID_{An}||VID_m||W||U).$
If $D' \neq D$ then Abort
else Accept A_n

Figure 3: Sequence diagram of two-way authentication phase

Step 1: The vehicle V_m Evaluates $E_i = h_0\,(VID_m\,||PsW_m||\,r_i)$, $R_{vm}||N_{vm} = K_i \oplus E_i$, $D' = h_3\,(h_2\,(R_{vm}\,||N_{vm}||\,E_i))$ and verify whether D and D' are same. If the values are not same, the V_m will discard the current session. If the values are same, the vehicle generate a random number say $u \epsilon Z_q^*$, and evaluates $U = u.G$, $HVID_m = h_4\,(X\,||\,VID_m||\,ID_{An}\,||N_{vm}||\,TS)$, $at = u + HVID_m R_{vm} modq)$, $CX = (VID_m\,||ID_{An}||\,N_{vm}||at) \oplus h_1\,(u.PrK_{An})$, where TS is current timestamp. Then V_m send the $\{TS, U, CX\}$ to A_n by using the public channel.

Step 2: Once A_n received the message $\{TC, U, CX\}$, it verifies TS and evaluates $(VID_m\,||ID_{An}||\,N_{vm}||\,at) = CX \oplus h_1\,(u.PrK_{An})$ then the A_n checks the following conditions satisfiability.

Condition 1: VID_m exists in the block N_{vm}.

Condition 2: Revocation status of the VID_m is zero, RVC_{vm} holds in the new block N_{vm}.

Condition 3: The blocks $N_u > N_{vm}$ does not have tuple $\{VID_m, PuK_{vm}, ID_{An}, PrK_{An}, RVC_{vm} = 1, S_{vm}, An_{vm}\}$

A_n Discard the session, even one of the above condition fails. Otherwise A_n takes the PuK_{vm} of V_m and verify the equation $at.G = U + h_4\,(U\,||\,VID_m||\,ID_{An}\,||N_{vm}||\,TS)\,.PuK_{vm}$ holds. If the equation does not hold, then A_n discard the session. If the equation holds, then A_n generates a random number $w \epsilon Z_q^*$ and evaluates $W = w.G$, $key = h_3\,(VID_m\,||ID_{An}|\,|U|\,|W|\,|at||\,w.U)$, $D = MAC\,(key,\ ID_{An}\,||\,VID_m|\,|W||\,U)$ after that A_n return the message $\{D, W\}$ to V_m via a public channel.

Step 3: After getting the message $\{D, W\}$ fromA_n. The V_m Evaluate $key' = h_3(VID_m\|\,|ID_{An}|\,|U|\,|W|\,\|at\|\|u.W)$, $D' = MAC\,(key', ID_{An}\,||\,VID_m|\,|W||\,U)$ and verify whether $D' = D$. If the condition is true, V_m completes the authenticate the A_n. Where MAC is Message Authentication Code which is calculated with the secret session key.

4.4 Revocability

The procedure of the revocability phase is explained in this section. When the vehicle's smartcard is lost, stolen the system should have to remove the account and re-register it to the authentication server. The process of revocability is explained as follows, Step1: The vehicle V_m chooses the nearest authentication server S_j in the distributed system and then select a fresh random number $R'_{vm} \epsilon Z_q^*$, set $RVC_{vm} = 0$, and compute the $PuK_{vm}^* = R'_{vm} * G$, $S'_{vm} = Sig\left(R'_{vm}, VID_m \,||TS_3||\, RVC_{vm}\right)$ where TS_3 is timestamp. This vehicle V_m submits the messages $\left\{TS_3, VID_m, RVC, PuK'_{vm}, S'_{vm}\right\}$ and several private attributes to A_n via a protected channel, where RVC is the prerequisite of revocability.

Step 2: Based on the acknowledgement of the message, the authentication node A_n will first verify the genuineness of private attributes and timestamp. After that, A_n will set $RVC_{vm} = 0$, and checks the equation $Ver\left(PuK'_{vm}, S'_{vm},\ VID_m \,||TS_3||\, RVC_{vm}\right) = 1$ holds. When it holds the condition, A_n gets the old PuK_{vm} of the VID_m by checking the blockchain in the background and computes.

5 Formal Security Analysis

This section explains the security analysis of the proposed method and how it meets the security requirements. The Low-level formatting phase, the Vehicle Enrollment phase, will be performed in the protected channel. The proposed system may endure security threads in the two-way authentication stage. Hence, we explain the security of the two-way authentication phase in this section. We proposed a security mechanism based on the work of Yu et al. [23] and Goldwasser et al. [23–26]. The security model of our system is designed by an adversary A_d and a turing-machine γ with the probabilistic polynomial time. Let instance $\prod_V^s$ be the vehicle in session s, A_d can create an oracle query as following,

1. $Extract V_m$: This inquiry imitates A_d registration as a legitimate vehicle. A_d issues this query with V_m's identity VID_m. γ generates the new block in block chain N_{vm}, V_m's PrK and PuK, saves them in the list L_{vm} and returns N_{vm} and VID_m to A_d.
2. $Extract A_n$: This inquiry imitates A_d registration as a legal A_n. A_d issues this inquiry with A_n's identity ID_{An}, γ generates A_n's $PuK\ and\ PrK$, saves them in List L_{An}.
3. $Send - Qr\ (p,\ s,\ p',\ M)$: This inquiry imitates the participant p sends message M to the $\prod_p^s$. A_d issues query and receive a response which is specified by the method.
4. $Leak - Qr\ (V_m,\ A_n\ ,\ s)$: This inquiry imitates the outflow of session-key attack and return the session key key as an output.

There are 2 corrupt queries,

1. $C\,(VID_m, PsM_m)$: This inquiry imitates password-leakage attack and obtain the vehicle password Psw_m.
2. $C\,(A_n)$: This query imitates the A_n Attack.

Definition 1: Similar sessions: The session of the instance vehicle $\prod_V^s$ and authentication node $\prod_{TA}^s$ are considered as similar if, s = s', $id_{vm} = id_{An}$ and both V_m and A_n have accepted it where $id_{vm}\ and\ id_{An}$ are peer identities.

Definition 2: Authentication protocol: The following properties should be held to say authentication protocol is secure,

$\prod_V^s$ and $\prod_{TA}^s$ are similar sessions and they should accept each other.

$\prod_V^s$ and $\prod_{TA}^s$ should obtain the same keys.

The probability of $\prod_V^s$ accepted A_d as $\prod_{TA}^s$ is trivial.

The probability of $\prod_{TA}^s$ accepted A_d as $\prod_V^s$ is trivial.

Initially, we discuss two mathematical challenges to analyze our proposed protocol as follows, *Definition 3:* Discrete logarithmic problem (DLP): Say $U = u.G$ where $u\epsilon Z_q^*$, $U = G$ impracticable to compute u. Our method is shown follow,

$V_m \rightarrow A_n: I_1 = \{TS, U, CX\}$

$A_n \rightarrow V_m: I_2 = \{D, W\}$

Theorem 1: Secure authentication of Vehicle: In our system, if hash function $h_0, h_1, .., h_4$ are ideally random functions, then the problem DLP is hard, so $\prod_{TA}^{s}$ will be accepted. So that there will not be any polynomial adversary who can cast the authentication message of a legal vehicles by a non-trivial probability.

Proof: Let assume that A_d cast the message of legal vehicle with a non-trivial probability. Then the DLP can be solve by a γ with a non-trivial probability by using the A_d. Let say the DLP probability is $P_{win}[DLP]$. Given DLP $(G, G_{Vc} = R_{Vc}.G)$, the task of γ is to evaluate $(R_{Vm}\epsilon Z_q^*)$. To win this, the γ should have to imitate an environmental of our method which is identical from the real method to the A_d. So, the γ should respond to all queries given by the A_d. To win this, the γ should generate all the parameter $\left\{A_g, G, PuK_{An}, h_0\ to\ h_4\right\}$ and publish them same time the γ need to generate all private keys of the vehicle $PrK_{vm}\epsilon Z_q^*$ other than private key R_{Vc} of the challenger VID_C and evaluate their public key $PuK_{vm} = R_{Vm}.G$. Then the γ will respond to the queries of A_d as follows,

1. $\mathrm{H_m}$ $(\mathrm{m_i})$: The query $\mathrm{H_m}$ is a hash query for message $\mathrm{m_i}$. The $\mathrm{H_m}$ $(\mathrm{m_i})$ where $\mathrm{i} = 0$ to 4, will maintain a list called $\mathrm{L_{hm}}$ which value is initiated as empty. The γ will check for the message $\mathrm{m_i}$ in the list $\mathrm{L_{hm}}$. If the $\mathrm{m_i}$ is exist in $\mathrm{L_{hm}}$, then the γ will return the value of $\mathrm{H_m}$ to $\mathrm{A_d}$. Otherwise, random number $\mathrm{h_m}$ will be generated by γ and stores the value $(\mathrm{m_i},\ \mathrm{h_m})$ into the list $\mathrm{L_{hm}}$ and give the value $\mathrm{h_m}$ to $\mathrm{A_d}$.
2. Extract$\mathrm{V_m}$: Here, the γ will maintain a list called $\mathrm{L_{Vm}}$ which value is initialized to empty. Then γ checks the $\mathrm{L_{Vm}}$ whether the tuple $(\mathrm{VID_m}, \mathrm{Puk_{Vm}}, \mathrm{R_{Vm}},\ \mathrm{N_{Vm}})$ exists. If it exists γ will return the $\mathrm{VID_m}$ and $\mathrm{N_{vm}}$ to the $\mathrm{A_d}$. Otherwise, it will follow the following procedure,
   A) If $\mathrm{VID_m} \neq \mathrm{VID_c}$, then γ will assign a random number to $\mathrm{N_{Vm}}$, select a random number $\mathrm{R_{Vm}}\epsilon \mathrm{Z_q^*}$ and evaluate the $\mathrm{PuK_{Vm}} = \mathrm{R_{Vm}.G}$. γ saves the tuple $(\mathrm{VID_m}, \mathrm{PuK_{Vm}}, \mathrm{R_{Vm}.N_{Vm}})$ in the list $\mathrm{L_{Vm}}$ and return $\mathrm{VID_m}$ and$\mathrm{N_{Vm}}$ to the $\mathrm{A_d}$.
   B) If $\mathrm{VID_m} = \mathrm{VID_c}$, then γ will assign a random number to $\mathrm{N_{Vm}}$, sets $\mathrm{R_{Vm}} = \theta$, and requests the $\prod_{\mathrm{V}}^{\mathrm{s}}$ to know private key of$\mathrm{VID_m}$. γ stores the tuple $(\mathrm{VID_c}, \mathrm{PuK_{VC}},\ \mathrm{R_{VC}}, \mathrm{N_{VC}})$ to the $\mathrm{A_d}$.
3. Extract$\mathrm{A_n}$: The γ maintain a list called $\mathrm{L_{An}}$ which values are initialized as empty. The γ will check the list $\mathrm{L_{An}}$ for the value of tuple $(\mathrm{ID_{An}}, \mathrm{PuK_{An}.PrK_{An}})$ Exists or not. If it exists, then γ will return the value of $\mathrm{ID_{An}}$ to the $\mathrm{A_d}$. Otherwise, the γ generate a $\mathrm{PrK_{An}}$ as a random value, evaluate $\mathrm{Puk_{An}} = \mathrm{Prk_{An}}$. G and save the tuple $(\mathrm{ID_{An}}, \mathrm{PuK_{An}}, \mathrm{PrK_{An}})$ in the list $\mathrm{L_{An}}$ and give the value of $\mathrm{ID_{An}}$ to the $\mathrm{A_d}$.
4. $\mathrm{Send - Qr}\ \ (\mathrm{V_m}, \mathrm{s}, \mathrm{A_n}, \mathrm{M})$: $\mathrm{A_d}$ sends the initial message $\mathrm{M_1}$ to the γ. The CT will be decrypted by γ and acquire $\mathrm{VID_m}$, $\mathrm{PuK_{Vm}}$ and returns $\mathrm{M_2}$ to $\mathrm{A_d}$.
5. $\mathrm{Send - Qr}\ \ (\mathrm{A_n}, \mathrm{s},\ \mathrm{V_m}, \mathrm{M})$: Once the γ gets the query send, it will check the equation $\mathrm{VID_m} = \mathrm{VID_c}$ holds or not. If it holds, then γ asks the $\prod_{\mathrm{V}}^{\mathrm{s}}$ to obtain the message $\mathrm{M_1}$ and send it to $\mathrm{A_d}$. Otherwise γ send the message $\mathrm{M_1}$ to $\mathrm{A_d}$ by following the steps of the proposed method.
6. $\mathrm{Leak - Qr}\ \ (\mathrm{V_m}, \mathrm{A_n}, \mathrm{s})$: In this query, the γ returns the key to the session among $\mathrm{V_m}$ and $\mathrm{A_n}$ in the current session s.
7. $\mathrm{Corrupt\ \ Query:\ C}\ \ (\mathrm{VID_m},\ \mathrm{f})$: once the γ receives the query, it asks $\prod_{\mathrm{V}}^{\mathrm{s}}$ to give the password $\mathrm{PsW_m}$ or the secret value of the vehicle. If $\mathrm{VID_m} = \mathrm{VID_c}$, then the γ will discard the request.
8. $\mathrm{C}\ \ (\mathrm{A_n})$: The γ will return the $\mathrm{PrK_{An}}$.

As per the queries, if A_d can by-pass vehicle authentication phase successfully, it implies that the adversary A_d can successfully forged the authentication message $\{TS, U, CX\}$ and send the message to the turing machine γ, where CX is given in the Section 5.3. A_d has casted another message $\{TS, U, CX'\}$ According to the forking theorem in [27] by repeating the imitation with different values of hash h_4. Therefore, we got two Eqs. (1) and (2) as shown below.

$$at = u + HVID_m R_{vm} \quad (1)$$

$$at' = u + HVID'_m R_{vm} \quad (2)$$

By the Eqs. (1) and (2),

$$at - at' = (HVID_m - HVID'_m)\ R_{vm} \quad (3)$$

The turing machine γ evaluates $(at - at')\ (HVID_m - HVID'_m)^{-1}$ as the solution for the DLP. The probability is, Let assume, λ is the non-trivial probability of the A_d which casts an authentication message of legal vehicle and ρ is the probability of γ getting success in the DLP when the A_d missed to cast the authorization message of vehicle. Based on the work of Yu et al. [23] the probability of turing machine γ for winning the DLP can be reduced as in Eq. (4),

$$P_{win}[DLP] = \frac{1}{q_s}.\,(\lambda + (1 - \lambda)\,.\rho) = \frac{\lambda + (q_s - \lambda)\,.\rho}{q_s} \quad (4)$$

where q_s is number of queries sent. According to the Eq. (5), $P_{win}[DLP]$ is non-trivial and the γ can get succussed in DLP with the non-trivial. Therefore, the legal vehicle authentication message cannot be cast by any polynomial A_d with a non-trivial probability.

Theorem 2: Secure Authentication of A_n: In our proposed method, if MAC and the hash functions $h_0, h_1,..\ h_4$ are ideally random functions, and $\prod_V^s$ has trusted. The legal A_n authentication message cannot be break by any polynomial A_d with non-trivial probability.

Proof: Let assume, the legal A_n authentication message can be breaking the A_d with non-trivial probability. Then there will be a γ, which can win the underlying MAC without the secret session key *key* with a non-trivial probability by using A_d.

A challenger and a MAC server $(\prod_{MAC})$ with a secret key *key* are the two participants of the MAC-game; the MAC value of any message can be requested by the challenger to $\prod_{MAC}$ as many times as it wants. Let the probability for winner the MAC-game is $P_{win}[MAC]$. The procedure of the game is given follow,

1. The challenger can send two messages $M_1\&M_2$ to the $\prod_{MAC}$.
2. The $\prod_{MAC}$ can select a random value $r\epsilon\{1, 2\}$. Say if r value is one, then $\prod_{MAC}$ returns $MAC\,(key, M_1)$ to the A_d. Otherwise, it will return $MAC\,(key,\ M_2)$.
3. The challenger can win the game by guessing the value of r'. Therefore $r = r'$.

The γ imitate the atmosphere of the method which is identical from the actual proposed method to the A_d, therefore the γ must response to each queries requested by the A_d; Initially the γ setup all the parameters of system other than identity of A_n's challenger $ID'_{Ac}s$ private key PrK_{Sc}. The γ should answer the hash, execute, and leak query as like in the Theorem 1. Then the γ answers A_n's query as below,

1. *Extract* V_m: Here, the γ will maintain a list called L_{Vm} which is initialized as empty and check if a tuple $(VID_m, PuK_{vm},\ R_{vm}, N_{vm},\ )$ exists in the list L_{vm}. If the tuple exists in L_{vm} then it will

return VID_m, $N_{vm}$to the A_d else γ will generate a random number as revocation status N_{vm}, select one more random number $R_{vm}\epsilon Z_q^*$ and evaluate the public key $PuK_{vm} = R_{vm}.G$. Then γ saves the tuple $(VID_m, PuK_{vm}, R_{vm}, N_{vm})$ in the list L_{vm} and give the values of VID_m and N_{vm} to the A_d.

2. $ExtractA_n$: The γ maintain a list called L_{An}which is initialized to empty. The γ will check if a tuple $(ID_{An}, PuK_{An},\ PrK_{An})$ exists in the list L_{An}. If the tuple exists, the γ will ID_{An} to the A_d. Otherwise, γ will follow the following procedure,
   A) If $ID_{An} = ID_{Ac}$, then the γ will set the $PrK_{An} = \theta$ and request the $\prod_{TA}^{s}$ to access public key so PuK_{An} of ID_{An}, saves the tuple $(ID_{An}, PuK_{An}, PrK_{An})$ in the list L_{An} and give the ID_{An} to A_d.
   B) If $ID_{An} \neq ID_{Ac}$, then the γ will set a random number to PrK_{An}, evaluate $PuK_{An}{=}PrK_{An}.G$, save the tuple $(ID_{An}, PuK_{An}, PrK_{An})$ into the list L_{An}.
3. $Send\ \ (V_m, s, A_n, M)$: An initially sends the message M_1 to the γ, then based on the proposed system, the γ operates and returns the message M_2 to the A_d. After the message M_2 from A_d. The γ sends the result of vehicle authentication message based on M_1& M_2 and result $\prod_{MAC}$ to verify the value of the MAC.
4. $Send\,(A_n, s, V_m, M)$: After getting this query, the γ will send the initial message M_1 to A_d by using the private key of vehicle PrK_{Vm} as our method specified. If $ID_{An} = ID_0$, then γ will discard the game.
5. $C\,(VID_m{,}f)$: Here, γ request $\prod_{V}^{s}$ to get the corresponding password PsW_m or the secret values of the vehicle.
6. $C\,(A_n)$: After getting the query, γ checks the equation $ID_{An} = ID_o$ holds, if the values match then γ discard the game, otherwise it will return the private key PrK_{An}.

Based on above queries, if the A_d can pass the authentication of A_n successfully, then A_n forge a message $\{D, W\}$ and send the message to γ, where the equation of D is explained in Section 5.3. Upon receiving $\{D, W\}$ the γ sends $M_1 = \{ID_{An}||VID_m||W||U\}$ and a random number $M_1{=}R_m$ to the $\prod_{MAC}$. Then $\prod_{MAC}$ sends MAC (key, M_r) to γ. Then γ can check the value of b is 1 or 2 by checking the $\{D, W\}$. Let assume λ is a non-trivial probability of A_n gets a legal authentication message of [23]. So, the probability of γ getting succussed in the MAC can be evaluated as follows in Eq. (5),

$$P_{win}\,[MAC] = \frac{1}{q_s}.\left(\lambda + (1-\lambda)\,.\frac{1}{2}\right) + \left(\frac{q_s-1}{qs}.\frac{1}{2}\right) - \frac{1}{2} = \frac{\lambda}{2q_s} \tag{5}$$

According to the above equation, the $P_{win}\,[MAC]$ is non-trivial and the λ can win the MAC game with non-trivial. Therefore, the legalA_n's authentication message cannot be forged by any polynomial A_n in a non-trivial probability.

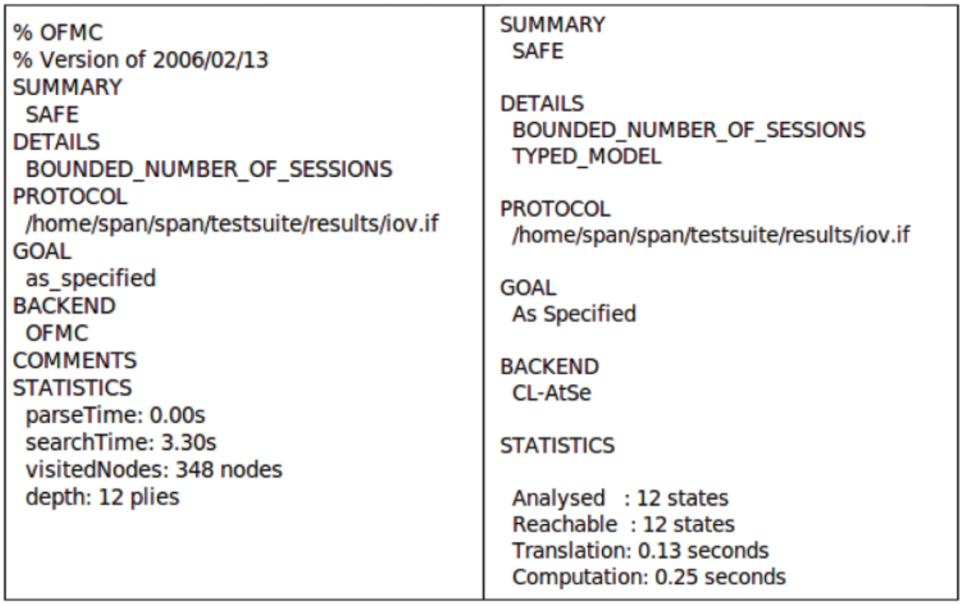
Theorem 3: The proposed method will be a secure protocol, if it follows the below condition,

1. $\prod_{V}^{s}$ and $\prod_{TA}^{s}$ has been accepted.
2. Hash h_0 to h_1, MAC are ideally random functions.
3. The Discrete probability problem is hard.

Proof: According to theorem 1 and 2, we understand the legal V_m or A_n cannot be forged by any polynomial adversary A_d. If the DLP is hard and the MAC is an ideally random function. Since $\prod_{V}^{s}$ has been trusted, it ensures there is a noble session of the method that has derived exactly the similar key. Based on above analysis, the suggested method is a reliable protocol.

6 Formal Security Verification Using AVISPA

We analyze the security of the proposed framework by using AVISPA tool simulation against the reply attack and MIM attack. The AVISPA toolset uses the "High-Language Protocol Specification Language" (HLPSL) language for specifying cryptographic protocols [28]. HLPSL specifications are translated into equivalent IF specifications by the HLPSL2IF translator. The current version of the tool integrates the four back-ends as follows, On-the-fly Model-Checker (OFMC), Constraint-Logic-based Attack Searcher (CL-AtSe), SAT-based Model-Checker (SATMC), Tree Automata based on Automatic Approximations (TA4SP). To analyze the security of our proposed system, we used the rule-oriented HLPSL. More details about HLPSL and AVISPA toolset specifications are explained in [28,29]. Various roles for the vehicle V_m, distributed authentication server A_n, goal, environment, and session are realized by using HSPSL for our proposed model. The TA4SP and SATMC do not have the support for XOR operations, so we have simulated the protocol with OFMC and CL-AtSe. The results of the proposed model are given in Fig. 4. Based on the result, we proved that our proposed method is viable to resist the MIM attack and reply attack based on the result.



```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/iov.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 3.30s
  visitedNodes: 348 nodes
  depth: 12 plies
```

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/iov.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 12 states
  Reachable  : 12 states
  Translation: 0.13 seconds
  Computation: 0.25 seconds
```

Figure 4: Simulation results of AVISPA

7 Informal Security Analysis

- Mutual Authentication. Based On theorem 1, if DLP problem is hard and MAC is an ideally random function, then we can determine that there will be no polynomial adversary that can be able to cast a legitimate V_m or A_n. Therefore, the vehicle V_m and the A_n can effectively authenticate to each other.
- Impersonate Attack. An impersonation attack is an attack in which an adversary successfully assumes the identity of one of the legal nodes in a system or a communication protocol [30] . In our proposed method, if the adversary A_d wants to impersonate a vehicle V_m, then the adversary must cast the message $\{TS, U, CX\}$ correctly. Based on Theorem 1 shows that it is not possible because the DLP problem is hard.

- *Man-in-Middle Attack.* In this attack, the Intruder secretly communicates and probably alters the communications among two nodes who believe that they are directly communicating with each other, as the Intruder has injected themselves between the two nodes [31]. In our proposed method, the message transferred between legitimate V_m or A_n are protected by $\{u, PuK_{An}\}$, the Intruder cannot cast the message without knowing the $u\ or\ PrK_{An}$. Hence, our system can resist the man-in-middle attack.
- *Server Spoofing Attack.* Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source [32–35]. According to theorem 1, without the private key of the legitimate user or authentication node, no polynomial adversary can cast the message. In our proposed method, the V_m or A_n only know their own PrK, does not know other vehicles or authentication node's private key. Hence the intruder cannot spoof any vehicles V_m to other A_n.
- *Repeat Attack.* A repeat attack is when the intruder records a communication session and replays the entire session, or some portion of the session, at a later on [36]. We prevent the repeat attack by using the challenge and response method in our proposed way. We are using two random numbers u and w.
- *Untraceable and Anonymity.* The vehicle's identity VID_m is encrypted by using the hash function $h_1\,(u.PrK_{An})$ so that we ensure the vehicle's real identity got protected. At the same time the value of the hash function $h_1\,(u.PrK_{An})$ refreshed for every session because of the random number u used in the computation of the function. The intruder cannot calculate the value of the hash function without knowing the random number u and the private key Prk_{An} of A_n. Therefore, our method ensures the vehicle activity is Untraceable and anonymous [37–40].
- *Poison block attack.* A poison block attack, sometimes referred to as a 'big block attack' is where a malicious miner will create a huge block that takes smaller miners with less hash power a long time to validate. In the proposed system the blockchain ledger only can be accessed by the DAS. So, there are no worries about the malicious miner in the blockchain network.
- *Wrong credential access.* In our proposed method, we used a password verification model $D = (h_3\,(h_2\,(R_{vm}\,||N_{vm}||\,E_i)))$ which is installed in the vehicle V_m, this model is used to verify the password correctness. If the entered password PsW_m is wrong, the verified data D and D' will not be same where $D' = h_3(h_2(K_i \oplus h_0\left(VID_m\left|\right|PsW_m'\left|\right|r_i\right)||h_0\left(VID_m\left|\right|PsW_m'\left|\right|r_i\right)))$. Therefore, our proposed model detects the unauthorized access to the authentication node [40–42].

8 Performance and Comparison Analysis

In this section to calculate the Comparison analysis of "security characteristics" and "communication cost" of the proposed method we have utilized the related studies [12,13], [16,17].

8.1 Security Comparison

In Tab. 2, we presented the security characteristics comparison of our proposed model with the related studies [12,13], [16,17]. By referring to Tab. 2, the existing schemes [12,13], [16,17] are endured various security attacks. Same time the related methods cannot provide authentication and anonymity in various cases. The proposed model for distributed authentication method prevents various security attacks and provides a revocability feature for lost vehicles.

Table 2: Comparison of security characteristics

Features	Li et al. [12]	Dua et al. [13]	Vasudev et al. [16]	Yu et al. [17]	Ours
SPF1	✓	✗	✗	✓	✓
SPF2	✓	✗	✓	✓	✓
SPF3	✓	✓	✗	✓	✓
SPF4	✓	✓	✗	✗	✓
SPF5	✗	✗	✓	✓	✓
SPF6	✗	✗	✗	✗	✓
SPF7	✗	✓	✗	✗	✓
SPF8	✗	✗	✗	✗	✓
SPF9	✗	✓	✗	✓	✓
SPF10	✗	✗	✗	✗	✓

Note: SPF$_1$-“Impersonation attack”, SPF$_2$-“Repeat attack/Reply attack”, SPF$_3$-“Man-in-Middle Attack”, SPF$_4$–“Authentication”, SPF$_5$–“User Anonymity”, SPF$_6$–“DoS attack”, SPF$_7$–“Perfect Forward Secrecy”, SFT$_8$–“Server spoofing”, SPF$_9$-“Mathematical analysis”, SPF$_{10}$-“Revocability”.

8.2 Storage Costs

We analyzed the storage costs of the proposed system with existing schemes [12,13], [16,17] According to [11], we estimate that the bit-lengths of the timestamp (L_T), random number/identity (L_{ID}), symmetric encryption/decryption ($L_{SD/SE}$), asymmetric encryption/decryption ($L_{AD/AE}$), signature (L_s) and hash function (L_h) are 8 bytes, 10 bytes, 16 bytes, 128 bytes, 192 bytes, and 32 bytes, respectively.

8.3 Computation Costs

We compared the computation cost of our proposed framework with the related works [12,13], [16,17] during the authentication. We estimated the following parameter values based on the Vasudev et al. [16] analysis method. T_{AE}, T_{AD}, T_{SE}, T_{SD}, T_s and T_h represents asymmetric decryption, asymmetric encryption, asymmetric decryption, asymmetric encryption, signing operation and hash function, respectively. Based on Vasudev et al. [16], we have represented the value of computations for various methods of cryptography operation in Tab. 2. we eliminated the computational values of XOR operation because compared to other cryptography operations, the XOR operation requires significantly computation time.

The computation time of the various cryptography operation in Tab. 3 is calculated based on the following desktop configuration, “Windows 10. Professional with an Intel (R) Core (TM) CPU i5–7200U, 8.1GB memory, @2.50 GHz” [16].

Table 3: Computation time for different cryptography operations [16]

Operations	Computation Costs
T_{AE}	4.406 ms
T_{AD}	7.761 ms

(Continued)

Table 3: Continued

Operations	Computation Costs
T_{SE}	7.761 ms
T_{SD}	0.001 ms
T_s	24.835 ms
T_{MAC}	0.014 ms
T_h	0.002 ms

The total computation cost of the related works and our proposed model are compared in Tab. 4. The total computation costs of the proposed framework and Vasudev et al.*’s* scheme [16] are 10.821 ms and 7.774 ms. Even though Vasudev et al.’s scheme has a minimum computation cost, many attacks still affect it, as demonstrated by Yu et al. [17] So, compared to that method, our proposed model has a better computation cost with strong security.

Table 4: Comparison of computation cost

Scheme	Computation cost	Total cost
Li et al. [12]	T_s	24.835 ms
Dua et al. [13]	$3T_{SE} + 12T_h$	23.283 ms
Vasudev et al. [16]	$6T_h + T_{SE} + T_{SD}$	7.774 ms
Yu et al. [17]	$5T_h + 2T_{SE}$	15.532 ms
Ours	$3T_{SD} + T_{MAC} + 3T_h + T_{SE}$	10.821 ms

8.4 Communication Costs

We have calculated the communication cost of the proposed framework with the related studies [12,13], [16,17]. To calculate a convincing comparison, we assumed that the bit length of timestamp, the block size of symmetric encryption, the block size of symmetric decryption, hash output, identity, the number of blocks, random number, and signature are 32 bits, 128 bits, 128 bits, 32 bits, 180 bits, 32 bits, 320 bits respectively. The bit length of the elliptic curve for digital signature is 160 bits, and the exponentiation is 1024 bits. The communication efficiency comparison is discussed in Tab. 5. [43,44].

Table 5: Comparison of communication cost

Scheme	Communication cost	Total cost
Li et al. [12]	$L_t + 2L_{ID} + L_s$	1760 bits
Dua et al. [13]	$3L_h + 4L_{IT} + L_s$	2144 bits
Vasudev et al. [16]	$4L_h + 2L_T + L_{SE}$	1024 bits
Yu et al. [17]	$5L_h + 2L_T$	1408 bits
Ours	$2L_S + 2L_H + L_{ID}$	1128 bits

In the proposed method, the initial message $\{T,\ U,\ CX\}$ needs $(320+32+180+32+32+32)=628$ bits and the reply message $\{D,\ W\}$ needs $(180+320)=500$ bits; by adding these two values, the total needed bits for the authentication phase are 1128 bits. By using the same bit length, the other related studies [12,13], [16,17]. also calculated as shown in Tab. 2. The analysis result and Fig. 5. show that our proposed model has the second lowest communication cost compared to other related schemes.

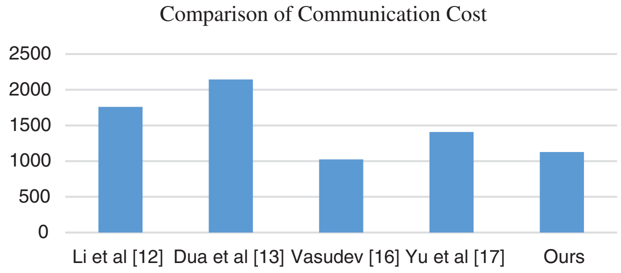


Figure 5: Graph for comparison of communication cost

Vasudev et al. [16] has the lowest communication cost, but it is affected by many attacks as demonstrated by Yu et al. [17]. In the security and communication cost wise the proposed model has efficient results, and it has the potential to implement in real time.

9 Conclusion

In this research, we proposed a distributed authentication mechanism for IoV environment based on blockchain technology with an ouroboros algorithm that protects the system from various security attacks such as man-in-middle attack, DDoS attack, server spoofing attack and provide a solution for single-point failure, forward secrecy, revocability, etc. The formal and informal security analysis proves that our proposed method is secure the random oracle model. The performance analysis demonstrates that the proposed model has high communication efficiency, which will be suitable for real time IoV environment.

Acknowledgement: This work was supported in part by the Ministry of Science and Technology, Taiwan, through grant MOST 110–2622-E-468–002 and 110–2218-E-468–001-MBK. The authors also gratefully acknowledge the helpful comments and suggestions of the Editor and anonymous reviewers, which have improved the presentation of this paper.

Funding Statement: This work was supported by the Ministry of Science and Technology of Taiwan, R.O.C., under Grant MOST 110–2622-E-468–002 and 110–2218-E-468–001-MBK.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] H. Stipp, "Number of IoT devices 2015–2025," *Statista*, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (accessed Apr. 08, 2022).

[2] A. Hbaieb, S. Ayed and L. Chaari, "A survey of trust management is the internet of vehicles," *Computer Networks: The International Journal of Computer and Telecommunications Networking*, vol. 203, no. C, pp. 108558, 2022.

[3] H. Chiroma, S. M. Abdulhamid, I. A. T. Hashem, K. S. Adewole, A. E. Ezugwu *et al.,* "Deep learning-based big data analytics for internet of vehicles: Taxonomy, challenges, and research directions," *Mathematical Problems in Engineering*, vol. 202, no. 12, pp. 20, 2021.

[4] J. Wang, K. Zhu and E. Hossain, "Green internet of vehicles (IOV) in the 6 G era: Toward sustainable vehicular communications and networking," *IEEE Transactions on Green Communications and Networking*, vol. 6, no. 1, pp. 391–423, 2022.

[5] S. Abbas, M. A. Talib, A. Ahmed, F. Khan, S. Ahmad *et al.,* "Blockchain-based authentication in internet of vehicles: A survey," *Sensors*, vol. 21, no. 23, pp. 23, 2021.

[6] Y. Sun, L. Wu, S. Wu, S. Li, T. Zhang *et al.,* "Security and privacy in the internet of vehicles," in *Int. Conf. on Identification, Information, and Knowledge in the Internet of Things (IIKI)*, Beijing, China, vol.21, no.5, pp. 116–121, 2015.

[7] M. K. Priyan and G. U. Devi, "A survey on internet of vehicles: Applications, technologies, challenges and opportunities," *International Journal of Advanced Intelligence Paradigms*, vol. 12, no. 1/2, pp. 98, 2019.

[8] J. Lauinger, "Identity management in internet of vehicles based on distributed ledger technology," *NIoVe*, 2021. [Online]. Available: https://www.niove.eu/index.php/blogs/identity-management-in-internet-of-vehicles-based-on-distributed-ledger-technology (accessed Mar. 19, 2022).

[9] A. Monrat, K. Andersson and O. Schelén, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 1, no. 1, pp. 99, 2019.

[10] L. Mendiboure, M. A. Chalouf and F. Krief, "Survey on blockchain-based applications in internet of vehicles," *Computers & Electrical Engineering*, vol. 84, no. 1, pp. 106646, 2020.

[11] N. Sharma, N. Chauhan, N. Chand and L. K. Awasthi, "Secure authentication and session key management scheme for internet of vehicles," *Transactions on Emerging Telecommunications Technologies*, vol. 6, no. 1, pp. 4451, 2022.

[12] J. Li, H. Lu and M. Guizani, "ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for vanets," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 938–948, 2015.

[13] A. Dua, N. Kumar, A. K. Das and W. Susilo, "Secure message communication protocol among vehicles in smart city," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 4359–4373, 2018.

[14] B. Ying and A. Nayak, "Anonymous and lightweight authentication for secure vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 12, pp. 10626–10636, 2017.

[15] C. -M. Chen, B. Xiang, Y. Liu and K. -H. Wang, "A secure authentication protocol for internet of vehicles," *IEEE Access: Security and Privacy for Cloud and IOT*, vol. 7, no. 1, pp. 12047–12057, 2019.

[16] H. Vasudev, D. Das and A. V. Vasilakos, "Secure message propagation protocols for IoVs communication components," *Computers and Electrical Engineering*, vol. 82, no. 1, pp. 106555, 2020.

[17] S. Yu, J. Lee, K. Park, A. K. Das and Y. Park, "IoV-SMAP: Secure and efficient message authentication protocol for IOV in smart city environment," *IEEE Access: Towards Smart Cities with IOT Based on Crowdsensing*, vol. 8, no. 1, pp. 167875–167886, 2020.

[18] D. Johnson, A. Menezes and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *International Journal of Information Security*, vol. 1, no. 1, pp. 36–63, 2001.

[19] O. Mir, M. Roland and R. Mayrhofer, "Decentralized, privacy-preserving, single sign-on," *Security and Communication Networks*, vol. 2022, no. 8, pp. 983–995, 2022.

[20] A. Tewari and B. B. Gupta, "Secure timestamp-based mutual authentication protocol for IOT devices using RFID tags," *International Journal on Semantic Web and Information Systems*, vol. 16, no. 3, pp. 20–34, 2020.

[21] J. Wang, W. Chen, Y. Ren, O. Alfarraj and L. Wang, "Blockchain based data storage mechanism in cyber physical system," *Journal of Internet Technology*, vol. 21, no. 6, pp. 1681–1689, 2020.

[22] A. Kiayias, A. Russell, B. David and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," *Advances in Cryptology-CRYPTO*, vol. 1, no. 2, pp. 357–388, 2017.

[23] J. Yu, G. Wang, Y. Mu and W. Gao, "An efficient generic framework for three-factor authentication with provably secure instantiation," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 12, pp. 2302–2313, 2014.

[24] S. Goldwasser, S. Micali and R. L. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 281–308, 1988.

[25] C. L. Stergiou, K. E. Psannis and B. B. Gupta, "IoT-Based big data secure management in the fog over a 6 g wireless network,". *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5164–5171, 2020.

[26] M. H. Lim, B. M. Goi and S. Lee, "An analysis of group key agreement schemes based on the bellare-rogaway model in multi-party setting," *KSII Transactions on Internet and Information Systems*, vol. 5, no. 1, pp. 822–839, Apr. 2011.

[27] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology*, vol. 13, no. 3, pp. 361–396, 2000.

[28] A. Armando, D. Basin, Y. Boichut and Y. Chevalier, "The AVISPA tool for the automated validation of internet security protocols and applications," *Lecture Notes in Computer Science*, vol. 3576, no. 1, pp. 135–165, 2005.

[29] G. Thomas, "SPAN: A security protocol animator for AVISPA," [Online]. Available: http://www.avispa-project.org. (Accessed May. 15, 2022).

[30] C. Adams and V. Tilborg, "Impersonation Attack," in *Encyclopedia of Cryptography and Security*, vol. 1. Boston, MA: Springer US, pp. 286–286, 2005.

[31] E. D. Knapp and J. T. Langill, "Chapter 7-Hacking industrial control systems," in *Industrial Network Security*, 2nd ed., vol. 1,. Boston: Syngress, pp. 171–207, 2015.

[32] M. Gregg, "Chapter 4-Layer 3: The network layer," in *Hack the Stack*, vol. 1. Burlington: Syngress, pp. 103–150, 2006.

[33] C. Adams, "Replay attack," in *Encyclopedia of Cryptography and Security*, vol. 4, Boston, MA: Springer US, pp. 1042–1042, 2011.

[34] J. Wang, B. Wei, J. Zhang, X. Yu and P. K. Sharma, "An optimized transaction verification method for trustworthy blockchain-enabled IIoT," *Ad Hoc Networks*, vol. 119, no. 1, pp. 102526, 2021.

[35] J. Y. Zhang, S. Q. Zhong, T. Wang, H. C. Chao and J. Wang, "Blockchain-based systems and applications: A survey," *Journal of Internet Technology*, vol. 21, no. 1, pp. 1–14, 2020.

[36] J. Zhang, S. Zhong, J. Wang, X. Yu and O. Alfarraj, "A storage optimization scheme for blockchain transaction databases," *Computer Systems Science and Engineering*, vol. 36, no. 3, pp. 521–535, 2021.

[37] Z. Xu, W. Liang, K. C. Li, J. Xu and H. Jin, "A Blockchain-based roadside unit-assisted authentication and key agreement protocol for internet of vehicles," *Journal of Parallel and Distributed Computing*, vol. 149, pp. 29–39, 2021.

[38] W. Sun, G. C. Zhang, X. R. Zhang, X. Zhang and N. N. Ge, "Fine-grained vehicle type classification using lightweight convolutional neural network with feature optimization and joint learning strategy," *Multimedia Tools and Applications*, vol. 80, no. 20, pp. 30803–30816, 2021.

[39] W. Sun, X. Chen, X. R. Zhang, G. Z. Dai, P. S. Chang *et al.,* "A multi-feature learning model with enhanced local attention for vehicle re-identification," *Computers, Materials & Continua*, vol. 69, no. 3, pp. 3549–3561, 2021.

[40] K. Alieyan, A. Almomani, M. Anbar, M. Alauthman, R. Abdullah *et al.,* "DNS Rule-based schema to botnet detection," *Enterprise Information Systems*, vol. 15, no. 4, pp. 545–564, 2021.

[41] I. Cvitić, D. Perakovic, B. B. Gupta and K. R. Choo, "Boosting-based DDOS detection in internet of things systems," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 1–1. 2021.

[42] A. Dahiya and B. B. Gupta, "A reputation score policy and Bayesian game theory based incentivized mechanism for DDoS attacks mitigation and cyber defense," *Future Generation Computer Systems*, vol. 117, no. 1, pp. 193–204, 2021.

[43] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in internet-of-things (IoTs) framework," *Future Generation Computer Systems*, vol. 108, no. 2, pp. 909–920, 2020.

[44] Z. Zhou and A. Gaurav, "A fine-grained access control and security approach for intelligent vehicular transport in 6 G communication system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 1, no. 3, pp. 23 2021.