IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

Cryptographic Solution Based Secure Elliptic Curve Cryptography Enabled Radio Frequency Identification Mutual Authentication Protocol for Internet of Vehicles

Surbhi Sharma[1], Baijnath Kaushik[1,*], Mohammad Khalid Imam Rahmani[2,*], Senior Member IEEE, Md Ezaz Ahmed[2]

[1]Department of Computer Science and Engineering, Shri Mata Vaishno Devi University, Katra, J&K, India
[2]College of Computing and Informatics, Saudi Electronic Universit, Riyadh, Saudi Arabia
[*]Corresponding author: Baijnath Kaushik (baijnath.kaushik@smvdu.ac.in), Mohammad Khalid Imam Rahmani (m.rahmani@seu.edu.sa).

ABSTRACT Internet of Vehicles (IoV) is one of the most active research disciplines in Intelligent Transportation Systems (ITS), intending to improve VANET (Vehicular-Ad-hoc Network) capabilities. The main objective of IoV is to enhance the safety of passengers by incorporating various advanced information and communication technologies thus, ease the driving experience of passengers and enhances traffic efficiency. IoV has numerous key technologies, and one of them is Radio-Frequency Identification Technology (RFID) which has a plethora of applications in IoV like automatic toll collection, intelligent parking, data dissemination, tracking the location of the vehicle, etc. which enhances the overall performance of IoV networks. Along with this, RFID devices are resource-constrained, thus security and privacy are a major concern and also IoV is a real-time sensitive network where security is of utmost importance. Keeping in mind the security perspective, the concept of Elliptic-Curve Cryptography (ECC) is taken into consideration. So, in this paper, we have proposed a Cryptographic solution-based secure ECC-enabled RFID mutual authentication protocol for IoV. The proposed protocol is comprised of three phases: Setup Phase, Tag Authentication Phase, and Server Authentication Phase. Security evaluation of the proposed protocol is performed by taking into consideration the analysis of security requirements as well as security attacks. Also, the simulation of the proposed protocol is done using the AVISPA tool and the results indicate that the proposed protocol is safe against various malevolent attacks. Performance evaluation of the proposed protocol is computed based on parameters i.e. storage requirements, communication cost, and computational cost. Results indicate that the proposed protocol contributes to high performance and security and has low computational cost than other existing authentication protocols. A novel Blockchain-based security framework for RFID-enabled IoV has also been proposed to further enhance the security of the IoV network.

INDEX TERMS Authentication, Attacks, ECC, IoV, Protocol, RFID, Security

I. INTRODUCTION

The concept of the Internet of Vehicles (IoV) has boosted the automotive industry due to the incorporation of smartness by merging the technologies like IoT (Internet of Things) and VANETs (Vehicular-Ad-hoc Network)[6]. It has led to the vision of smart transportation and smart cities as it gives beforehand information regarding any casualties like traffic accidents or other life-threatening scenarios. Due to this, cities will be properly organized so the quality of life will be improved and casualties will also be minimized[7].

One of the core technologies of IoV is RFID technology as it ensures road safety and efficient traffic management which is the main objective of IoV networks. RFID is a widely adopted technology in IoV networks due to a plethora of applications[8]:

i. Automatic toll collection.
ii. Numerous vehicles moving at high speeds are identified.
iii. Tracking the location of the vehicle.
iv. Intelligent parking system.
v. Distant vehicle identification.
vi. Traffic-flow monitoring
vii. Data dissemination between vehicles.

RFID is an automatic identification technology that relies on wireless communication using radio waves for data

transmission[9, 10]. An RFID system is composed of three primary components[11, 12] as shown in Fig.1. They are mentioned below:

i. Tags: It consists of a small microchip with limited data storage and limited logic functionalities. RFID tags are fixed on objects to verify the uniqueness of an object.
ii. Readers: RFID readers transmit a radio signal to interrogate the tag.
iii. Electronic database (Server): Databases stores tag related information

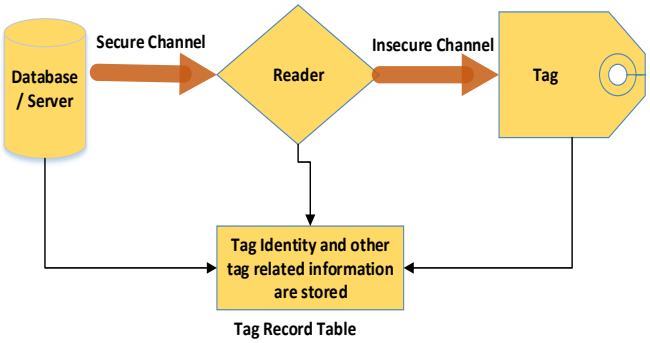

Fig 1. Primary Components of RFID System [1]

Tags are further classified into two categories based on powering techniques[13].

Active Tags: Such tags have their transmitter and power source. Active tags are large, expensive and have a longer read range, and thus are suitable for tracking of large-objects.

Passive Tags: The electromagnetic energy sent from the RFID reader powers these tags, and have no internal power source. These tags have a shorter read range, small in size, less expensive, and more flexible than active tags. So, passive tags are suitable for low-cost items.

As RFID technology relies on wireless communication, so it is vulnerable to various security threats. Compromising the security of RFID impacts the security of the IoV system which may lead to hazardous results. IoV is a real-time dynamic network in which security and privacy are a major concern, so RFID based IoV system must be secure from all security attacks. Various authentication schemes are suggested by researchers to secure the RFID-based systems but all have limitations as some focus on preventing the security attacks while few focus on computational resources of RFID tags.

A. MOTIVATION

RFID devices are resource-constrained thus, it is essential to maintain a paradox between security and efficiency in the design of authentication protocol for RFID-based vehicular systems. RFID tags have less computational power and low memory due to limited logic gates. Therefore, few factors are required to be considered in the design of RFID-based authentication protocol for IoV: Authentication cost must be taken into consideration for practical implementation, Number of logic gates determines the Tag's computing overhead where tag have 5000-1000 logic gates of which only 2000-3000 can be used for encryption and decryption[14].

So, RFID authentication schemes for IoV networks should be able to authenticate fast while also protecting the privacy of users.

Keeping in view the above factors, we have employed the concept of Elliptic-Curve Cryptography (ECC) which is a popular light-weight public-key cryptographic algorithm due to its smaller key size and offers high security which is perfect for resource-constrained devices. In this paper, we have designed a cryptographic-based secure ECC-enabled RFID authentication protocol for the Internet of Vehicles which offers strong security.

B. MAIN CONTRIBUTIONS OF THIS ARTICLE

The main contributions of this article are mentioned below:

1) In this paper, the applicability of RFID technology in IoV is explored to enhance its performance.
2) Proposed a Cryptographic-solution-based secure ECC-enabled RFID authentication protocol for Internet of Vehicles.
3) Security analysis of the proposed protocol is evaluated based on security requirements and its ability to mitigate the security attacks in the IoV system.
4) Formal verification of proposed is done using simulation software: AVISPA
5) Performance analysis of the proposed protocol is done based on parameters i.e. security requirements, communication cost, and computational cost and results indicate that our proposed protocol is better thus provides strong security and enhances the effectiveness of IoV networks.
6) Proposed a Blockchain-based novel security framework for RFID-enabled IoV.

C. PAPER ORGANIZATION

The workflow of the whole paper is as follows: Section II discusses the related work in which existing authentication protocols are discussed. Section III elaborates the background of ECC and its important functionalities where all the basic features of ECC are discussed. Section IV explains the proposed cryptographic-solution-based ECC-enabled secure RFID authentication protocol for the Internet of Vehicles. Section V mentions the security evaluation of the proposed protocol in which analysis of different security requirements and security attacks are done. Section VI is the simulation analysis of the proposed protocol using AVISPA which indicates that the protocol is safe using different backends. Section VII discusses the performance analysis of the proposed protocol in terms of three parameters- Storage Requirements, Communication Cost, and Computational Cost and results are compared with the existing 4 authentication protocols. Section VIII proposes a Blockchain-based novel security framework for RFID-enabled IoV. Section IX is the conclusion section which summarizes the whole paper.

II. RELATED WORK

RFID devices are resource-constrained as they have low memory and low computational power due to limited logic gates and thus the security and privacy are a major concern[9].

Numerous RFID authentication protocols are suggested by researchers keeping in view the computational and operational cost of tags.

Authors in [15] have classified the RFID authentication protocols into 4 major classifications based on the operational and computational cost of tags:

Class-I: It is also known as 'full-fledged class'. This category relies on Classical cryptography-based techniques, Cryptographic One-way function, etc. It has a large computational overhead.

Class-II: This category of the class is also known as 'Simple'. It supports Random number generation and Hash-functions etc.

Class-III: It is also known as 'lightweight'. This category of class supports simple operations like checksum, pseudorandom number generation, etc. It doesn't support hash functions.

Class-IV: This category is also known as 'ultralightweight'. It relies on simple bit-wise operations like OR, AND, XOR, rotation, permutation, etc. on tags. It has the lowest overhead in terms of computation and storage. This category of authentication protocol requires only 300 logic gates for implementation so these schemes are quite efficient.

Minimalist Cryptography-based authentication protocol is proposed by authors in [16] for low-cost RFID tags. It is independent of traditional cryptographic primitives. It uses the concept of multiple pseudonyms and relies on the rotation of a tag for authentication. It also takes into account one-time pads across multiple tag-verifier sessions to retain the secrecy.

Authors in [17] proposed an authentication protocol for low-cost RFID tags known as LMAP. Tag identification, Mutual Authentication, Index Pseudonym Updating, and Key Updating are the different steps of the proposed protocol.
It relies on lightweight operations i.e. Addition mod 2^m (+), Bitwise AND (/\). Bitwise XOR ($\oplus$) and Bitwise OR (\/). It takes into account the concept of index pseudonyms. It ensures Mutual Authentication, Data Integrity, Data Confidentiality, Tag Anonymity, and security against various security attacks like replay attacks, man-in-the-middle attacks, etc. But the proposed LMAP protocol is prone to full-disclosure attacks and desynchronization attacks.

Authors in [18] proposed a hash-based RFID Authentication protocol. It ensures security against various attacks like replay attacks, impersonation, and eavesdropping, etc. It is suitable for scenarios where the computational load is heavy and the number of tags is large. Authors in [19] have done the cryptanalysis of the paper proposed by authors in [18] and claim that the proposed protocol is prone to untraceability attacks and tag information leakage.

Low-Cost Location Privacy Authentication protocol for RFID is proposed by authors in [20] to achieve high efficiency with minimal cost. It consists of 3 phases-Initialization Phase, Authentication Phase, and Updation Phase. It uses a hash function that is embedded in the tag and the same hash function is also used on the server-side. It ensures that the proposed scheme is feasible, resists replay attacks, and achieves forward secrecy.

A mutual authentication protocol for RFID is designed by authors in [21] to enhance the security of RFID. The initialization Phase and Authentication Phase are the two phases of the proposed protocol. It relies on the concept of Pseudo-random numbers and Cyclic-Redundancy Check (CRC). It ensures forwards secrecy, anonymity, privacy and also resists DoS attacks. Authors in [22] have done the cryptanalysis of the authentication protocol proposed by authors in [21]. They have pointed that the proposed protocol has various security failures i.e. prone to identity impersonation attacks (both tag and backend database), auto-desynchronization attacks, non-forward security tracking, and failed unequivocal identification.

Authentication and Privacy are the core requirements in RFID security and among all the authentication protocols, ECC-based RFID authentication protocols are assumed to be more suitable because ECC provides high security even with smaller key size and perform efficient computations. Few prominent ECC-based RFID authentication protocols are discussed below:

A secure ECC-based RFID authentication protocol is proposed by authors in [3] in which ID-verifier transfer protocol is also integrated. The setup Phase and Authentication Phase are the two phases in the proposed protocol. It satisfies all the security goals like Mutual authentication, Anonymity, Forward security, etc., and resists various security attacks like Cloning attacks, Replay attacks, DoS attacks, etc. Although, the proposed scheme is prone to impersonation attacks.

Authors in [4] designed a lightweight ECC-based RFID authentication protocol to overcome the limitations in the existing schemes. It makes use of simple and lightweight operations like Addition mod 2^m, Elliptic Scalar Multiplication, and Bitwise XOR, etc. It shows all strong security properties and its performance is measured based on parameters i.e. Storage Cost, Computational Cost, Communication Cost. Results indicate that the proposed scheme is quite suitable for practical applications. However, it is vulnerable to active tracking attacks.

A new ECC-based RFID authentication protocol for E-Health systems is proposed by authors in [2] to enhance their computational performance. Authentication and Setup are the two phases of the proposed protocol. Hash operation, Bitwise XOR, Elliptic Scalar Multiplication, Addition mod 2^m, etc. are the prominently used lightweight operations used in the proposed protocol. The proposed protocol satisfies all security requirements and is secure against all security threats. Results indicate that it outperforms the existing protocols in terms of less computational cost, less communication cost, and less storage cost.

Efficient and Lightweight ECC-based Authentication

protocol for RFID systems is designed by authors in [23]. It is classified into 3 phases- Initial Setup Phase, Server Authentication Phase, and Tag Authentication Phase. The protocol's main distinguishing feature is that it is entirely dependent on ECC operations, with only two message exchanges between the tag and the reader. The results show that the technique is feasible enough to be deployed in RFID-enabled scenarios to enhance safety and reliability.

Authors in [24] designed a secure ECC-based RFID mutual authentication protocol to eliminate the current RFID vulnerabilities. The initialization Phase and Authentication Phase are the two main stages in the proposed protocol. It relies on the two core concepts of the ECC algorithm- ECDLP (Elliptic Curve Discrete Logarithmic Problem) and ECFP (Elliptic Curve Factorization Problem). A temporary secret key is used to encrypt the transmitted messages and is generated using Elliptic-Curve Diffie Hellman (ECDH) agreement protocol. The proposed protocol relies on less number of operations and results indicate that it outperforms in terms of time complexity as compared to other similar protocols and also provides strong security properties.

RFID authentication protocol based on ECC is presented by authors in [5]. The proposed protocol consists of 3 phases- Set up Phase, Authentication Phase, and Updation Phase. It includes simple lightweight operations like Bitwise XOR, Elliptic Scalar Multiplications. It satisfies all the security requirements and resists different security attacks. Also, the results indicate that the proposed protocol outperforms the other existing protocols as it has a higher security level and less computational overhead.

III. BACKGROUND OF ELLIPTIC CURVE RYPTOGRAPHY (ECC) AND ITS IMPORTANT FUNCTIONALITIES

Our proposed protocol relies on the concepts of ECC. So, in this section, ECC is discussed in brief regarding its security features and other functionalities.

Elliptic Curve Cryptography was introduced in 1985 by Neal Koblitz and Victor S. Miller[25]. ECC is an asymmetric key cryptosystem based on the concept of elliptic curves.

A set of points that satisfy a specific mathematical equation is known as an elliptic curve, and it is represented by the generic equation given below[26]:

$$y^2 = x^3 + ax + b \quad (1)$$

where a and b are constants.

- **Trapdoor Function-** Each public-key cryptographic algorithm has its trapdoor function. A trapdoor function is a one-way function that difficult to compute in the reverse direction and is simple to compute in one direction.

- **Elliptic- Curve Discrete Logarithmic Problem (ECDLP):** It is one of the hard problems in the foundation of ECC. Let E_p (a,b) is an Elliptic curve. And consider the equation $Q = kP$ where P, Q are the two points that lie on the Elliptic curve and k<n. ECDLP illustrates that if k and P are known, then it is easy to compute the value of Q. But if the values of Q and P are known, then it's extremely difficult to calculate the value of k[24]. It is a one-way function i.e. Trapdoor function of ECC.

- **Elliptic Scalar Multiplication:** New point on the curve can be computed by multiplying a point on the curve by a number. If P is a point on the elliptic curve then the value of another point, Q can be computed by $Q = kP$ =P+P+……P (k times).

A. UNIQUE FEATURES OF the ECC

The unique features of ECC that make it different from other public cryptosystems are mentioned below:

1) The most distinguishing feature of ECC is that it provides the same security with a 160-bit key as the RSA algorithm provides with a 1024-bit key size. Table 1 shows the comparison of key sizes of RSA and ECC with equivalent security[27].

2) It is the most popular algorithm among public key cryptosystems due to the creation of smaller, faster, and efficient cryptographic keys[28].

3) ECC is highly suited to devices with limited resources, like mobile phones, RFID devices, and cryptocurrencies, etc. due to its small key size.

4) ECC offers a better tradeoff- High security with short and fast keys.

5) Due to its lightweight nature, ECC is widely used in various applications. E.g., Bitcoin uses ECC, For safe web browsing via SSL/TLS, this is the preferred form of authentication.

IV. PROPOSED CRYPTOGRAPHIC SOLUTION BASED SECURE ECC -ENABLED RFID MUTUAL AUTHENTICATION PROTOCOL FOR INTERNET OF VEHICLES (IoV)

Table 1.Comparison of Key Sizes of ECC and RSA[27]

Key Size of ECC in bits	Key Size of RSA in bits
112	512
160	1024
224	2048
256	3072
384	7680
512	15360

In this section, the proposed ECC-based RFID mutual authentication protocol for IoV is discussed. RFID technology plays a key role in the IoV environment as it ensures road safety and efficient traffic management due to numerous applications i.e., automatic toll collection, identification of high-speed movement of multiple vehicles, tracking the location of vehicle, intelligent parking system, etc.[8]. Due to these applications, RFID based authentication protocol for IoV is proposed to enhance the efficiency and overall performance of IoV networks.

RFID systems consist of three entities- Readers, Tags, and Servers where the reader acts as an intermediate agent for

information exchange between server and tag. So, the proposed protocol takes into consideration only two entities i.e., Servers and Tags for the implementation purpose. The communication between Server and Reader is assumed to be secure while communication between Tag and Reader is assumed to be insecure.

A. DIFFERENT PHASES OF THE PROPOSED PROTOCOL

Proposed protocol consists of three phases:

1) Phase-1: Set up Phase
2) Phase 2: Tag Authentication Phase
3) Phase 3: Server Authentication Phase

The proposed protocol relies on the basic concepts of ECC for a public and private key-pair generation. Simple lightweight operations of ECC i.e., ECC scalar multiplication, point addition, hash operation are used in the proposed protocol. The different notations used in the proposed protocol are mentioned in Table 2.

1) PHASE-I: SET UP PHASE

It is one of the important phases of the proposed protocol. Following are the different steps involved in this phase:

- *Step-1*: RFID Tags and Servers are equipped with public domain parameters of the Elliptic curve i.e. (G, a, b, n, q) as mentioned in Table 2.
  Step 2: Along with this, public-private key pair calculation is also done in this phase using ECC-based operations. The server chooses a random number $Pr_S \in Z_n^*$ as its private key. Then public key of the Server P_S is computed by ECC scalar multiplication of computed private key, Pr_S and generator point, G thus, Public key of Server, $P_S = Pr_S.G$
- *Step 3*: A random number, $Pr_T \in Z_n^*$ is chosen as the Private key of Tag. Then the public key of Tag, P_T is computed by scalar multiplication of computed private key, Pr_T and generator point, G thus, Public-key of Tag, $P_T = Pr_T.G$.

At the end of this phase, Server and Tag are equipped with the following entities:

Server:

- Elliptic curve parameters - (G, a, b, n, q)
- Its Private-Public key pair- (Pr_S , P_S)
- Public and Private-key of Tag- (Pr_T , P_T).

RFID Tag:

- Elliptic curve parameters - (G, a, b, n, q)
- Its Private-Public key pair - (Pr_T , P_T)
- Public-key of Server- (P_S)

2) PHASE-II: TAG AUTHENTICATION PHASE

This is the most crucial step in the mutual authentication of Tag and Server. During this phase, the Server authenticates the Tag, and if the tag seems to be legitimate then, only the data communication is continued otherwise the connection is terminated.

Table 2. List of Notations

Notations	Description
$F(q)$	Size of finite field, $F(q)$ is represented by q
E	Elliptic curve is defined by the equation, $y^2 = x^3 + ax + b$ over finite field, $F(q)$
n	Elliptic curve order
G	Elliptic curve, E having Generator point with order n.
a, b	Parameters of Elliptic Curve,E
H(.)	One-way hash function
P_S	Server's Public-key
Pr_S	Server's Private-key
P_T	Tag's Public-key
Pr_T	Tag's Private-key
s_1	Server generates random number
t_1	Tag generates random number.

Different steps involved in the Tag Authentication Phase are elaborated below and is shown in Fig. 2.

- *Step-1:* A random number is generated by the server, $s_1 \in Z_n^*$ and then it computes S_1 using ECC scalar multiplication of s_1 and G, thus
$$S_1 = s_1.G \quad (2)$$
- *Step-2:* Server then sends the message $\{S_1\}$ to Tag.
- *Step-3:* Tag chooses a random number, $t_1 \in Z_n^*$ and then it computes T_1 using ECC scalar multiplication of t_1 and G, thus
$$T_1 = t_1.G \quad (3)$$
- *Step-4:* After this, Tag computes its two secret keys i.e. TP_1 and TP_2 using ECC scalar multiplication. Value of TP_1 is calculated using scalar multiplication of its random value, t_1 and S_1 thus,
$$TP_1 = t_1.S_1 \quad (4)$$
and Value of TP_2 is calculated using scalar multiplication of its random value, t_1 and public-key of Server, P_S thus,
$$TP_2 = t_1 . P_S. \quad (5)$$
- *Step-5:* Finally the Tag computes the value of A_T token which involves one-way Hash-function and Point Addition was authenticated in the last phase will now authenticate the Server as mutual authentication is a must before actual data operations i.e.,
$$A_T = P_T + H(TP_1) + TP_2 . \quad (6)$$

The steps of the Server-Authentication Phase are mentioned

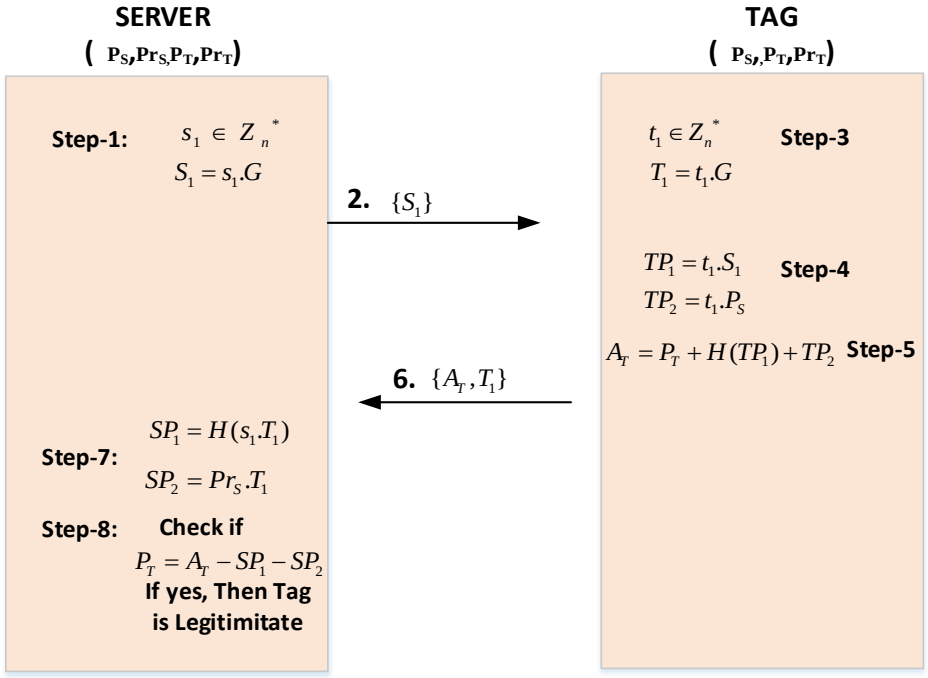

Fig 2. Tag Authentication Phase

- *Step*-6: Tag then sends the value of $\{A_T, T_1\}$ to the server for authentication purpose.
- *Step-7:* In this step, Server performs different operations to authenticate the Tag. Initially, Server computes the value of SP_1 and SP_2 i.e.,

$$SP_1 = H(s_1.T_1), \quad (7)$$

$$SP_2 = Pr_S.T_1. \quad (8)$$

- *Step-8:*Then, the Server uses these computed values to retrieve the Tag value P_T using the following equation:

$$P_T = A_T - SP_1 - SP_2 \quad (9)$$

Then, the server searches the computed value of P_T in the database. If the same value is found, then the server confirms that the tag is legitimate. In case of successful tag authentication, the next phase will be continued by the server i.e., Server Authentication Phase otherwise the connection is terminated due to an illegitimate tag.

Algorithm 1 shows in detail the above steps of the Tag Authentication Phase.

3) PHASE-II: SERVER AUTHENTICATION PHASE

This phase of the proposed protocol proceeds after the Tag Authentication Phase. In this phase, the legitimate tag which was authenticated in the last phase will now authenticate the Server as mutual authentication is a must before actual data transmission takes place.

below and is shown in Fig. 3:

- *Step-1*: In this step, the Server computes the value of A_S token using a one-way hash function, ECC scalar multiplications, and Point addition operation. Thus, the value of

$$A_S = Pr_T.H(S_1 + T_1) + s_1.P_T \quad (10)$$

- *Step-2:* Server sends the computed value of $\{A_S\}$ to the desired Tag.
- *Step-3:* Tag computes the value of A_S' token based on previously calculated values i.e.

$$A_S' = P_T.H(t_1 + s_1) + Pr_T.S_1 \quad (11)$$

- *Step-4:* After calculating the value of A_S', the value of receiving $\{A_S\}$ and $\{A_S'\}$ are checked. If values of $\{A_S\}$ = $\{A_S'\}$ are equal, then it indicates that the Server is authenticated else the Server is illegitimate and the connection is terminated.

Algorithm 2 shows in detail the above-mentioned steps of Server Authentication Phase.

Algorithm 1: Tag Authentication Algorithm

Input: Elliptic curve parameters-(G,a,b,n,q), Public and Private-key pair of Tag:(Pr_T , P_T), Random numbers: (s_1 , t_1), Hash function, H(.), ECC Scalar Multiplication (.), Point Addition (+).
Output: Successful Tag Authentication
Assumptions: Server have its own private-public key pair as well as Tag's public-private key pair. Also, Tag has its own private-public-key and Server's public key.

1. A random number is generated by Server, $s_1 \in Z_n^*$
2. Server then calculates the value of $S_1 = s_1.G$
3. Server then sends the computed value of $\{S_1\}$ to Tag.
4. A random number is chosen by Tag, $t_1 \in Z_n^*$
5. Tag calculates the value of T_1 using the equation-$T_1 = t_1.G$
6. Tag computes its secret-key, TP_1 where, $TP_1 = t_1.S_1$
7. Tag computes its other secret-key, TP_2 where, $TP_2 = t_1.P_S$
8. Finally the Tag computes the value of A_T token using the equation: $A_T = P_T + H(TP_1) + TP_2$
9. Tag then sends the value of $\{A_T, T_1\}$ to the server for authentication purpose.
10. Server computes the value of $SP_1 = H(s_1.T_1)$
11. Server computes the value of $SP_2 = Pr_S.T_1$.
12. **if** ($P_T = A_T - SP_1 - SP_2$) computed by Server**, then**
13. Tag Successfully Authenticated by Server
14. **else**
15. Terminate the connection
16. **end if**

V. SECURITY EVALUATION OF PROPOSED PROTOCOL

In this section, the security evaluation of the proposed protocol is discussed in two aspects- the ability to mitigate the security attacks in the IoV system and analysis of security requirements.

The strength of our proposed protocol is discussed in terms of these security requirements i.e., Mutual Authentication, Anonymity, Availability, Scalability, and Forward Secrecy.

Also, our proposed protocol resists the prominent security attacks that exists in the IoV and RFID system: Replay attack, DoS attack , Tag Masquerading Attack, Server Spoofing Attack and Cloning Attack.

A. ANALYSIS OF SECURITY REQUIREMENTS

Different security requirements satisfied by the proposed protocol is discussed in this section.

In order to sustain the security requirements, following are the few assumptions:

i) All the random numbers generated by Tag and Server i.e. t_1 and s_1 are fresh in every session.

ii) Server's private key, Pr_S is unknown to except the Server.

iii) Tag's private-public key pair i.e. (Pr_T , P_T) are unknown to everyone except the Tag and Reader.

iv) Server's public key i.e. P_S and G being common tag.

MUTUAL AUTHENTICATION BETWEEN SERVER AND TAG

Algorithm 2: Server Authentication Algorithm

Input: Elliptic curve parameters-(G,a,b,n,q), Public and Private-key pair of Server: (P_S , Pr_S), Public and Private- key pair of Tag:(Pr_T , P_T), Random numbers: (s_1 , t_1), Hash function, H(.), ECC Scalar Multiplication (.), Point Addition (+).
Output: Successful Server Authentication
Assumptions: Server has successfully authenticated the Tag.

1. Server computes the value of A_S using the equation:
   $A_S = Pr_T.H(S_1 + T_1) + s_1.P_T$
2. Server then sends the value of $\{A_S\}$ to the Tag for authentication purpose.
3. Tag computes the value of A_S' using the equation:
   $A_S' = P_T.H(t_1 + s_1) + Pr_T.S_1$
4. **if** ($A_S = A_S'$)**, then**
5. Server is successfully Authenticated by Tag
6. **else**
7. Terminate the connection
8. **end if**

Mutual authentication between two entities is one of the important security requirements in authentication protocols.
In Step-6 of Tag Authentication Phase, Tag sends $\{A_T, T_1\}$ to Server for Authentication where $A_T = P_T + H(TP_1) + TP_2$. The server on receiving these values will decrypt the value of P_T using its secret keys i.e. $P_T = A_T - SP_1 - SP_2$ .Then, the server will check the value of P_T in the database, if both the values are equal then the tag will be authenticated by the server. In case, Adversary (A) introduces itself as a legitimate tag then, it should produce the correct value of A_T where $A_T = P_T + H(TP_1) + TP_2$ which is not possible without the correct value of P_T which is known only to server and tag.

On the other hand, for Server authentication, the Server will calculate the value of $A_S = Pr_T.H(S_1 + T_1) + s_1.P_T$ and send the value of $\{A_S\}$ to Tag. On receiving this value, Tag itself computes the value of $A_S' = P_T.H(t_1 + s_1) + Pr_T.S_1$ using its private key and public key and checks whether both values i.e. $A_S = A_S'$ are equal. If both are equal, then the server is successfully authenticated by Tag. Here also. If the adversary itself seeks as the legitimate server then it should produce a correct value of $\{A_S\}$ which is comprised of Tag's secret key which is known only to the server and Tag.

Thus, our proposed protocol guarantees mutual authentication between Server and Tag.

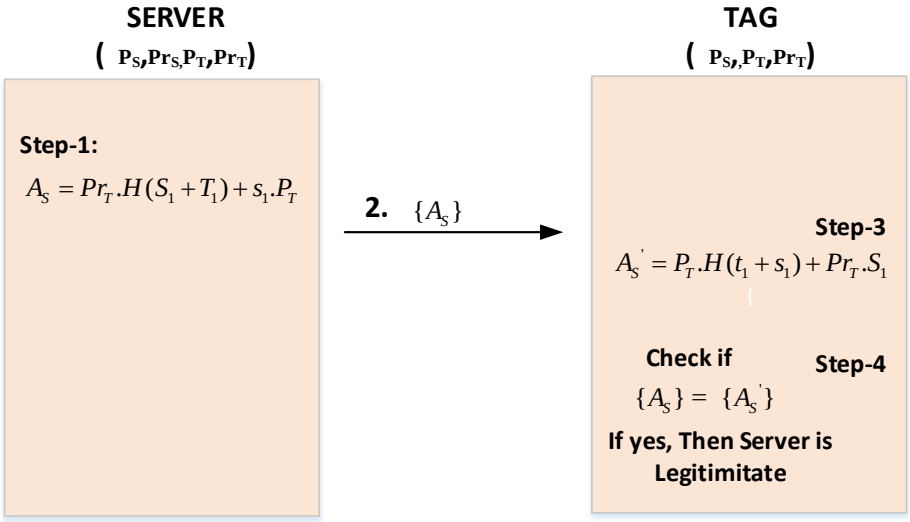

Fig 3. Server Authentication Phase

1) ANONYMITY

Anonymity is also an important security requirement in authentication protocols as it ensures that identity is not revealed to everyone.

Our proposed protocol relies on the freshness of random numbers as in each run, pseudo-random numbers (t_1, s_1) are generated. Also, these random numbers are used in further calculations i.e. $TP_1 = t_1.S_1$, $TP_2 = t_1.P_S$, $T_1 = t_1.G$, $S_1 = s_1.G$ $A_T = P_T + H(TP_1) + TP_2$. So, different values will be generated in each run thus, it will prevent the attacker from predicting the Tag's identity.

Thus, our proposed protocol ensures the protection against anonymous behavior of Tags and Server.

2) SCALABILITY

Scalability is a desirable property in all systems which enables the system to adapt to increasing demands. RFID authentication protocol should also be scalable with an increasing number of Tags.

In Step-8 of our Tag Authentication Phase. The server extracts the value of P_T from received A_T and then searches the matched value in the database. So, the Server doesn't need to search the tag's identity linearly thus, it saves the computation cost while the number of tags increases.

Thus, our proposed protocol provides scalability with an increased number of tags.

3) AVAILABILITY

In our proposed protocol, based on Assumption (iii), the ID-verifier of Tag i.e. P_T is secure and the attacker can't access it Also, its value is the same in the exchanged messages and thus, the server and tag are constantly synchronized.

Thus, the proposed protocol ensures the availability of a property.

4) PERFECT FORWARD SECURITY

Forward Security ensures that previously transmitted information should not be traced using the present transmission information.

In our proposed protocol, if it is assumed that adversary (A) predicts the private-public key pair of Tag (Pr_T, P_T) by physical attacks, still adversary cannot predict the further calculations as they are based on fresh temporary generated random values. So, the adversary can't predict the transmitted messages and can't use this information later.

Thus, our proposed protocol ensures perfect forward security.

B. ANALYSIS OF DIFFERENT SECURITY ATTACKS

IoV network is a real-time dynamic network comprised of Vehicles, RSUs, personal devices, etc. and it includes a huge amount of sensitive data. Security is one of the important concerns in such networks as these networks are delay tolerant and any misleading action can result in hazardous actions i.e. loss of lives. The main objective of IoV is to ensure road safety and traffic efficiency but nothing is ideal, several security attacks still exist in such networks.

So, in this paper, the proposed protocol is designed in such a way that it must mitigate the security attacks which are possible in IoV and RFID systems.

In this section, the efficacy of the proposed ECC-based RFID authentication protocol to prevent the security attacks in the IoV system is discussed:

1) PREVENTION AGAINST REPLAY ATTACK

A replay attack is an active attack in which a malicious user deliberately transmits the information repeatedly.

In our proposed protocol, suppose the adversary intercepts the intermediate tokens calculated in the both tag and server authentication phase i.e., $A_T = P_T + H(TP_1) + TP_2$ and $A_S = Pr_T.H(S_1 + T_1) + s_1.P_T$ to launch the replay attack by using previous A_T and A_S. But his action will fail due to Assumption (i) because the freshness of A_T and A_S are assured

in each session as these two tokens are computed using random numbers (t_1 , S_1). Thus, the proposed protocol resists the Replay attack.

2) PREVENTION AGAINST DENIAL-OF-SERVICE (DOS) ATTACK

DoS attack is an active attack in which the malicious user prevents the legitimate users from accessing the specific resources/service.

In our proposed protocol, Tag's ID-verifier P_T is securely transmitted to the server and the attacker can't access it as mentioned in Assumption(i). Also, its value is the same and thus, the tag and server are constantly synchronized. Thus, the proposed protocol resists the DoS attack.

3) PREVENTION AGAINST TAG MASQUERADING ATTACK

A masquerading attack is an attack where an attacker pretends to be a legitimate user to access the resources for which he is not authorized.

In our proposed protocol, if an adversary tries to attempt the tag masquerading attack then it will masquerade the identity of the tag. So, in step 6 of the Tag authentication phase, where the tag sends $\{A_T, T_1\}$to the server for authentication then it has to generate the valid A_T otherwise the server will not be able to authenticate it as it matches the entry with the database entry. But, the valid value of A_T cannot be generated by the adversary as he doesn't know the value of Tag's verifier, P_T. Thus, our proposed protocol resists the Tag Masquerading attack.

4) PREVENTION AGAINST SERVER SPOOFING ATTACK

The term 'Server Spoofing' refers to an attack in which an attacker pretends to be the server to take advantage.

In our proposed protocol, if the attacker masquerades as the server, then in step 1 of the Server Authentication phase, an attacker needs to generate a valid A_S. But it is not possible for the attacker as the value of A_S cant is generated without knowing the private-key of Tag which is known only to tag and a legitimate server. Thus, the proposed protocol resists the Server Spoofing attack.

5) PREVENTION AGAINST CLONING ATTACK

Cloning attacks are possible if a set of tags share the same secret key and utilize it for authentication.

In our proposed protocol, each tag has its unique private key (Pr_T) and ID-verifier (P_T). In case, the attacker captures the unique keys of a particular tag, then it cannot use the same keys to derive the keys of other tags. Thus, our proposed protocol resists the cloning attack.

VI. SIMULATION OF PROPOSED PROTOCOL USING AVISPA: FORMAL ANALYSIS

For the formal verification of cryptographic protocols, the AVISPA tool is used which is widely used for the evaluation of security protocols[29]. This tool is used to check whether the cryptographic protocol is SAFE or UNSAFE from active and passive security attacks[30].

In AVISPA, protocols are specified using "High-level Protocol Specification language (HLPSL)". The HLPSL specification is converted to 'Intermediate Format' (IF) using the HLPSL2IF translator. IF is a lower-level language than HLPSL and is thus directly read by backends of AVISPA[31]. Verification of protocols is performed by four different backend tools i.e. OFMC, CLAtSe, SATMC, and TA4SP.IF uses one of these four backends to generate output format.

For formal analysis of our proposed protocol, we have simulated the proposed protocol on AVISPA where Tag Authentication Phase and Server Authentication Phase are implemented using HLPSL language. In our proposed protocol, entities used in HLPSL are- role_tag and role_server. Dolev-Yao intruder model is taken as baseline for performing the security analysis of protocol where channel (dy) is used.

Results in Fig. 4 and Fig. 5 indicates that proposed protocol is safe under two backends i.e. OFMC and CL-AtSe and clearly guarantees that the same scheme is secure against active and passive attacks.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/Surbhi/ProposedProtocol.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.03s
  visitedNodes: 16 nodes
  depth: 4 plies
```

Fig 4. Results of OFMC Backend

VII. PERFORMANCE ANALYSIS

The efficiency of any authentication protocol is determined by its performance. In this section, we have evaluated the performance of the proposed ECC-based RFID authentication protocol for IoV in terms of 3 parameters i.e., Storage Requirements, Communication Cost, and Computational Cost.

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  /home/span/Surbhi/ProposedProtocol.if
GOAL
  As Specified
BACKEND
  CL-AtSe
STATISTICS
  Analysed   : 5 states
  Reachable  : 1 states
  Translation: 0.00 seconds
  Computation: 0.00 seconds
```

Fig 5. Results of CL-AtSe Backend

1. *Computational Cost*: It represents the running time required by Server and Tag while executing the authentication phases.
2. *Communication Cost:* In the authentication phase, the length of messages exchanged between Tag and Server represents the Communication Cost.
3. *Storage Requirement:* It represents the memory space used by Server and Tag in authentication phases for storing the required data.

For comparative analysis, we have compared the performance of our proposed protocol with 4 existing ECC-based RFID authentication protocols like Lee et al.'s protocol[2], Liao et al.'s protocol [3], He et al.'s scheme[4], and Dinarvand et al.'s protocol[5].

A. ANALYSIS OF COMPUTATIONAL COST

Computational cost is computed by the elliptic curve's run time. For computing the Computational cost of authentication protocols, we have assumed the elliptic curve of 160 bit, and the running time of different operations computed on 5 MHz Tag and PC (Server) are shown in Table 3 as mentioned by authors in [32, 33].

Table 3. Running time of Elementary Operations

Operations	5 MHz Tag	PC (Server)
Hash Function(SHA-1)	0.0000648 sec	0.000002217 sec
EC Scalar Multiplication over $E(F_{160})$	0.064 sec	0.00112405 sec

Also, the average running time for the basic arithmetic operations in GF (2^m) where m=163 is computed in microseconds using LiDIA [34, 35] as mentioned below:

- Addition Operation- 0.6 μs
- Multiplication Operation- 10.5 μs
- Inversion Operation- 96.2 μs

1) COMPUTATIONAL COST OF TAG:

Based on average running times calculated by LiDIA, the following assumptions have been made for Tag:

'T': Running time required for Multiplication operation, Then, 'T/20': Running time required for Addition operation and Subtraction operation (For multiplication, value is 10.5 μs and for addition, its value is 0.6 μs which is approximately T/20 of multiplication operation)

And Similarly, '9T': Running time required for Inversion operation. Also, the running time of the hash function as mentioned in Table 2 is very less so, it can be neglected while computing the Computational Cost.

The Computational cost of Tag in the proposed protocol is compared with the other 4 existing RFID-based ECC-authentication protocols and is mentioned in detail in Table 4.

The graphical representation of Comparative Analysis of Tag's Computational Cost is shown in Fig. 6.

2) COMPUTATIONAL COST OF SERVER:

Based on average running times calculated by LiDIA, the following assumptions have been made for the Server:

T': Running time required for Multiplication operation in Server,

Then, T'/20: Approximate Running time required for Addition operation (For multiplication, value is 10.5 μs and for addition, its value is 0.6 μs which is approximately T/20 of multiplication operation),

T'/20: Approximate Running time required for Subtraction operation.

And Similarly, '9T': Running time required for Inversion operation.

The Computational cost of the Server in the proposed protocol is compared with the other 4 existing RFID-based ECC-authentication protocols and is mentioned in detail in Table 5.

The graphical representation of Comparative Analysis of Server's Computational Cost is shown in Fig. 7.

B. ANALYSIS OF COMMUNICATION COST

Each point on the elliptic curve is assumed to be 320 bits since the Elliptic curve length is 160 bits[4].

1) COMMUNICATION COST OF TAG:

In the proposed protocol, Tag sends the message $\{A_T, T_1\}$ to the Server where $T_1 = t_1.G$ and $A_T = P_T + H(TP_1) + TP_2$. So, the communication cost of Tag is 320 + 320 = 640 bits.

2) COMMUNICATION COST OF SERVER:

In the proposed protocol, the Server sends the message $\{S_1\}$ and $\{A_S\}$ to the Tag where $S_1 = s_1.G$ and $A_S = Pr_T.H(S_1 + T_1) + s_1.P_T$. So, the communication cost of the Server is 320 + 320 = 640 bits.

The comparative analysis of the Communication cost of the proposed protocol (Both Tag and Server) with the other 4 existing ECC-based RFID authentication protocols is

Table 4. Analysis of Tag's Computational Cost

Protocol	Operations	Computational Cost
Lee.et.al's protocol [2]	Scalar Multiplication- 7 Inversion- 4 Addition- 3 Hash Functions- 2	Computational Cost= 7*T + 4*9T+ 3*(T/20)+ 2*H= 43.15 T=43.3*0.064=2.7616 sec
Liao.et.al's protocol [3]	Scalar Multiplication- 5 Addition- 3	Computational Cost = 5*T+3*(T/20)= 5.15T= 5.15*0.064=0.3296sec.
He.et.al's scheme [4]	Scalar Multiplication- 5 Inversion- 2 Addition-2	Computational Cost= 5*T+2*9T+2*(T/20)= 23.1T= 23.1*0.064=1.4784sec
Dinarvand.et.al's protocol [5]	Scalar Multiplication- 11 Inversion- 10 Addition-4	Computational Cost= 11*T+10*9T+4*(T/20)= 101.2T=101.2*0.064=6.4768sec
Proposed protocol	Scalar Multiplication- 6 Addition- 4 Hash Functions- 2	Computational Cost = 6*T+4*(T/20)+ 2*H= 5.15T= 5.15*.064=0.3968sec.

Table 5. Analysis of Server's Computational Cost

Protocol	Operations	Computational Cost
Lee.et.al's protocol [2]	Scalar Multiplication- 7 Inversion- 4 Addition- 3 Hash Functions- 2 Subtraction-1	Computational Cost= 7*T'+ +4*9T'+3*T'/20+2*H +1*T'/20=43.2T'=43.2*0.001124= 0.0485568 sec
Liao.et.al's protocol [3]	Scalar Multiplication- 5 Addition- 1 Subtraction-2	Computational Cost = 5*T'+1*T'/20+2*T'/20 =5.15T' =5.15*0.001124=0.0057886 sec.
He.et.al's scheme [4]	Scalar Multiplication- 7 Inversion- 4 Addition-3 Subtraction-1	Computational Cost= 7*T'+4*9T'+3*T'/20+1*T'/20 =43.2T'=43.2*0.001124= 0.0485568 sec
Dinarvand.et.al's protocol [5]	Scalar Multiplication- 7 Inversion- 5 Addition-2	Computational Cost= 7*T'+5*9T'+2*(T'/20)= 52.1T'=52.1*0.001124= 0.0585604 sec
Proposed protocol	Scalar Multiplication- 6 Addition- 2 Hash Functions- 2 Subtraction-1	Computational Cost = 6*T'+2*T'/20+1*T'/20+2*H=6.15T'= 6.15*0.001124= 0.0069126 sec.

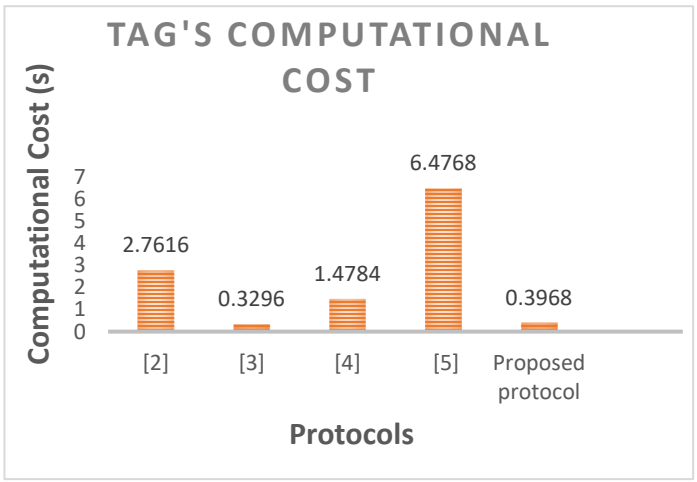

Fig 6. Comparative Analysis of Tag's Computational Cost

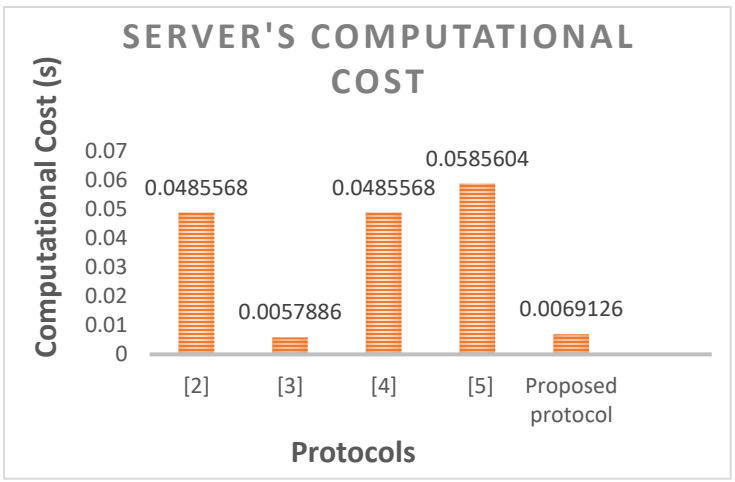

Fig 7. Comparative Analysis of Server's Computational Cost

mentioned in Table 6.

Table 6. Comparative Analysis of Communication Cost

Protocols	Tag	Server	Total (Tag + Server)
Lee.et.al's protocol [2]	640 bits	640 bits	1280 bits
Liao.et.al's protocol [3]	640 bits	640 bits	1280 bits
He.et.al's scheme [4]	640 bits	640 bits	1280 bits
Dinarvand.et.al's protocol [5]	800 bits	640 bits	1440 bits
Proposed protocol	640 bits	640 bits	1280 bits

Table 7. Comparative Analysis of Storage Requirements

Protocols	Tag	Server	Total (Tag + Server)
Lee.et.al's protocol [2]	1600 bits	(1440+320x)bits	(3040+320x)bits
Liao.et.al's protocol [3]	1760 bits	(1440+480x)bits	(3200+480x) bits
He.et.al's scheme [4]	1600 bits	(1440+320x)bits	(3040+320x)bits
Dinarvand.et.al's protocol[5]	1760 bits	(1440+800x)bits	(3200+800x)bits
Proposed protocol	1600 bits	(1440+320x) bits	(3040+320x)bits

C. ANALYSIS OF STORAGE REQUIREMENTS

Storage Requirements indicate the amount of storage needed by Tag and Server in the Authentication phase for storing the required parameters.

1) STORAGE REQUIREMENT OF TAG:

In the proposed protocol, Tag stores the Elliptic curve parameters i.e. (G, a, b, n, q), Its Private-Public key pair, (Pr_T, P_T). So, the required storage space by Tag is (320+160+160+160+160) + (160+320) bits = 1600 bits.

2) STORAGE REQUIREMENT OF SERVER:

In the proposed protocol, Server stores the Elliptic curve parameters i.e. (G, a, b, n, q), Its Private-Public key pair, (Pr_S, P_S) and Private-key of Tag, (Pr_T). So, the required storage space by Server is (320+160+160+160+160) + (160+320) + {(160)x} bits= (1440+320x) bits where 'x' is the number of tags in a system.

The comparative analysis of Storage requirements of the proposed protocol (Both Tag and Server) with the other 4 existing ECC-based RFID authentication protocols is mentioned in Table 7.

VIII. PROPOSED BLOCKCHAIN-BASED SECURITY FRAMEWORK FOR RFID-ENABLED IoV

Blockchain is one of the trending technology nowadays and has applications in different domains. Blockchain was initially introduced as an underlying technology for Bitcoin and other digital currencies[36, 37]. It is a collection of blocks that contain transactions, records, and other information, and all of the blocks are connected to form a chain using cryptographic techniques[38, 39]. The unique features of Blockchain are decentralization, immutability, transparency, and peer-to-peer communication[40, 41].

In the majority of IoV application scenarios, Blockchain offers several innovative solutions. The integrity of blockchain into IoV improves security, privacy as well as enhances the overall system performance[42, 43]. Apart from this, Blockchain is a lifesaver in situations when the participating entities lack trust[44]. Blockchain performs effectively in IoV networks where critical information exchange takes place among vehicles all the time and vehicles lack trust among each other. Unlike centralized functioning, blockchain technology distributes the task of ensuring privacy and security among all entities in the IoV[45, 46].

A. MOTIVATION OF PROPOSING BLOCKCHAIN BASED SECURITY FRAMEWORK FOR RFID-ENABLED IoV NETWORK

Blockchain due to its vast secure usability in different research areas and networks can also be applied to the RFID-based IoV for further enhancement of the IoV security which is very much required because IoV is directly associated with the lives of the people**.** The Proposed Blockchain-Based Security Framework when used along with the ECC-based RFID system will considerably enhance the security as well as the integrity of the whole IoV network.

RFID technologies are not just limited to toll collections. It is also being used in various other application areas of IoV such as remote patient health monitoring, parking management, etc. So, the integration of secure ECC-based RFID technology along with the blockchain will strengthen the overall network. RFID technology ensures road safety and efficient traffic management due to numerous applications in IoV i.e. automatic toll collection, identification of high-speed movement of multiple vehicles, tracking the location of vehicle, intelligent parking system, etc**.**

If we consider the scenario of RFID-based Automatic toll collection, Blockchain will enhance the user experience as the

user details are stored in a particular server where details regarding money deduction on crossing the toll or the time of toll crossing, etc. are stored. So this critical information can be hacked by a malicious user but the incorporation of blockchain in RFID enabled IoV will prevent data tempering due to immutability and decentralization**.**

Similarly, RFID technology felicitates the intelligent parking system and tracking the location of a vehicle in IoV scenarios, but if the location of the vehicle and parking information regarding vacant parking slots, etc. is compromised by a malicious user, it can result in hazardous actions. So, blockchain is a lifesaver in such scenarios where blockchain will preserve the critical information of the IoV network due to its unique features**.**

Thus, the integration of Blockchain technology in the RFID-enabled IoV network will add to the strength of the network. This is the main reason for also proposing a blockchain-based security framework in this article along with the ECC-based authentication.

B. PROPOSED BLOCKCHAIN-BASED SECURITY FRAMEWORK FOR IoV

Keeping in the mind the above considerations, a Blockchain-based security framework for IoV is proposed. The proposed system is composed of different entities of the IoV network i.e. RSU, Vehicles, Blocks, Cloud Server, Critical messages.

a) **RSU**: RSU plays an important role in the IoV network as it has more computing power and storage than vehicles. Also, it disseminates the safety information from vehicles to Cloud for storage, such critical information needs to be securely transmitted as any tampering can lead to hazardous results. In the proposed system, RSU is responsible for authentication in V2I communication and legitimate RSU creates the first block of blockchain known as the genesis block.

b) **Vehicles**: Vehicles are the main entities of the IoV network and are equipped with OBU (On-board Unit) consisting of Sensors, GPS, RFID tags, etc. V2V communication is performed among different vehicles while communicating with each other. On the occurrence of any critical event like accident information, other traffic hazards, etc. A nearby vehicle will send the critical message to the nearest RSU and RSU checks the authenticity of the message and vehicle.

c) **Cloud Server:** It is one of the important entities of proposed system and has various responsibilities. Before the actual deployment, all vehicles and RSUs need to register themselves with the Cloud where all the information is stored including keys, identities etc.

d) **Blocks**: Blocks are main entity of blockchain. It consists of Block header and Block body are the components of Block where block header includes previous block's hash, Merkle root, timestamp and nonce. In our proposed protocol, critical messages acts as transactions of blockchain unlike cryptocurrency as transactions in Bitcoin. So, here block body consists of list of critical messages and the trust level (TL) of vehicles.

e) **Critical Messages**: In networks like IoV, a lot of real-time data is involved so, critical messages play an important role. Critical messages include accident information, emergency vehicle information, etc., and are given priority over other messages as such messages can't be delayed otherwise it can lead to loss of lives. In our proposed protocol, critical messages have a key role so whenever such an incident occurs, then critical messages are forward by a nearby vehicle to the nearest RSU.

In our proposed protocol, the different phases involved are Setup Phase, Registration Phase, Critical Event Detection and Authentication Phase, Block Creation, and Validation.

a) **Set up Phase**: In the Setup Phase, all the public and private key pairs are generated based on ECC operations and are stored in the Cloud Server. It is assumed that the server is secure from all attacks and thus, all stored information will be properly secured.

b) **Registration Phase**: In this phase, all the vehicles will register themselves with the nearest RSU using their unique ID-verifier and RSU will register itself with the Server.

c) **Critical Event Detection Phase and Authentication Phase**: In this phase, whenever any vehicle notices some critical event then it transmits the critical message to the nearest RSU. In our proposed protocol, the critical message consists of information like event type, location, trust level (TL), the ID of the sender vehicle. Trust level is computed as the fraction of valid critical messages 'a' sent by vehicle to the total critical messages a+b, i.e.,

$$TL = a/a+b \quad (12)$$

On receiving the critical message, RSU verifies the authenticity of the sender vehicle and critical message by calculating the trust level of the sender vehicle and forwards the received message to the server. The server then checks its database and based on that, it sends an acknowledgment to RSU**.**

d) **Block Creation and Validation:** Once the critical message is verified to be a true message then RSU creates a new block and forwards it to other RSUs. Other RSUs on receiving the block perform necessary verification and adds a new block to the blockchain-based on Proof of Authentication (PoAh) as a consensus mechanism which is suitable for resource-constrained applications like IoV and IoT[47-49]. Also, the trust level of vehicles in the block header is updated by 1 when a new block is added to the blockchain.

The proposed Blockchain-based method seems to be quite secure due to the below reasons:

- Each block is based on the hash value of the previous block, so it's very unrealistic that any malicious vehicle will insert the fake block as it requires a lot of computational power to change the hash of succeeding blocks.

- As the size of the IoV network increases, blockchain becomes more difficult to be compromised by malicious vehicles.

A. EVALUATION OF PROPOSED BLOCKCHAIN-BASED SCHEME IN TERMS OF STORAGE AND MESSAGE OVERHEAD:

In this section, the storage and message overhead of the proposed blockchain-based scheme is evaluated. The size of the block header is about 80 bytes and the size of the critical message will be about 512 bytes. So, the total size of one block with a single transaction will be (512+80) =592 bytes. In our proposed scheme, to prevent the attacks, it is assumed that each block is generated in 80 sec. Based on this, the total number of blocks that would be generated per hour is 45. Also, the Size of Blockchain is calculated by the mathematical formula:

$$\text{Blockchain size} = T_x * B_x * T \quad (13)$$

where T_x denotes the number of message transactions per time, B_x denotes the Size of Block and T is time in units.

In our proposed scheme, the size of Blockchain with a single transaction per week = (592*45*24*7) = 4.268 MB.

The proposed Blockchain-based scheme is scalable with a large amount of data as the IoV network is vast and the estimated growth of blockchain with different transactions per time is mentioned in Table 8.

For 100 transactions, the size of Blockchain per month= 100*(592 bytes*60*60*24*30) = 0.139 GB. Similarly for 100 transactions, size of Blockchain per 6 months= 6*0.139 GB= 0.837 GB and for 100 transactions, the size of Blockchain per year= 12*0.139 GB= 1.668 GB. Similarly, the size of the Blockchain is computed for 200 and 500 transactions and is shown in Table 8.

Table 8. Estimated growth of blockchain with different transactions per time

Transactions	One Month	6 Months	1 year
100	0.139 GB	0.837 GB	1.668 GB
200	0.279 GB	1.674 GB	3.348 GB
500	0.697 GB	4.186 GB	8.364 GB

The complete workflow of the proposed blockchain-based security framework for RFID-enabled IoV is illustrated in Fig. 8.

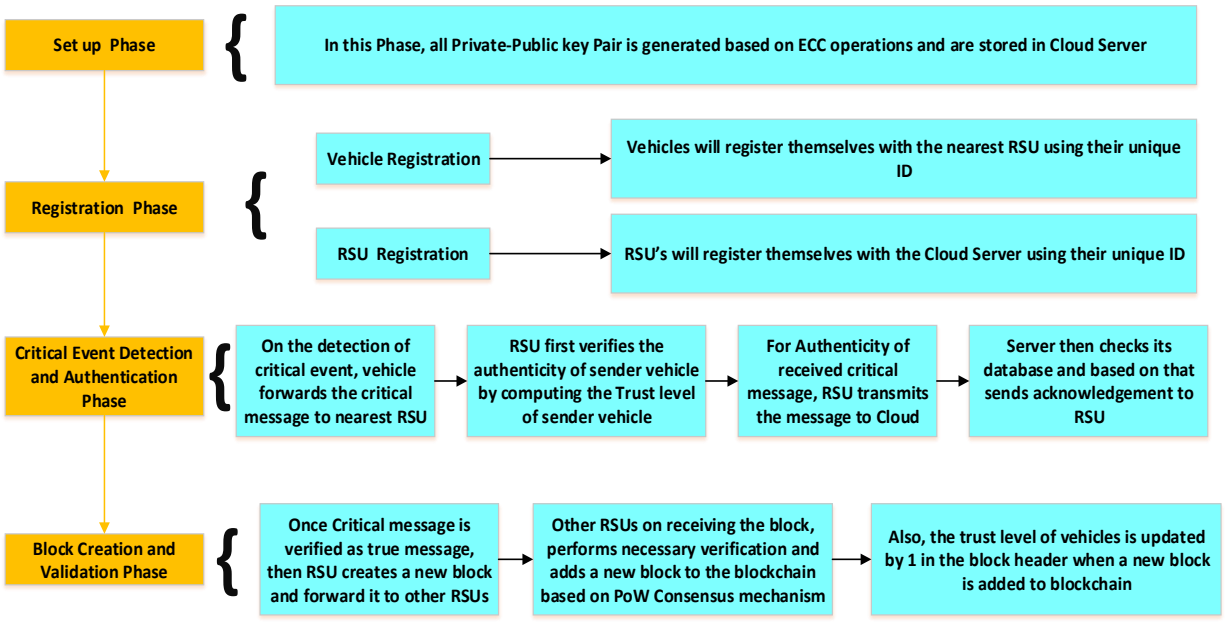

Fig 8. Proposed Blockchain-based novel security framework for RFID-enabled IoV

IX. CONCLUSION AND FUTURE SCOPE

Internet of Vehicles (IoV) have revolutionized transportation systems and have gained huge market interest due to the incorporation of emerging technologies like RFID technology, Edge Computing, Fog Computing, and Cloud Computing, etc. RFID technology is one of the prominent technologies of IoV which is based on wireless communication for data exchange. RFID has numerous applications in IoV networks like automatic toll collection, data dissemination among vehicles,

distant vehicle identification, etc. which can greatly enhance the performance and effectiveness of IoV networks. Along with this, RFID devices are prone to numerous security threats which will, in turn, hamper the performance of the IoV network as it is a real-time dynamic network.

Keeping in view the above scenarios, a Cryptographic solution-based secure ECC-enabled RFID authentication protocol is proposed for the Internet of Vehicles. The proposed protocol consists of ECC-based lightweight operations and is comprised of three phases: Setup Phase, Tag Authentication Phase, and Server Authentication Phase. Security evaluation of the proposed protocol is done by taking into consideration the analysis of security requirements as well as security attacks. The proposed protocol satisfies various security requirements like Mutual Authentication, Availability, Anonymity, etc. and it also prevents different security attacks like DoS attacks, Replays attacks, Cloning Attacks, etc. Also, the simulation of the proposed protocol is done using AVISPA, and results are shown using backends OFMC and Cl-AtSe and both backends indicate that the proposed protocol is safe and is secure from all passive and active attacks. The performance evaluation of the proposed protocol is done based on parameters i.e. security requirements, communication cost, and computational cost and Results indicate that the proposed protocol contributes to high performance and security and has low computational cost than other existing authentication protocols.

A novel blockchain-based security framework for RFID-enabled IoV has also been proposed to further enhance the security of the IoV network. Also, the estimated growth of the proposed blockchain with different transactions per time is computed. As future work, the implementation of the proposed blockchain-based security framework may be done and the performance of the blockchain-based framework may be evaluated.

REFERENCES

1. Gurubani, J.B., H. Thakkar, and D.R. Patel. *Improvements over extended LMAP+: RFID authentication protocol*. in *IFIP International Conference on Trust Management*. 2012. Springer.
2. Lee, C.-I. and H.-Y.J.I.J.o.D.S.N. Chien, *An elliptic curve cryptography-based RFID authentication securing E-health system.* 2015. **11**(12): p. 642425.
3. Liao, Y.-P. and C.-M.J.A.h.n. Hsiao, *A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol.* 2014. **18**: p. 133-146.
4. He, D., et al., *Lightweight ECC based RFID authentication integrated with an ID verifier transfer protocol.* 2014. **38**(10): p. 1-6.
5. Dinarvand, N. and H.J.W.N. Barati, *An efficient and secure RFID authentication protocol using elliptic curve cryptography.* 2019. **25**(1): p. 415-428.
6. Sharma, S., B.J.S. Kaushik, and P.i.t.I.o. Things, *Security Solutions for Threats in IoT-Based Smar t Vehicles.* 2020: p. 133.
7. Sharma, S. and B.J.I.J.o.C.S. Kaushik, *A survey on nature-inspired algorithms and its applications in the Internet of Vehicles.* p. e4895.
8. Sharma, S. and B.J.V.C. Kaushik, *A survey on internet of vehicles: Applications, security issues & solutions.* 2019. **20**: p. 100182.
9. Song, B. and C.J. Mitchell. *RFID authentication protocol for low-cost tags*. in *Proceedings of the first ACM conference on Wireless network security*. 2008.
10. Benssalah, M., M. Djeddou, and K.J.T.o.E.T.T. Drouiche, *A provably secure RFID authentication protocol based on elliptic curve signature with message recovery suitable for m-health environments.* 2017. **28**(11): p. e3166.
11. Hunt, V.D., A. Puglia, and M. Puglia, *RFID: a guide to radio frequency identification*. 2007: John Wiley & Sons.
12. Duroc, Y. and S.J.C.R.P. Tedjini, *RFID: A key technology for Humanity*. 2018. **19**(1-2): p. 64-71.
13. Cole, P.H. and D.C.J.L. Ranasinghe, UK: Springer. doi, *Networked RFID systems and lightweight cryptography*. 2008. **10**: p. 978-3.
14. Fan, K., et al., *Permutation matrix encryption based ultralightweight secure RFID scheme in internet of vehicles.* 2019. **19**(1): p. 152.
15. Chien, H.-Y.J.I.t.o.d. and s. computing, *SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity*. 2007. **4**(4): p. 337-340.
16. Juels, A. *Minimalist cryptography for low-cost RFID tags*. in *International conference on security in communication networks*. 2004. Springer.
17. Peris-Lopez, P., et al. *LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags*. in *Proc. of 2nd Workshop on RFID Security*. 2006.
18. Tian-tian, Y. and F. Quan-yuan. *A security RFID authentication protocol based on hash function*. in *2009 International Symposium on Information Engineering and Electronic Commerce*. 2009. IEEE.
19. Lv, C., et al., *Security analysis of two recently proposed RFID authentication protocols.* 2011. **5**(3): p. 335-340.
20. Chen, Y.-Y., et al. *A low-cost RFID authentication protocol with location privacy protection*. in *2009 Fifth International Conference on Information Assurance and Security*. 2009. IEEE.
21. Chien, H.-Y., C.-H.J.C.S. Chen, and Interfaces, *Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards.* 2007. **29**(2): p. 254-259.
22. Peris-Lopez, P., et al., *Cryptanalysis of a novel authentication protocol conforming to EPC-C1G2 standard.* 2009. **31**(2): p. 372-380.
23. Kaur, K., et al. *Lightweight authentication protocol for RFID-enabled systems based on ECC*. in *2016 IEEE Global Communications Conference (GLOBECOM)*. 2016. IEEE.
24. Alamr, A.A., et al., *A secure ECC-based RFID mutual authentication protocol for internet of things.* 2018. **74**(9): p. 4281-4294.
25. Miller, V.S. *Use of elliptic curves in cryptography*. in *Conference on the theory and application of cryptographic techniques*. 1985. Springer.
26. He, D., et al., *Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks.* 2015. **21**(1): p. 49-60.
27. Kumar, N., et al., *An intelligent RFID-enabled authentication scheme for healthcare applications in vehicular mobile cloud.* 2016. **9**(5): p. 824-840.
28. Gabsi, S., et al. *Architectural choices for implementing a secure ECC-based lightweight RFID tag*. in *2019 IEEE International Conference on Design & Test of Integrated Micro & Nano-Systems (DTS)*. 2019. IEEE.
29. Vigano, L.J.E.N.i.T.C.S., *Automated security protocol analysis with the AVISPA tool.* 2006. **155**: p. 61-86.
30. Team, T.J.I.s.t.p.h.a.-p.o., *AVISPA v1. 1 User manual.* 2006.
31. Guide, A.B.s., *HLPSL Tutorial.* 2006.
32. Gódor, G. and S. Imre. *Elliptic curve cryptography based authentication protocol for low-cost RFID tags*. in *2011 IEEE international conference on RFID-technologies and applications*. 2011. IEEE.
33. Gódor, G., N. Giczi, and S. Imre. *Elliptic curve cryptography based mutual authentication protocol for low computational capacity RFID systems-performance analysis by simulations*. in *2010 IEEE international conference on wireless communications, networking and information security*. 2010. IEEE.
34. Biehl, I., J. Buchmann, and T. Papanikolaou, *LiDIA: A library for computational number theory.* 1995.

35. López, J. and R. Dahab. *Fast multiplication on elliptic curves over GF (2 m) without precomputation*. in *International Workshop on Cryptographic Hardware and Embedded Systems*. 1999. Springer.
36. Puri, V., et al., *A vital role of blockchain technology toward internet of vehicles*, in *Handbook of research on blockchain technology*. 2020, Elsevier. p. 407-416.
37. Zhang, J., et al., *Blockchain-based systems and applications: a survey*. 2020. **21**(1): p. 1-14.
38. Frizzo-Barker, J., et al., *Blockchain as a disruptive technology for business: A systematic review*. 2020. **51**: p. 102029.
39. Wang, J., et al., *Blockchain-based data storage mechanism for industrial internet of things.* 2020. **26**(5): p. 1157-1172.
40. Mollah, M.B., et al., *Blockchain for the internet of vehicles towards intelligent transportation systems: A survey*. 2020. **8**(6): p. 4157-4185.
41. Zhang, J., et al., *A storage optimization scheme for blockchain transaction databases.* 2021. **36**(3): p. 521-535.
42. Xu, Z., et al., *A blockchain-based roadside unit-assisted authentication and key agreement protocol for internet of vehicles.* 2021. **149**: p. 29-39.
43. Wang, J., et al., *Data secure storage mechanism of sensor networks based on blockchain.* 2020. **65**(3): p. 2365-2384.
44. Belotti, M., et al., *A vademecum on blockchain technologies: When, which, and how*. 2019. **21**(4): p. 3796-3838.
45. Dwivedi, S.K., et al., *Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism.* 2020. **54**: p. 102554.
46. Wang, J., et al., *Blockchain Based Data Storage Mechanism in Cyber Physical System.* 2020. **21**(6): p. 1681-1689.
47. Puthal, D. and S.P.J.I.P. Mohanty, *Proof of authentication: IoT-friendly blockchains.* 2018. **38**(1): p. 26-29.
48. Puthal, D., et al. *Proof-of-authentication for scalable blockchain in resource-constrained distributed systems*. in *2019 IEEE International Conference on Consumer Electronics (ICCE)*. 2019. IEEE.
49. Umran, S.M., et al., *Secure data of industrial internet of things in a cement factory based on a Blockchain technology.* 2021. **11**(14): p. 6376.

Surbhi Sharma is perusing her Ph.D. in the Department of Computer Science and Engineering, Shri Mata Vaishno Devi University, Katra, India and has obtained M.Tech CSE from SMVD University in 2016. Her research interests include Security, Internet of vehicles, Cryptography and Ad-hoc networks. She has published various research articles in reputed SCI/Scopus indexed journals

Dr Baijnath Kaushik received B.E. in Computer Science and Engineering from Nagpur University, Nagpur in 1997, Master of Technology from University School of Information Technology, GGSIPU, New Delhi in 2009 and Ph.D. in Computer Science from IIT Dhanbad, Dhanbad in 2016.. Presently, he is an Associate Professor in the School of Computer Science & Engineering, SMVDU, Katra, J&K. His research areas of interest include Machine Learning, Deep Learning, Nature Inspired Algorithms, Soft Computing and Parallel Algorithms.

MOHAMMAD KHALID IMAM RAHMANI (SMIEEE) was born in Patherghatti, Kishanganj, Bihar, India in 1975. He received the B.Sc. (Engg.) and the M.Tech. degrees in Computer Engineering from Aligarh Muslim University, India in 1998 and Maharshi Dayanand University Rohtak in 2010 respectively, and the Ph.D. degree in Computer Science Engineering from Mewar University, India, in 2015. From 1999 to 2006, he was a Lecturer with

Maulana Azad College of Engineering and Technology, Patna. From 2006 to 2008, he was a Lecturer and Senior Lecturer with Galgotias College of Engineering and Technology, Greater Noida. From 2010 to 2011 he was Assistant Professor in GSMVNIET, Palwal. From 2017 he is an Assistant Professor in the Department of Computer Science, College of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia. His research interests include Algorithms, IoT, Cryptography, Image Retrieval, Pattern Recognition, Machine Learning, and Deep Learning. He has published more than 35 research papers in journals and conferences of international repute, 3 book chapters and holds one patent of innovation.

Md Ezaz Ahmed received the M.E. (Master of Engineering) degree in Computer Science & Engineering from MDU University Rohtak, Haryana India, in 2008, and the Ph.D. degree in Computer Science from Jodhpur National University, India, in 2013.
He was with NCU, (North Cap University) earlier Known as ITM University Gurgaon Haryana, India as an Assistant Professor, and other rank from 2002 to 2013. Since 2014, he has been with the Department of Computer Science, College of Computing and Informatics, Saudi Electronic University, as an Assistant Professor. His research interests include Data mining, Web Technology, machine learning, deep learning, Data Science and IoT