RESEARCH ARTICLE

INTERNATIONAL RESEARCH JOURNAL OF MULTIDISCIPLINARY TECHNOVATION

Asian Research Association

DOI: 10.54392/irjmt25327

Secure Firmware over the Air Updates for Vehicles using Blockchain, Signcryption, and Proxy Re-encryption

Rachana Y. Patil [a,*], Yogesh H. Patil [b], Deepali Naik [a], Rupali Gangarde [c], Aparna Joshi [a, d], Aparna Bannore [e]

[a] Department of Computer Engineering, Pimpri Chinchwad College of Engineering, Pune, Maharashtra, India.
[b] D. Y. Patil College of Engineering, Akurdi, Pune, Maharashtra, India.
[c] Symbiosis Institute of Technology, Pune, Symbiosis International (Deemed) University, Pune, India.
[d] epartment of Computer Engineering, Pimpri Chinchwad College of Engineering, Pune, Maharashtra, India.
[e] SIES Graduate School of Technology, Nerul, Navi Mumbai, India.
* Corresponding Author Email: rachana.patil@pccoepune.org

DOI: https://doi.org/10.54392/irjmt25327
Received: 29-02-2024; Revised: 13-05-2025; Accepted: 21-05-2025; Published: 30-05-2025

Abstract: Modern electric cars with upgraded passenger vehicles experience security risks from wireless firmware updates that allow attackers to threaten the safety of drivers and their passengers. This research develops a distinctive technique that unites blockchain technology with signcryption and proxy re-encryption to ensure vehicle-manufacturer communication and resolve this problem. Through IPFS (Inter Planetary File System) firmware updates can be safely distributed to permissioned vehicles. The proposed method implements identity-based cryptography as a fusion of signcryption with proxy re-encryption to enhance air-based firmware update security. The security evaluation of this method provides evidence about how well the cryptographic update operations function within the firmware procedure. The study performs a simulation investigation with AVISPA through the implementation of OFMC and Cl-AtSe models. The simulation study results demonstrate that the proposed security techniques prove their resistance to both man in the middle and replay attacks. The study investigates vehicle firmware update security weaknesses to develop a framework which protects firmware update integrity and confidentiality.

Keywords: Firmware Over-The-Air Updates, Signcryption, Blockchain, Re-Encryption, AVISPA

1. Introduction

The automotive industry goes through fundamental changes because of quick developments in automotive technology [1, 2]. The technology evolution brings new capabilities to vehicles which simultaneously enhance safety standards and develops their intelligent capabilities and network connectivity and complexity [3, 4]. The estimated market penetration for internet-connected light-duty trucks and vehicles is set to reach 70 percent by 2023 according to current data [5]. Automobiles connected to the internet open many possibilities and advantages that benefit operators and occupants [6, 7]. The present automotive sector provides numerous vehicles with intelligent systems and advanced connectivity capabilities. The vehicles house multiple electronic control units (ECUs) that enhance their safety and comfort performance capabilities. From the beginning to the end of automotive life cycles Original Equipment Manufacturers (OEMs) must sustain software efficiency [8]. The Original Equipment Manufacturer (OEM) plays a critical role in achieving the best possible software performance of vehicles. Original Equipment Manufacturers possess the responsibility to create software solutions which boost vehicle performance while resolving possible problems that could develop. The original equipment manufacturer (OEM) actively maintains and supervises vehicle software and firmware components to ensure vehicle security [9].

Software efficiency improvement falls under the responsibility of original equipment manufacturers who maintain ongoing inspections of their products. The team fixes software and firmware problems which threaten vehicle safety or security to enhance overall vehicle capabilities [10]. The automotive industry depends on software-driven functionalities which requires maximum emphasis on software reliability and efficiency. Original equipment manufacturers (OEMs) meet their obligations through vehicle production focused on quality improvement and performance enhancement which results in better driving safety and user satisfaction [11].

Current research findings indicate that software-related issues account for a major percentage of product recalls. The Society of Indian Automobile Manufacturers

(SIAM) reported significant growth in vehicle recalls that manufacturers conducted voluntarily during the year 2022. The companies issued vehicle recalls for 206,238 units consisting of cars and SUVs together with two-wheelers. Manufacturers demonstrate significant dedication toward identifying safety risks before they affect consumers as shown by the provided data. Adhering to safety standards in the automotive industry remains essential so vehicle recalls become necessary for industry protection. Traditional recall processes generate substantial expenses while requiring extensive time duration and producing unfavorable environmental effects. FOTA software deployments offer manufacturers a means to reshape the traditional recall approach. Original equipment manufacturers (OEMs) possess the capability to perform remote software updates on vehicles so that physical inspections and repairs become unnecessary [12]. FOTA technology allows manufacturers to provide swift and efficient solutions to problems which results in major cost reductions alongside reduced operational disruptions and decreased environmental impact.

The Federation of Automobile Technicians and Analysts (FOTA) updates significantly boost vehicle capabilities and performance levels. Original equipment manufacturers (OEMs) maintain authority to enhance their existing software by adding new features which also include additional functionalities and improvements. FOTA updates function as a critical element which maintains peak performance and ensures high vehicle safety standards for occupants inside vehicles. Software bugs along with software deficiencies and susceptibilities are resolved to achieve this outcome. FOTA updates bring many advantages to users while exposing them to multiple security threats. The security of vehicles and their integrity becomes vulnerable when software update procedures remain insecure [13]. The unauthorized update process control by a malicious user can result in equipment failure and operational breakdowns which creates risks to vehicle occupants.

OEMs rely on established cloud providers to implement network storage with replication systems that enhance data access speed. Security and privacy issues might arise from OEM implementation of point-to-point encryption between autonomous vehicles and cloud services because end-to-end encryption is absent. Data confidentiality issues and unauthorised access stem from the ability of both cloud providers and OEMs to determine what updates each vehicle requests [14, 15]. Proper encryption solutions and industrial collaboration enable FOTA updates to achieve both quick delivery and secure performance [16, 17]. We present Blockchain-based Signcryption with Proxy Re-encryption (SC-PRE) as our new approach to securing Firmware Over-The-Air (FOTA) updates in vehicles because of existing challenges. Our FOTA system implements blockchain technology to develop an auditable and open and trustworthy update management system. FOTA update management benefits from decentralized auditing features within blockchain technology to ensure interoperability along with audit trails. The participants of the FOTA ecosystem use this technology to perform safe information exchanges. The SC-PRE scheme enhances FOTA update security through secure privacy together with access controls and authentication functions. The combination of competent encryption and digital signatures is achieved through signcryption practices to ensure both authenticity and stability of the update method. Proxy re-encryption functions as a cryptographic method which grants authorized parties safe decryption privileges for processed encrypted data modifications.

The proposed solution in this research fully resolves the issues pertaining to FOTA updates in a comprehensive manner. The solution combines blockchain technology with signcryption and proxy re-encryption methods to achieve its purpose. FOTA updates in automotive systems achieve security through the framework by ensuring both authorization and authentication as well as vehicle access control. The goal of the proposed protocol is to provide secure end-to-end communication of firmware updates by using the BC-SC-PRE-FOTA scheme, This article's many contributions include: The proposed scheme includes essential functions with registration of Data users and data owners with the TTP, signcryption, re0encryption key generation, re-encryption, and decryption, as well as using smart contract and blockchain for keeping track of firmware updates and it’s release. The proposed BC-SC-PRE-FOTA scheme has been shown to be secure against MITM and replay attacks through AVISPA tool.

The continuing segments of the paper are planned as follows: Section 2 provides a summary of related work in the field of FOTA updates using blockchain and proxy re-encryption. Section 3 presents the system overview and preliminaries, introducing the key components and background concepts. In Section 4, the construction of the proposed scheme is explained in detail, outlining the integration of blockchain and proxy re-encryption for secure firmware updates. The security analysis and correctness proofs of the scheme are discussed in Section 5 to ensure its resilience against potential vulnerabilities. Section 6 attends a simulation finding using AVISPA to assess the scheme's security under diverse attack situations. Finally, Section 7 concludes the paper by summarizing all the results, underlining the contributions, and implying future research advice.

2. Related Work

The objective of developing secure FOTA update practices has been the center of many proposed schemes. In this section, we portray a curated set of academic works that extend significant insights into the breadth of our research.

Uptane, a secure framework for vehicles software updates that is built on TUF is presented in [18]. Uptane approaches robust shield against security attacks like man-in-the-middle, while safeguarding the integrity of signing keys continues uncompromised. A unique scheme for updating the firmware of independent vehicles via blockchain technology and smart contracts is discussed in [19]. The intended scheme efficiently handles standing values for vehicles engaged in communicating updates, confirming the validity and integrity of firmware updates. Attribute-Based Encryption (ABE) and zero-knowledge proof protocols characterize advanced cryptographic systems that enable the enabling of directed firmware distribution and secure update exchange. To improve operating efficiency, the utilization of a cumulative signature scheme permits the consolidation of several proofs into an individual blockchain transaction.

A safe protocol for wireless firmware updates in smart cars is presented by authors of [20]. The protocol efficiently eases the hazard of repeat attacks, while concurrently guaranteeing the continuation of data integrity, confidentiality, and authentication. This paper explores the computational efficiency, low memory overhead, and correctness for wireless communication of the protocol, as well as realistic considerations for its execution. The firmware update protocol that has been suggested utilizes lightweight mechanisms, representing it appropriate for implementation within a vehicular ecosystem.

To address these difficulties, this study reports on advanced automotive security framework that influences blockchain technology. The work also emphasizes software update system based on blockchain technology and supports a proof-of-concept implementation to showcase the pertinency of this architecture in automotive systems. In addition, the efficiency of the architecture is evaluated through the consideration of its various components.

A framework for self-verification of firmware updates in vehicle ECUs over the air is discussed in [21]. It involves a trusted portal issuing updates with verification codes, securely downloaded by the vehicle using a FOTA protocol. Virtualization techniques enable simultaneous operation of control and functional systems. A microkernel-based control system flashes and verifies the firmware in the functional system, ensuring correct download and flashing of firmware in memory [22]. The framework addresses the need to detect malicious changes and ensure proper firmware updates in the automotive industry's growing trend of over-the-air updates.

The primary security requirement for any security application is ensuring confidentiality, authentication, non-repudiation, and integrity [23-24]. Conventionally, these requirements are met by digitally signing the message first and then encrypting it. However, a more streamlined approach is the utilization of signcryption, a cryptographic technique that combines both signature and encryption in a single step.

Identity-based cryptography (IBC) plays a crucial role in identity-based signcryption techniques, making it advantageous in various scenarios. Over time, several effective methods for identity-based signcryption (IBSC) have been proposed.

Proxy re-encryption (PRE) is another cryptographic technique that enables a trusted proxy, acting as a third party, to re-encrypt a ciphertext intended for user A into a new ciphertext for user B without requiring user A's private key. The proxy is provided with a re-encryption key (rk_(A→B)) by user A, facilitating the transformation. Throughout this process, the proxy remains unaware of the message's content. The combination of IBC and PRE, known as IBPRE, has resulted in the development of effective IBPRE systems.

In 2008, researchers in [25] introduced a fusion of signcryption with PRE. This system allows a proxy to re-encrypt a signcrypted ciphertext meant for user B into a new ciphertext for user C, excluding user B's private key. However, it should be noted that the security of this scheme against chosen ciphertext attacks is uncertain. Additionally, from a mathematical perspective, the scheme proposed in [25] is considered incorrect.

In the smart grid ecosystem, the massive amount of data generated by IoT devices requires secure storage and management in the cloud server. To meet the security needs of this communication, signcryption with proxy re-encryption is an appropriate technique, allowing a semi-trusted third party to transform ciphertexts without accessing the original message. However, current schemes for signcryption with proxy re-encryption in the smart grid environment suffer from bandwidth and computational inefficiencies [26].

Almazroi et al (2023) [26] proposes a heterogeneous signcryption with proxy re-encryption (HSC-PRE) scheme to address challenges in EHR systems. It demonstrates how the scheme, combined with blockchain technology, achieves secure, interoperable, auditable, and accessible EHR systems. Security analysis confirms the scheme's effectiveness and efficiency compared to other related schemes.

A blockchain-based Split-PRE method for enhancing security and privacy in IoT is presented in [27]. The system enables dynamic smart contracts and efficient proxy re-encryption to improve efficiency, security, and feasibility. Experimental results validate the effectiveness of the approach compared to existing methods.

The paper [28, 29] presents a blockchain-based proxy re-encryption scheme for secure sharing of IoT data, utilizing dynamic smart contracts.

Table 1. Summary of Related Work on Secure Frameworks for FOTA and IoT

Study/Work	Framework/Technique	Key Features	Limitations	Security Focus	IoT Suitability	Scalability
Uptane [18]	TUF-based secure framework	Protects against MITM attacks; Key integrity	No FOTA-specific focus	High	Moderate	Low
Blockchain [19]	Blockchain and smart contracts	Ensures update validity and integrity	High overhead	High	High	Moderate
Wireless [20]	Lightweight mechanisms for vehicles	Confidentiality, authentication; Efficient wireless communication	Limited to vehicular use cases	Moderate	Low	High
Self-Verification [21,22]	FOTA with trusted portal	Verifies firmware; Microkernel-based control	Complex real-time implementation	High	Moderate	Moderate
IBPRE [25]	Identity-based proxy re-encryption	Secure ciphertext transformation	Not secure against CCA; Incorrect	Low	Moderate	Low
HSC-PRE [26]	Heterogeneous signcryption with PRE	Secures EHR systems; Interoperability	Bandwidth issues	High	Low	Moderate
Split-PRE [27]	Blockchain-based proxy re-encryption	Dynamic smart contracts; Efficient security	IoT resource constraints	High	High	High
IoT Data [28, 29]	Blockchain with proxy re-encryption	Data confidentiality; Performance	Not feasible for FOTA	Moderate	High	Moderate

The system ensures data confidentiality by employing an efficient proxy re-encryption method, enhancing both performance and security.

Despite continuous research efforts over the past decade to enhance security, most of the currently available solutions are not feasible for FOTA updates schemes due to limitations in computing resources [30, 31]. Table 1 summarizes the key features and limitations of existing secure frameworks for FOTA and IoT, highlighting their varying focus on security, IoT suitability, and scalability.

Existing research has only partially tackled the issue of securely sharing IoT data, and the constraints of computing and power resources on IoT devices make it challenging to implement complex security algorithms. To address this, our proposed solution involves combining blockchain technology with a signcryption and proxy re-encryption scheme. This approach not only provides a secure trading platform but also ensures the safe transfer of data to the intended recipient

3. Preliminaries

This section briefly introduces essential prerequisites and Bilinear Map [32]

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two cyclic group , with the prime order $\mathbb{p}$ and the generator $\mathbb{g}$. A bilinear map is a function: $\Psi : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ that meets the properties:

1 Bilinearity: $\forall\ \mathfrak{a}, \mathfrak{b} \in \mathbb{Z}_p^*$ and $\forall\ \mathbb{g} \in \mathbb{G}$, we have: $\Psi(\mathbb{g}^{\mathfrak{a}}, \mathbb{g}^{\mathfrak{b}}) = \Psi\ (\mathbb{g}, \mathbb{g})^{\mathfrak{a}\mathfrak{b}}$

2 Non-degeneracy: For any non-zero $\mathfrak{a} \in \mathbb{G}$, $\Psi(\mathfrak{a}, \mathfrak{a}) \neq 1$

3 Computability: An efficient algorithm exists for computing $\Psi(\mathfrak{a}, \mathfrak{a})$, $\forall\ \mathfrak{a} \in \mathbb{G}$

4. System Overview

In this section, we describe the system model and outline the design objectives of our proposed BC-SC-PRE-FOTA system. Our explanation is based on Ethereum smart contracts and leverages immutable logs and trusted events. We specify a detailed description of the design of our proposed scheme, which directs to serve secure and immutable firmware updates to authentic vehicles.

Figure 1 shows the system model of our proposed system, which incorporates five main entities: the Vehicle Manufacturer (data owner), Firmware Update Center, Trusted Third Party (TTP), Vehicles (data users), and a blockchain platform with smart contracts.

Vehicle Manufacturer (data owner): The vehicle manufacturer is accountable for developing and releasing the vehicles. The firmware updates are also created by the manufacturer and sent to vehicles.

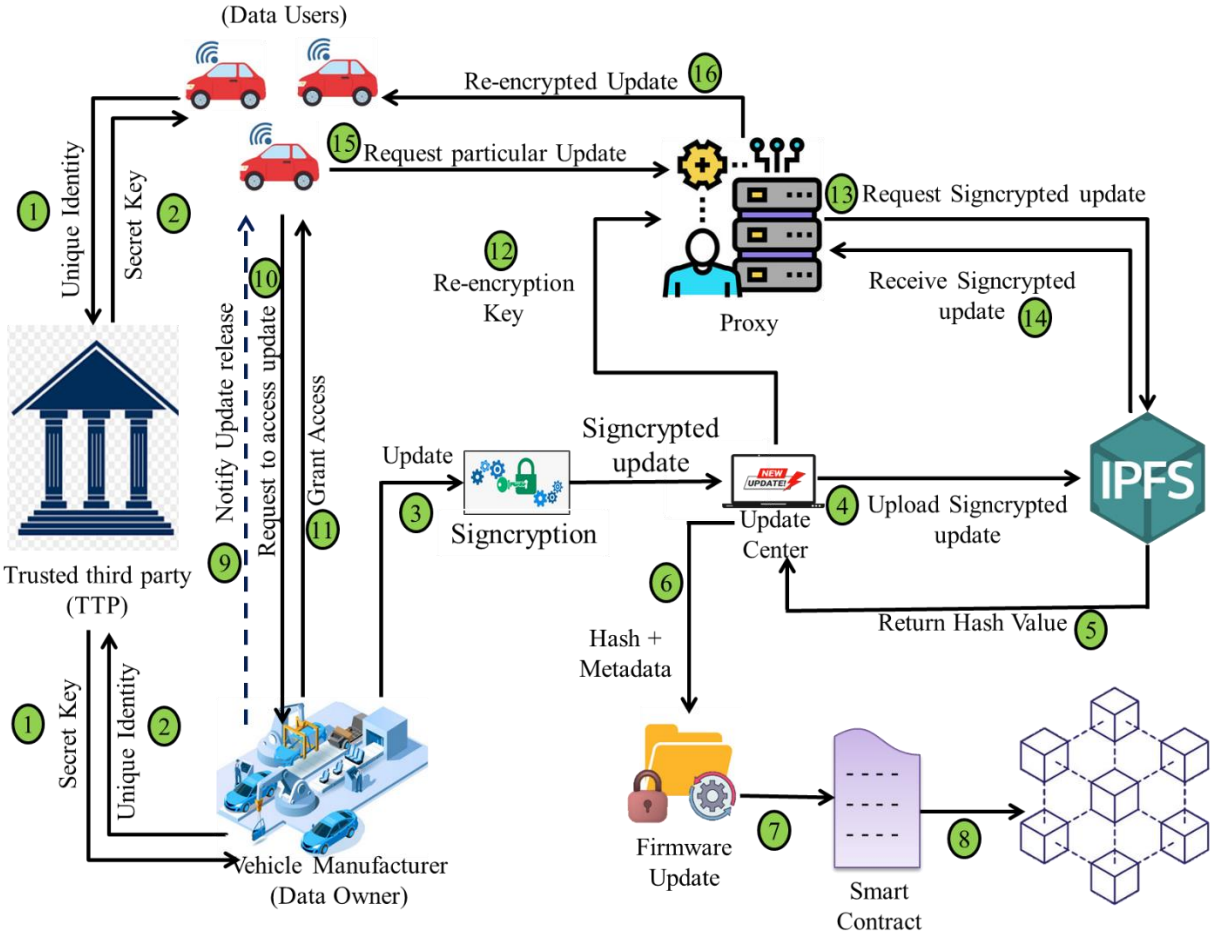

Figure 1. System model of proposed BC-SC-PRE-FOTA scheme

The manufacturer signcrypts and re-encrypts the firmware updates prior to communicating them to the planned vehicles.The Trusted Third Party (TT P) functions as a faithful body essential to the scheme operation. All sharing entities receive their secret keys from the TTP to ensure safe data communication and transfer operations. The system requires existence of Public Key Infrastructure (PKI) systems to ensure secure key management capabilities.

The vehicles which include Electronic Control Units (ECUs) function as data users who obtain firmware updates directly from the manufacturer. The vehicles can decrypt signcrypted and re-encrypted updates through their private key to perform successive updates.

The system operates on a public blockchain platform through which smart contracts become possible. The blockchain platform delivers a ciphertext matching service to securely exchange data between manufacturers who own the data and vehicles who use the data. The blockchain platform maintains a transparent and immutable record of all new firmware updates that it stores. Figure 1 represents the system model which connects these entities to distribute firmware updates securely and efficiently through signcryption and re-encryption along with blockchain-based smart contracts.

The proposed BC-SC-PRE-FOTA system incorporates several key functions to enable secure and efficient firmware update distribution. Here are the functions described step by step:

- Both manufacturers and vehicles register with the TTP, providing unique identity information. The TTP generates partial secret keys for each registered entity.
- A manufacturer uses signcryption to secure firmware updates by ensuring both confidentiality and integrity of the update before distribution. The firmware update center receives the signcrypted update after its transmission.
- The firmware update center stores the signcrypted update on Inter Planetary File System (IPFS) while it retrieves the matching hash value.
- The firmware update center establishes a smart contract on the blockchain to preserve update metadata by including hash values and essential metadata. The system triggers an event named "new update release" to reach this objective.
- The manufacturer adopts a process to inform vehicles about available new firmware updates.

The firmware update service allows vehicles to obtain access upon their request.

- The update center develops proxy re-encryption keys dedicated for each individual vehicle. After generation the proxy server receives the specific key.
- The proxy server obtains signcrypted updates from IPFS through its re-encryption and distribution process. The proxy server executes re-encryption through its possession of the proxy re-encryption key after receiving the update. After re-encryption the firmware update proceeds to its designated vehicle.
- The vehicle completes decryption followed by unsigncryption after receiving the re-encrypted update from the system. The operations enable access to the original update which lets the Electronic Control Unit (ECU) perform the installation.

By following these functions, the BC-SC-PRE-FOTA system ensures secure and controlled distribution of firmware updates to vehicles while leveraging blockchain, signcryption, and re-encryption techniques.

5. Formal model of BC-SC-PRE-FOTA scheme

A system consisting of seven algorithms forms the BC-SC-PRE-FOTA scheme to fulfill specific tasks within the framework. The system model presentation includes a formal depiction of this scheme as illustrated in Figure 2. The implementations through algorithms enable secure FOTA update procedures by maintaining both data integrity and confidentiality while executing the BC-SC-PRE-FOTA scheme efficiently. The notations used in the algorithms are summarized in Table 2.

Table 2. Notation and Symbol Definitions for the BC-SC-PRE-FOTA Scheme

Symbol	Description
$\mathcal{P}_{Pub}$	Public system parameters
$\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3$	Hash functions
$\mathbb{Z}_{p^*}$	Finite field of prime order p
$\mathbb{G}$, $\mathbb{G}_T$	Cyclic groups with prime order p
Ψ	Bilinear pairing
ℓ	Bit length of the message
μ	Master secret key (Msk)
M_{Pub}	Master public key
ID_M	Manufacturer's identity
Sk_M	Manufacturer's secret key
PK_M	Manufacturer's public key
F_U	Firmware update
ID_V	Vehicle's identity
Sk_V	Vehicle's secret key
PK_V	Vehicle's public key
$\oplus$	XOR operation
$\perp$	Invalid output symbol in case of failure

During the System Initilization Algorithm phase of the BC-SC-PRE-FOTA scheme the main goal is to establish essential parameters that will support the system functionality. The system generates accessible public parameters for complete participation by all entities that take part in the scheme. The trusted third party generates a master secret which remains known only to themselves during this phase. Public parameters together with the master secret serve essential functions to maintain both security and operational integrity of the BC-SC-PRE-FOTA scheme.

In the Key Extraction Algorithm, each user participating in the system sends their unique identity, denoted as ID_M, to the TTP. Subsequently, the secret key, represented as SK_M, is generated. The first part of this secret key, SK_{M1}, is computed and securely transmitted back to the user through a confidential communication channel. This process ensures that each user possesses their respective secret key necessary for secure operations within BC-SC-PRE-FOTA.

The Key Extraction Algorithm operates by enabling users to deliver their individual ID_M to the TTP which generates the secret key SK_M. During the next stage the system creates a secret key that is represented by SK_M. A confidential communication channel delivers the first portion of the secret key SK_{M1} to users after its computation. Secure operations within BC-SC-PRE-FOTA require users to gain their unique secret key through this process.

The Signcryption Algorithm is responsible for generating a first-level signcrypted firmware update, denoted as $F_{\sigma_{M\to Uc}}$ by utilizing public system parameters, the firmware update F_U, ID_M, Secret key of manufacturer M, $Sk_M = (Sk_{M1}, Sk_{M2})$. Additionally, the algorithm requires public key of manufacturer M $Pk_M = (Pk_{M1}, Pk_{M2})$ and update center Pk_{Uc} as a input, The resulting signcrypted firmware update is then securely transmitted to the intended receiver through a secure channel.

The Re-encryption Key Generation Algorithm generates the re-encryption key by using the Secret key $Sk_{Uc} = (Sk_{U1}, Sk_{U2})$ of the firmware update center with identity ID_{Uc} and Public key $Pk_V = (Pk_{V1}, Pk_{V2})$ of vehicle V as input and generates the re-encryption key $rk_{M\to V} = (rk_1, rk_2)$. The Re-encryption Algorithm is responsible for creating the re-encrypted firmware update $F_{\sigma_{M\to V}}$ using the first-level ciphertext (signcrypted update) $F_{\sigma_{M\to Uc}}$ and the re-encryption key $rk_{M\to V} = (rk_1, rk_2)$.

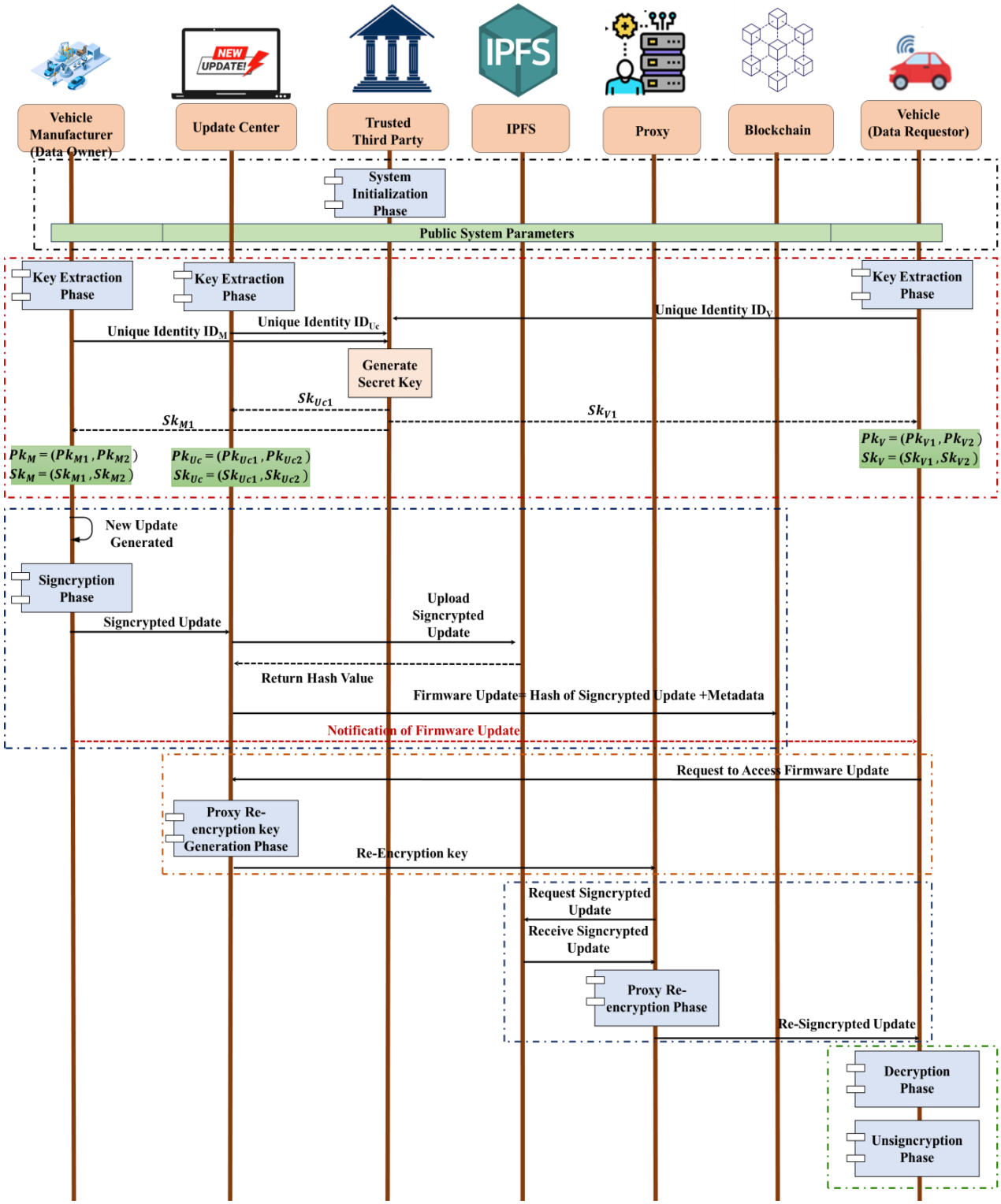

Figure 2. Process flow of proposed BC-SC-PRE-FOTA scheme

The Unsigncryption Algorithm is designed to handle the received signcrypted firmware update $F_{\sigma_{M\to Uc}}$, the receiver's private key Sk_{Uc}, the public keys of the manufacturer and update center $Pk_M = (Pk_{M1}, Pk_{M2})$ $Pk_{Uc} = (Pk_{Uc1}, Pk_{Uc2})$, respectively, and the identities of both the manufacturer and update center (ID_M and ID_{Uc}).Its purpose is to generate the original firmware update, if the signcrypted update has not been tampered with. If the signcrypted update has been tampered with, the algorithm returns the symbol ⊥ (denoting an error or invalid output).

The Decryption Algorithm is responsible for decrypting the signcrypted firmware update $F_{\sigma_{M\to V}}$ using the secret key Sk_V of the vehicle. Its purpose is to

output the original update F_U or an error if the decryption process encounters any issues.

5.1 Our Construction

5.1.1 System Initilization Algorithm $\{\wp \rightarrow \mathcal{P}_{Pub}\}$

The TTP carries out the step involving $\wp$ to produce the public system parameters ($\mathcal{P}_{Pub}$). Suppose we define the unidirectional hashing function as follows $\mathcal{H}_1$: $\{0,1\}^* \rightarrow \mathbb{Z}_{p^*}$, $\mathcal{H}_2$: $\{0,1\}^* \rightarrow \mathbb{G}$, and $\mathcal{H}_3$: $\{0,1\}^* \rightarrow \{0,1\}^{\ell}$. The Third party randomly selects $\mu \in_R \mathbb{Z}_{p^*}$ as the master secret key $M_{sk.}$ and compute the $M_{Pub} = \mu * g$. The TTP publish the $\mathcal{P}_{Pub}$ as {$\mathbb{G}$, $\mathbb{G}_T$, Ψ, ℓ ,M_{Pub},$\mathcal{H}_1$, $\mathcal{H}_2$, $\mathcal{H}_3$, g}The $M_{sk.}$, μ is kept secret, where ℓ is bit length of message.

Key Extraction Algorithm $\{\mathrm{ID_M} \rightarrow (Pk_M = (Pk_{M1}, Pk_{M2}),\ Sk_M = (Sk_{M1}, Sk_{M2}))\}$

The manufacturer M with identity $\mathrm{ID_M}$ randomly picks $Sk_{M2} = \vartheta_M \in_R \mathbb{Z}_{p^*}$ and computes the public key as $PK_{M1} = \vartheta_M * \mathcal{H}_1(ID_M)$ *and* $PK_{M2} = \vartheta_M * g$. Further the manufacturer sends its identity $\mathrm{ID_M}$ to TTP, the TTP then computes $SK_{M1} = \mu * \mathcal{H}_1(ID_M)$ and sends it to manufacturer M.

Signcryption Algorithm $\{\mathcal{P}_{Pub}, F_U, \mathrm{ID}_M, Sk_M, Pk_M, Pk_{Uc} \rightarrow F_{\sigma_{M\rightarrow Uc}}\}$

The user M with identity $\mathrm{ID_M}$ performs the following steps and generates the signcrypted firmware update $F_{\sigma_{M\rightarrow Uc}}$. It computes $F_{\sigma_1} = \alpha * \mathcal{H}_1(ID_M)$ whereas α is randomly selected from $\mathbb{Z}_{p^*}$. Further it computes T= $\vartheta_M * Pk_{Uc2}$ and U= Ψ $(SK_{M1}, PK_{Uc1})^{\alpha}$. Further it computes $F_{\sigma_2} = \beta \oplus \gamma$ *and* $F_{\sigma_3} = F_U \oplus \beta$, whereas $\beta = \mathcal{H}_2$ (T, U) and $\gamma = \mathcal{H}_2$ (T, U, $F_{\sigma_1}, PK_{M2}, \mathrm{ID_{Uc}}, PK_{Uc1}, PK_{Uc2}$). Then it generates the key Ќ = $\mathcal{H}_3$ ($F_{\sigma_1}, F_{\sigma_3}, F_U$) and computes F_{σ_4} = (α + Ќ) SK_{M1}. The signcrypted firmware update $F_{\sigma_{M\rightarrow Uc}}$ = $\{F_{\sigma_1}, F_{\sigma_2}, F_{\sigma_3} F_{\sigma_4}\}$ is uploaded to the IPFS.

Re-encryption Key Generation Algorithm $\{Sk_{Uc}, PK_V \rightarrow \mathrm{rk_{M\rightarrow V}}\}$

The firmware update center with identity ID_{Uc} will compute the re-encryption key $\mathrm{rk_{M\rightarrow V}}$=($\mathrm{rk_1}$, $\mathrm{rk_2}$). It first computes T= $\vartheta_{Uc} * Pk_{Uc2}$ and U= Ψ $(F_{\sigma_1}, \vartheta_{Uc} * SK_{Uc1})$. It then randomly choose $\alpha_1 \in_R \mathbb{Z}_{p^*}$, and computes the $\mathrm{rk_1}$= $\alpha_1 * \mathcal{H}_1(ID_{Uc})$. Further it computes $\gamma = \mathcal{H}_2$ (T, U, $F_{\sigma_1}, PK_{M2}, \mathrm{ID_{Uc}}, PK_{Uc1}, PK_{Uc2}$), T_1= $\vartheta_{Uc} * PK_{V2}$ and U_1= Ψ $(SK_{Uc1}, PK_{V1})^{\alpha_1}$. By using this T_1 and U_1, it further computes $\bar{\gamma} = \mathcal{H}_3$ (T_1 , $U_1, F_{\sigma_1}, \mathrm{rk_1}, PK_{V1}, PK_{V2}, \mathrm{ID_M}$). The second part of re-key is computed as $\mathrm{rk_2} = \gamma \oplus \bar{\gamma}$. The Re-key is $\mathrm{rk_{M\rightarrow V}}$ = ($\mathrm{rk_1}$, $\mathrm{rk_2}$). Finally the update center send the re-key to the proxy for re-encryption.

Re-encryption Algorithm $\{F_{\sigma_{M\rightarrow Uc}} = \{F_{\sigma_1}, F_{\sigma_2}, F_{\sigma_3} F_{\sigma_4}\}, \mathrm{rk_{M\rightarrow V}} \rightarrow F_{\sigma_{M\rightarrow V}}\}$

After receiving the $\mathrm{rk_{M\rightarrow V}}$ from the update center, the proxy server sends the request and receive the IPFS to get the first level signcrypted firmware update. The proxy then computes the re-encrpted firmware update $F_{\sigma_{M\rightarrow V}} = \{F_{\sigma_1}, F_{\sigma_2}', F_{\sigma_3}, F_{\sigma_4}, F_{\sigma_5}\}$, where as $F_{\sigma_2}' = F_{\sigma_2} \oplus \mathrm{rk_2}$ and $F_{\sigma_5} = \mathcal{H}_1(ID_V) + \mathrm{rk_1}$.

Unsigncryption Algorithm $\{\mathcal{P}_{Pub}, ID_M, Pk_M, F_{\sigma_{M\rightarrow Uc}}, Sk_{Uc}, Pk_{Uc} \rightarrow F_U \ or \ \perp\}$

The firmware update center with identity $\mathrm{ID_{Uc}}$ will download the signcrypted firmware update $F_{\sigma_{M\rightarrow Uc}}$ and perform the following operations to compute the original update F_U . It first computes T= $\vartheta_{Uc} * PK_{M2}$, U= Ψ $(F_{\sigma_1}, \vartheta_{Uc} * SK_{Uc1})$ and $\gamma = \mathcal{H}_2$ (T, U, $F_{\sigma_1}, PK_{M2}, \mathrm{ID_{Uc}}, PK_{Uc1}, PK_{Uc2}$). Further it computes β = $\mathcal{H}_2$ (T, U) and verify that $\gamma = \beta + F_{\sigma_2}$ if it holds then proceed to next step and generate the original firmware update F_U, else it returns ⊥. If the previous condition holds, it computes F_U= $F_{\sigma_3} \oplus \beta$ and Ќ = $\mathcal{H}_3$ ($F_{\sigma_1}, F_{\sigma_3}, F_U$) and verify if Ψ ($F_{\sigma_4}$, g) = Ψ ($F_{\sigma_1}$ + Ќ $\mathcal{H}_1(ID_M)$, M_{Pub}) holds…(1)

Decryption Algorithm $\{\mathcal{P}_{Pub}, F_{\sigma_{M\rightarrow V}}, Sk_V \rightarrow F_U\}$

The update requestor vehicle with identity $\mathrm{ID_V}$ after receiving the re-encrypted update $F_{\sigma_{M\rightarrow V}}$ from the proxy will calculate $\mathrm{rk_1}$= F_{σ_5}- $\mathcal{H}_1(ID_V)$, T_1=$\vartheta_{Uc} * PK_{V2}$ and U_1= Ψ $(\mathrm{rk_1}, \vartheta_V * Sk_{V1})$. Further it computes $\bar{\gamma} = \mathcal{H}_3$ (T_1, U_1, $F_{\sigma_1}, \mathrm{rk_1}, PK_{V1}, PK_{V2}, \mathrm{ID_M}$) and β = $F_{\sigma_2}' \oplus \bar{\gamma}$. The original firmware update can be computed as $F_U' = \beta \oplus F_{\sigma_3}$. For the verification of the computed firmware update, it further computes Ќ = $\mathcal{H}_3$ ($F_{\sigma_1}, F_{\sigma_3}, F_U'$) and verify if Ψ ($F_{\sigma_4}$, g) = Ψ ($F_{\sigma_1}$ + Ќ $\mathcal{H}_1(ID_M)$, M_{Pub}) holds.

5.2 Security Analysis

5.2.1 Proposition

The unsigncryptor ensures the correctness of the received signcrypted update. The unsigncryptor considers Ψ (F_{σ_4}, g) and Substitute F_{σ_4} =(α + Ќ) SK_{M1} to get Ψ ((α + Ќ) SK_{M1} , g). Now substitute $SK_{M1} = \mu * \mathcal{H}1(ID_M)$ to get Ψ ((α + Ќ) $\mu * \mathcal{H}1(ID_M)$, g) = Ψ ((α + Ќ) $\mathcal{H}1(ID_M), \mu * g$) = Ψ (($\alpha$ + Ќ) $\mathcal{H}1(ID_M), M_{Pub}$) where as M_{Pub} = $\mu * g$. Now Ψ (($\alpha * \mathcal{H}1(ID_M) + Ќ * \mathcal{H}1(ID_M), M_{Pub}$) = Ψ(F_{σ_1} + Ќ $* \mathcal{H}1(ID_M), M_{Pub}$), (∵ $\alpha * \mathcal{H}_1(ID_M) = F_{\sigma_1}$).

Hence Ψ (F_{σ_4}, g) = Ψ (F_{σ_1} + Ќ $\mathcal{H}_1(ID_M)$, M_{Pub}) is verified. The firmware update can now be computed as F_U= $F_{\sigma_3} \oplus \boldsymbol{\beta}$.

5.2.2. Proposition

Correctness for decryption of firmware update by the update center. The firmware update can be computed as F_U= $F_{\sigma_3} \oplus \boldsymbol{\beta}$ since T=$\vartheta_{Uc} * PK_{M2} = \vartheta_{Uc} *$

$\vartheta_M * g$, and U= Ψ $(F_{\sigma_1}, \vartheta_{Uc} * SK_{Uc1})$. Here we prove that U= Ψ $(SK_{M1}, PK_{Uc1})^{\alpha}$

Let us consider U= Ψ $(F_{\sigma_1}, \vartheta_{Uc} * SK_{Uc1})$, $Substitute\ F_{\sigma_1} = \alpha * \mathcal{H}_1(ID_M)$ = Ψ $(\alpha * \mathcal{H}_1(ID_M), \vartheta_{Uc} * SK_{Uc1})$, $Substitute\ SK_{Uc1} = \mu * \mathcal{H}_1(ID_{Uc})$

= Ψ $(\alpha * \mathcal{H}_1(ID_M), \vartheta_{Uc} * \mu * \mathcal{H}_1(ID_{Uc}))$ = Ψ $(\mu * \mathcal{H}1(ID_M), \vartheta_{Uc} * \mathcal{H}1(ID_{Uc}))^{\alpha}$, Substitute $\mu * \mathcal{H}1(ID_M) = SK_{M1}$ and $\vartheta_{Uc} * \mathcal{H}1(ID_{Uc}) = PK_{Uc1}$ = Ψ $(SK_{M1}, PK_{Uc1})^{\alpha}$ = U, Hence proved

5.2.3 Proposition

Correctness of decryption of firmware update for vehicle V.

The vehicle V can get a firmware update $F_U{}' = \beta \oplus F_{\sigma_3}$ since $T_1 = \vartheta_{Uc} * PK_{V2}$, U_1= Ψ $(rk_1, \vartheta_V * Sk_{V1})$and $\beta = F_{\sigma_2}{}' \oplus \bar{\gamma}$. We show that $\beta = F_{\sigma_2}{}' \oplus \bar{\gamma}$ because the correctness of $T_1 = \vartheta_{Uc} * PK_{V2}$, U_1= Ψ $(rk_1, \vartheta_V * Sk_{V1})$ is same as that of $T = \vartheta_{Uc} * PK_{M2}$ and U= Ψ $(F_{\sigma_1}, \vartheta_{Uc} * SK_{Uc1})$.

$\beta = F_{\sigma_2}{}' \oplus \bar{\gamma}$, Substitute $F_{\sigma_2}{}' = F_{\sigma_2} \oplus rk_2$ and $rk_2 = \gamma \oplus \bar{\gamma} = F_{\sigma_2} \oplus rk_2 \oplus rk2 \oplus \gamma = F_{\sigma_2} \oplus \gamma$

6. Simulation Study

The AVISPA tool is used to simulate the ECC-IBASC-MIoT scheme, utilizing HLPSL (High-Level Protocol Specification Language) to model security protocols. HLPSL, based on process algebraic notation, defines protocol roles and message exchanges [33-34]. AVISPA then generates attack scenarios and verifies security through model checking and simulations.

Our setup runs SPAN (Security Protocol Animator) on Oracle VM VirtualBox [35]. AVISPA employs four verification back-ends: CL-AtSe, OFMC, TA4SP, and SATMC, with OFMC and CL-AtSe validating our scheme [36-37]. The Attack Validation and Demonstration Console simulates adversaries intercepting and replaying messages. If the protocol resists MITM and replay attacks, the system returns a "SAFE" status. Otherwise, OFMC provides an attack trace. CL-AtSe detects vulnerabilities faster due to its optimized computations.

7. Experimental Evaluation

7.1 Computation cost Analysis

To evaluate the efficiency of our proposed BC-SC-PRE-FOTA scheme, we compared its performance with existing signcryption and proxy re-encryption (PRE) schemes. The comparison focuses on three key cryptographic operations: pairing operations($\mathcal{P}$), Scalar multiplication operation ($\mathcal{M}$) and, exponentiation operatio ($\mathcal{E}$). The results of this comparison are summarized in Table 2. The execution time for each cryptographic operation, as reported is as follows:

- Pairing operation ($\mathcal{P}$): 3.1504 ms
- Scalar multiplication ($\mathcal{M}$): 0.4623 ms
- Exponentiation ($\mathcal{E}$): 1.6513 ms

To assess computational efficiency, we apply a straightforward time estimation method. For instance, the scheme proposed by Chandrasekar S. [37] requires 14P and 6M operations operations. Using the above execution times, the total computational cost for this scheme amounts to 46.879 ms. similarly, the computation time for each evaluated scheme is calculated and presented in Table 3. It is evident that our proposed BC-SC-PRE-FOTA scheme achieves superior performance compared to existing approaches.

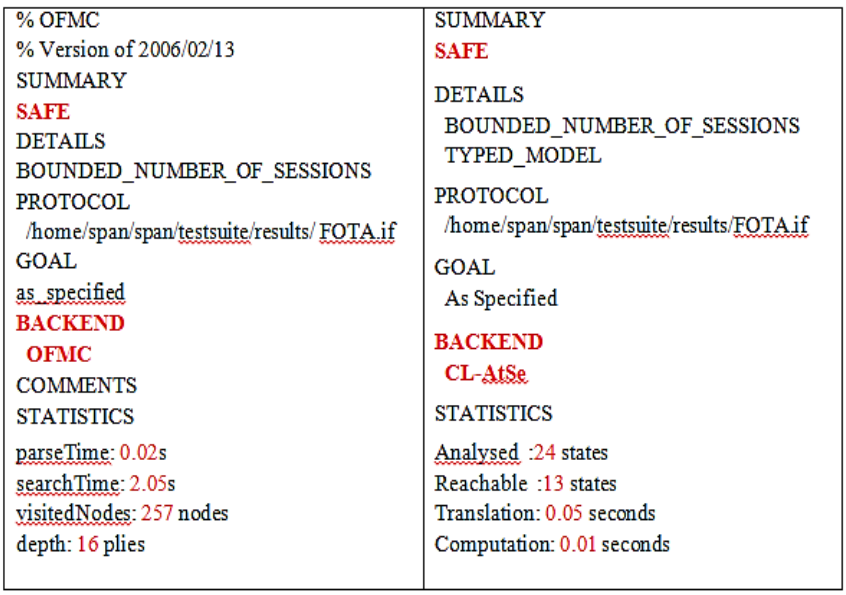

Figure 3. AVISPA output with OFMC and CL-AtSe backends

Table 2. Comparison of various Schemes Computation Operations

Scheme	Signcryption	Proxy Key Generation	Re-encryption	Unsigncryption	Decryption	Total
Chandrasekar. S [37]	1 $\mathcal{P}$ +4$\mathcal{M}$	1 $\mathcal{P}$	3 $\mathcal{P}$	5 $\mathcal{P}$+1$\mathcal{M}$	4 $\mathcal{P}$+1$\mathcal{M}$	14 $\mathcal{P}$+6$\mathcal{M}$
Li. F [38]	1$\mathcal{P}$ +2$\mathcal{M}$ +1$\mathcal{E}$	1$\mathcal{M}$	1$\mathcal{M}$	3 $\mathcal{P}$+1$\mathcal{M}$	4 $\mathcal{P}$+1$\mathcal{M}$	8$\mathcal{P}$+6M+1$\mathcal{E}$
BC-SC-PRE-FOTA	1 $\mathcal{P}$ +3$\mathcal{M}$	2 $\mathcal{P}$+3$\mathcal{M}$	1 $\mathcal{P}$+1$\mathcal{M}$	1 $\mathcal{P}$+2$\mathcal{M}$	1 $\mathcal{P}$+2$\mathcal{M}$	6 $\mathcal{P}$+11$\mathcal{M}$

Table 3. Computation cost comparison of various Schemes

Scheme	Signcryption	Proxy Key Generation	Re-encryption	Unsigncryption	Decryption	Total
Chandrasekar. S [37]	5.000	3.150	9.451	16.214	13.064	46.879
Li. F [38]	5.726	0.462	0.462	9.914	13.064	29.628
BC-SC-PRE-FOTA	4.537	7.688	3.613	4.075	4.075	23.988

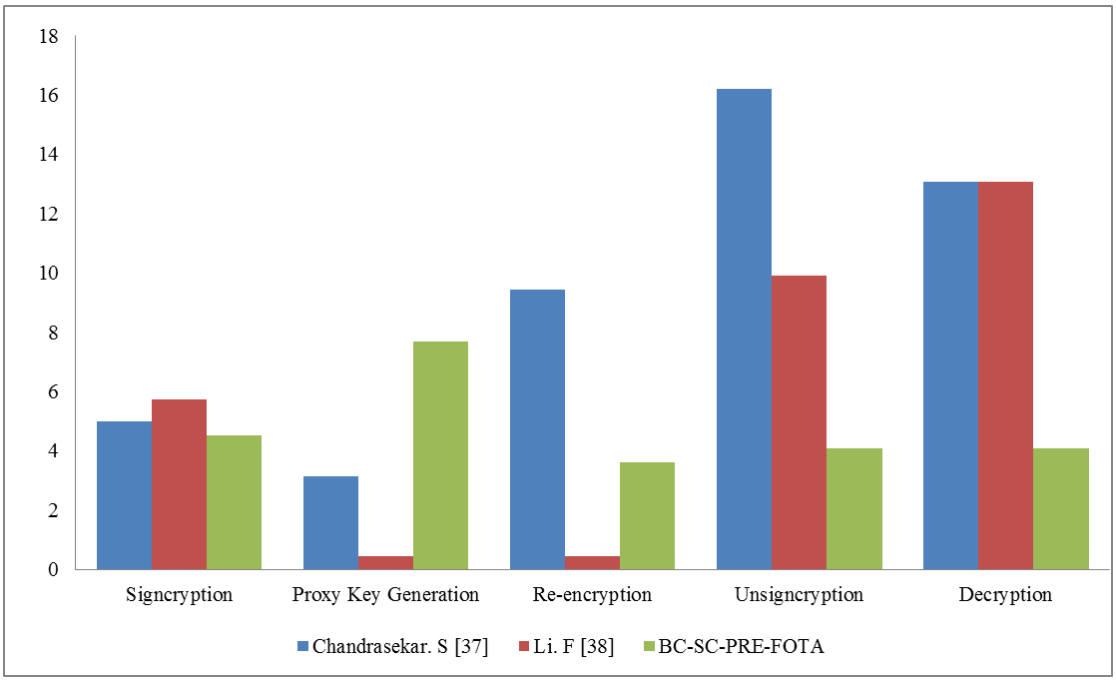

Figure 4. Comparison of computation cost with proposed scheme

A graphical representation of the computational cost, measured in milliseconds (ms) for each phase, is provided in Figure 4. As shown in Table 3 and Figure 4, the proposed BC-SC-PRE-FOTA scheme achieves the lowest total computational cost (23.988 ms), outperforming Chandrasekar *et al.* [37] by approximately 48.8% and Li et al. [39] by 19.0%. This efficiency gain is primarily due to the reduced number of expensive pairing operations and the optimization of scalar multiplications. Unlike prior approaches that rely heavily on pairing operations in multiple phases, our design strategically shifts complexity to less costly operations (e.g., $\mathcal{M}$), which are faster and more scalable for resource-constrained environments such as FOTA updates in IoT systems.

Moreover, the integration of signcryption and proxy re-encryption in our scheme reduces redundancy and ensures that cryptographic transformations are efficiently cascaded. This contributes to the lower

computational latency observed across all operational phases.

7.2 Communication cost Analysis

The additional number of bits sent along with the original message constitutes communication overhead. We carried out performance evaluation of the BC-SC-PRE-FOTA scheme by assessing its communication overhead against the approaches presented by Chandrasekar S. [37] and Li F. [38]. We evaluated the parameters by using a 1024-bit sized bilinear pairing element (|$\mathbb{G}$|) along with 512-bit hashing and 100-bit message (|$\mathcal{M}$ |) size. The communication cost of BC-SC-PRE-FOTA amounts to 1 $\mathcal{M}$ +1$\mathbb{G}$+2$\mathcal{H}$ under the established assumptions. Data transmission efficiency of the proposed scheme shows significant enhancement in comparison to the solutions presented in [38, 39] (Tables 4). The visual illustration in Figure 5 shows this improvement.

The communication overhead, summarized in Table 4, demonstrates that BC-SC-PRE-FOTA significantly reduces the number of bits transmitted, especially in the proxy signcryption phase. For instance, our scheme transmits only 2048 bits compared to 3272 bits in [38] and 2148 bits in [39], representing a 37.4% and 4.6% reduction respectively. These improvements are crucial for bandwidth-limited or intermittently connected environments.

The compactness of our cryptographic payload is achieved by minimizing the size and number of cryptographic elements, including ciphertext components and proxy keys. This design choice directly impacts communication efficiency and makes our scheme suitable for real-time or constrained deployments. Compared to recent works such as [40] which still incur higher overhead during delegation, BC-SC-PRE-FOTA offers a more communication-efficient protocol while preserving security guarantees.

8. Future Research Directions

Future research and practical implementations of the BC-SC-PRE-FOTA scheme could explore several promising directions to further enhance its applicability and effectiveness. One key area is expanding scalability to support a wide variety of IoT devices with differing resource constraints. This could be achieved through hierarchical blockchain models or edge-based frameworks. Additionally, integrating quantum-safe cryptographic techniques, such as lattice-based cryptography, can ensure protection against potential threats from quantum computing advancements. Another significant aspect involves testing the scheme in real-world scenarios [40]. Deploying prototypes in operational vehicles will provide insights into its performance under dynamic conditions, including challenges related to latency and network disruptions.

Table 4. Communication Cost comparison

Scheme	Proxy Delegation	Proxy Delegation (Bits)	Proxy signcryption	Proxy signcryption (Bits)	Total
Chandrasekar. S [37]	1 $\mathcal{M}$ +2$\mathbb{G}$	2148	2 $\mathcal{M}$ +3$\mathbb{G}$	3272	3 $\mathcal{M}$ +5$\mathbb{G}$
Li. F [38]	1 $\mathcal{M}$+1G	1124	1 $\mathcal{M}$ +1$\mathbb{G}$+2$\mathcal{H}$	2148	4 $\mathcal{M}$ +1$\mathbb{G}$+3$\mathcal{H}$
BC-SC-PRE-FOTA	3 $\mathcal{M}$ +1$\mathcal{H}$	812	1$\mathbb{G}$+2$\mathcal{H}$	2048	1$\mathcal{M}$ +1$\mathbb{G}$+2$\mathcal{H}$

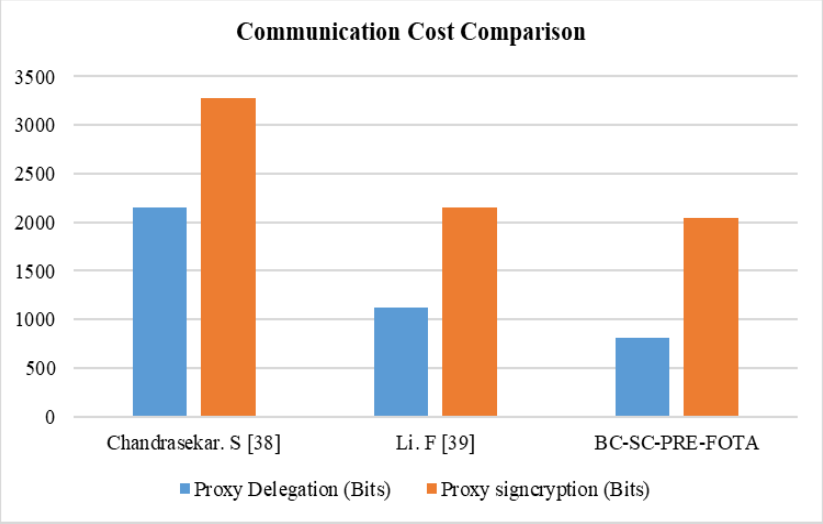

Figure 5. Comparison of communication cost with proposed scheme

Adapting the framework for cross-sector applications is another avenue for future research. Secure wireless updates could be applied to sectors like healthcare devices, industrial IoT systems, and smart city technologies. Incorporating artificial intelligence can further optimize the firmware update process, providing capabilities such as anomaly detection and efficient resource management. Additionally, improving energy efficiency will be essential for making updates feasible in devices with limited power supplies, particularly those operating in remote locations or using batteries. Through these advancements, the BC-SC-PRE-FOTA scheme can achieve greater scalability, adaptability, and security, significantly broadening its practical applications.

9. Conclusion

This study reveals crucial weaknesses in modern connected vehicles stemming from wireless firmware updates because they allow attackers to endanger both drivers' safety and passengers' safety. The combination of blockchain technology alongside signcryption and proxy re-encryption serves as a new method to create safe communication between vehicles and manufacturers while reducing security risks. Using IPFS technology allows firmware updates to reach authorized vehicles safely as it strengthens the entire update security framework. The proposed scheme strengthens both confidentiality and integrity levels in the firmware update procedure. Security practitioners performed thorough analysis which confirmed that cryptographic operations implemented in the scheme work correctly and provide effective security. A simulation analysis conducted with AVISPA confirmed the security and robustness of the proposed techniques through its implementation of OFMC and Cl-AtSe models. This research develops an effective solution to handle vehicle firmware update vulnerabilities by implementing security measures which protect both data integrity and confidentiality throughout the update procedure. The proposed scheme requires additional research to advance performance and extent its application but also needs examination of defensive measures against new security risks affecting connected vehicles and firmware updates.

References

[1] P. Dakić, I. Stupavský, V. Todorović, The effects of global market changes on automotive manufacturing and embedded software. Sustainability, 16(12), (2024) 4926. https://doi.org/10.3390/su16124926

[2] F. Vapiwala, D. Pandita, H. Choudhury, (2023) Strategies for digital innovation in talent management of Automotive Industry 4.0. 2023 8th International Conference on Business and Industrial Research (ICBIR), 200-205, IEEE, Thailand. https://doi.org/10.1109/ICBIR57571.2023.10147499

[3] V. Agarwal, A. Z. Hameed, S. Malhotra, K. Mathiyazhagan, S. Alathur, A. Appolloni, Role of Industry 4.0 in agile manufacturing to achieve sustainable development. Business Strategy and the Environment, 32(6), (2023) 3671-3688. https://doi.org/10.1002/bse.3321

[4] S. Wasnik, R. Venkatesh, (2022) Understanding usage of IoT applications and its impact on consumer decision-making in Indian automobile industry. 2022 International Conference on Decision Aid Sciences and Applications (DASA), IEEE, Thailand. https://doi.org/10.1109/DASA54658.2022.9765216

[5] A.N. Brooks, (2002) Vehicle-to-grid demonstration project: Grid regulation ancillary service with a battery electric vehicle.

[6] S. Jafarnejad, L. Codeca, W. Bronzi, R. Frank, T. Engel, (2015) A car hacking experiment: When connectivity meets vulnerability. 2015 IEEE Globecom Workshops (GC Wkshps). IEEE, USA. https://doi.org/10.1109/GLOCOMW.2015.7413993

[7] J. Eriksson, H. Balakrishnan, S. Madden, Cabernet: Vehicular content delivery using WiFi. Proceedings of the 14th ACM International Conference on Mobile Computing and Networking, (2008) 199-210. https://doi.org/10.1145/1409944.1409968

[8] G. Shi, Z. Ke, F. Yan, J. Hu, W. Yin, Y. Jin, (2015) A vehicle electric control unit over-the-air reprogramming system. 2015 International Conference on Connected Vehicles and Expo (ICCVE), IEEE, China. https://doi.org/10.1109/ICCVE.2015.21

[9] S. Acharya, Y. Dvorkin, H. Pandžić, R. Karri, Cybersecurity of smart electric vehicle charging: A power grid perspective. IEEE Access, 8, (2020) 214434-214453. https://doi.org/10.1109/ACCESS.2020.3041074

[10] G. Kim, I.Y. Jung, Integrity assurance of OTA software update in smart vehicles. International Journal on Smart Sensing and Intelligent Systems, 12(1), (2019) 1-8. https://doi.org/10.21307/ijssis-2019-011

[11] L.B. Othmane, H. Weffers, M.M. Mohamad, M. Wolf, A survey of security and privacy in connected vehicles. Wireless Sensor and Mobile Ad-Hoc Networks: Vehicular and Space Applications, (2015) 217-247. https://doi.org/10.1007/978-1-4939-2468-4_10

[12] T. Mirfakhraie, G. Vitor, K. Grogan, (2018) Applicable protocol for updating firmware of automotive HVAC electronic control units (ECUs)

over the air. 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, Canada. https://doi.org/10.1109/Cybermatics_2018.2018.00038

[13] B.A. Mohammed, M.A. Al-Shareeda, S. Manickam, Z.G. Al-Mekhlafi, A. Alreshidi, M. Alazmi, J. S. Alshudukhi, M. Alsaffar, FC-PA: Fog computing-based pseudonym authentication scheme in 5G-enabled vehicular networks. IEEE Access, 11, (2023) 18571-18581. https://doi.org/10.1109/ACCESS.2023.3247222

[14] Z.G. Al-Mekhlafi, M.A. Al-Shareeda, S. Manickam, B.A. Mohammed, A. Qtaish, Lattice-based lightweight quantum-resistant scheme in 5G-enabled vehicular networks. Mathematics, 11(2), (2023) 399. https://doi.org/10.3390/math11020399

[15] A.S. Thangarajan, M. Ammar, B. Crispo, D. Hughes, (2019) Towards bridging the gap between modern and legacy automotive ECUs: A software-based security framework for legacy ECUs. 2019 IEEE 2nd Connected and Automated Vehicles Symposium (CAVS), IEEE, USA. https://doi.org/10.1109/CAVS.2019.8887788

[16] J. Deng, L. Yu, Y. Fu, O. Hambolu, R.R. Brooks, Security and data privacy of modern automobiles. Data Analytics for Intelligent Transportation Systems, (2017) 131-163. https://doi.org/10.1016/B978-0-12-809715-1.00006-7

[17] T. Karthik, A. Brown, S. Awwad, D. McCoy, R. Bielawski, C. Mott, S. Lauzon, A. Weimerskirch, J. Cappos, Uptane: Securing software updates for automobiles. International Conference on Embedded Security in Car, (2016) 1-11.

[18] M. Baza, M. Nabil, N. Lasla, K. Fidan, M. Mahmoud, M. Abdallah, (2019) Blockchain-based firmware update scheme tailored for autonomous vehicles. IEEE Wireless Communications and Networking Conference (WCNC), IEEE, Morocco. https://doi.org/10.1109/WCNC.2019.8885769

[19] D.K. Nilsson, U.E. Larson, (2008) Secure firmware updates over the air in intelligent vehicles. ICC Workshops - 2008 IEEE International Conference on Communications Workshops, IEEE, China. https://doi.org/10.1109/ICCW.2008.78

[20] Z.G. Al-Mekhlafi, M.A. Al-Shareeda, S. Manickam, B.A. Mohammed, A. Alreshidi, M. Alazmi, J. S. Alshudukhi, M. Alsaffar, A. Alsewari, Chebyshev polynomial-based fog computing scheme supporting pseudonym revocation for 5G-enabled vehicular networks. Electronics, 12(4), (2023) 872. https://doi.org/10.3390/electronics12040872

[21] M.A. Al-Shareeda, S. Manickam, COVID-19 vehicle based on an efficient mutual authentication scheme for 5G-enabled vehicular fog computing. International Journal of Environmental Research and Public Health, 19(23), (2022) 15618. https://doi.org/10.3390/ijerph192315618

[22] B.A. Mohammed, M.A. Al-Shareeda, S. Manickam, Z.G. Al-Mekhlafi, A.M. Alayba, A.A. Sallam, Anaa-Fog: A novel anonymous authentication scheme for 5G-enabled vehicular fog computing. Mathematics, 11(6), (2023) 1446. https://doi.org/10.3390/math11061446

[23] M. Steger, A. Dorri, S. S. Kanhere, K. Römer, R. Jurdak, M. Karner, Secure wireless automotive software updates using blockchains: A proof of concept. Advanced Microsystems for Automotive Applications 2017: Smart Systems Transforming the Automobile, Springer International Publishing, (2018) 137-149. https://doi.org/10.1007/978-3-319-66972-4_12

[24] D.K. Nilsson, L. Sun, T. Nakajima, (2008) A framework for self-verification of firmware updates over the air in vehicle ECUs. IEEE Globecom Workshops, IEEE, USA. https://doi.org/10.1109/GLOCOMW.2008.ECP.56

[25] A.A. Almazroi, M. A. Alqarni, M.A. Al-Shareeda, M.H. Alkinani, A.A. Almazroey, T. Gaber, FCA-VBN: Fog computing-based authentication scheme for 5G-assisted vehicular blockchain network. Internet of Things, 25, (2024)101096. https://doi.org/10.1016/j.iot.2024.101096

[26] A.A. Almazroi, E.A. Aldhahri, M.A. Al-Shareeda, S. Manickam, ECA-VFog: An efficient certificateless authentication scheme for 5G-assisted vehicular fog computing. PLoS One, 18(6), (2023) e0287291. https://doi.org/10.1371/journal.pone.0287291

[27] V. Kirtane, C.P. Rangan, RSA-TBOS signcryption with proxy re-encryption. Proceedings of the 8th ACM Workshop on Digital Rights Management, (2008) 59-66. https://doi.org/10.1145/1456520.1456531

[28] E. Ahene, J. Walker, R.M.O.M. Gyening, G. Abdul-Salaam, J.B. Hayfron-Acquah, Heterogeneous signcryption with proxy re-encryption and its application in EHR systems. Telecommunication Systems, 80(1), (2022) 59-75. https://doi.org/10.1007/s11235-022-00886-2

[29] B.S. Rawal, G. Manogaran, M. Hamdi, Multi-tier stack of blockchain with proxy re-encryption method scheme on the Internet of Things platform. ACM Transactions on Internet Technology (TOIT), 22(2), (2021) 1-20. https://doi.org/10.1145/3421508

[30] S. Hussain, I. Ullah, H. Khattak, M. Adnan, S. Kumari, S.S. Ullah, M.A. Khan, S.J. Khattak, A lightweight and formally secure certificate-based signcryption with proxy re-encryption (CBSRE) for Internet of Things enabled smart grid. IEEE Access, 8, (2020) 93230-93248. https://doi.org/10.1109/ACCESS.2020.2994988

[31] A. Manzoor, M. Liyanage, A. Braeke, S.S. Kanhere, M. Ylianttila, (2019) Blockchain-based proxy re-encryption scheme for secure IoT data sharing. 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), IEEE, Korea (South). https://doi.org/10.1109/BLOC.2019.8751336

[32] P.R. Yogesh, R. Devane Satish, Formal verification of secure evidence collection protocol using BAN logic and AVISPA. Procedia Computer Science, 167, (2020) 1334-1344. https://doi.org/10.1016/j.procs.2020.03.449

[33] R.Y. Patil, S.R. Devane, Network forensic investigation protocol to identify true origin of cyber crime. Journal of King Saud University-Computer and Information Sciences, 34(5), (2022) 2031-2044. https://doi.org/10.1016/j.jksuci.2019.11.016

[34] P.R. Yogesh, Backtracking tool root-tracker to identify true source of cyber crime. Procedia Computer Science, 171, (2020) 1120-1128. https://doi.org/10.1016/j.procs.2020.04.120

[35] Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuéllar, P. H. Drielsma, P. C. Héam, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, L. Vigneron, The AVISPA tool for the automated validation of internet security protocols and applications. Computer Aided Verification 17th International Conference, CAV 2005, 17, (2005) 281-285. https://doi.org/10.1007/11513988_27

[36] Y. Belfaik, Y. Lotfi, Y. Sadqi, S. Safi, A comparative study of protocols' security verification tools: AVISPA, Scyther, ProVerif, and Tamarin. International Conference on Digital Technologies and Applications, (2024) 118-128. https://doi.org/10.1007/978-3-031-68653-5_12

[37] S. Chandrasekar, K. Ambika, C. P. Rangan, Signcryption with proxy re-encryption. IACR Cryptol. ePrint Archive, (2008) 276.

[38] F. Li, B. Liu, J. Hong, An efficient signcryption for data access control in cloud computing. Computing. Computing, 99(5), (2017) 465. https://doi.org/10.1007/s00607-017-0548-7

[39] A. Obiri, A.A. Addobea, E. Affum, J. Ankamah, A.K. Kwansah Ansah, A certificateless signcryption with proxy-encryption for securing agricultural data in the cloud. Journal of Computer Security, 32(2), (2024) 77-115. https://doi.org/10.3233/JCS-220107

[40] P.N. Bathula, M. Sreenivasulu, A blockchain enabled proxy re-encryption framework for secure and low latency data sharing in fog based IoT networks. Journal of Information Systems Engineering and Management, 10(13s), (2025). https://doi.org/10.52783/jisem.v10i13s.2059

Authors Contribution Statement

Rachana Y. Patil: Conceptualization, Methodology, Formal analysis, Data curation, Writing Original Draft. Yogesh H. Patil: Conceptualization, Methodology, Formal analysis, Data curation, Writing Original Draft. Deepali Naik: Data curation, Visualization. Rupali Gangarde: Formal analysis, Data curation. Aparna Joshi: Writing, review & editing. Aparna Bannore: Writing, review & editing. All the authors read and approved the final version of the manuscript.

Funding

The authors declare that no funds, grants or any other support were received during the preparation of this manuscript.

Competing Interests

The authors declare that there are no conflicts of interest regarding the publication of this manuscript.

Data Availability

The data supporting the findings of this study can be obtained from the corresponding author upon reasonable request.

Has this article screened for similarity?

Yes

About the License