RESEARCH **Open Access**

A service-categorized security scheme with physical unclonable functions for internet of vehicles

Nadhir Ben Halima[1], Ala Saleh Alluhaidan[2*], Mohammad Zunnun Khan[3,4], Mohd Shahid Husain[5] and Mohammad Ayoub Khan[3]

*Correspondence: asalluhaidan@pnu.edu.sa

[1] Department of Information Technology, Community College of Qatar, 7344 Doha, Qatar
[2] Department of Information Systems, College of Computer and Information Science, Princess Nourah Bint Abdulrahman University, Riyadh, P.O. Box 84428, 11671, Saudi Arabia
[3] College of Computing and Information Technology, University of Bisha, Bisha 67714, Saudi Arabia
[4] Department of Computer Science & Engineering, Integral University, Lucknow 226026, India
[5] College of Computing and Information Sciences, University of Technology and Applied Sciences, Ibri, Sultanate of Oman

Abstract

In smart cities, communication and information exchange for the Internet of Vehicles rely on open and closed infrastructures along the roadside. Secure communications rely on the sender and receiver devices having self-sustaining authentication methods. The perquisites of the authentication methods are to grip communication without being falsified by an adversary or unidentified third parties. This article introduces the Service-Categorized Security Scheme (SCSS) with a physically unclonable function (PUF) for handling sensitive guidance/communication information. The vehicle-side authentication, access control, and service demands are governed using service-based PUF factors such as digital signatures, passwords, etc. To prevent anonymous third parties and adversaries, the PUF operates over compromised and uncompromised communication devices. Device-specific keys generated by PUFs based on intrinsic physical variances help identify between compromised and uncompromised devices, while keys generated by uncompromised devices conform to their expected profiles In the service-sharing process, mutual authentication using synchronized keys is used for security and service verification. The synchronized keys are integrated with the PUF for monitoring de-synchronization and individual operation. This decision is made using federated learning from the external service provider and the communicator of the vehicle. Through the learning process, a de-synchronization occurrence at the service provider and vehicle is identified as the reason for disconnecting the session. As a result, any suspicious activity that contradicts service security is identified, and the information of the communicating vehicle is secured. The proposed scheme is analyzed using the metrics authentication time, adversary detection ratio, complexity, de-synchronization time, and successful sessions.

Keywords: PUF, IoV, Federated learning

Introduction

Internet of Vehicles (IoV) connects vehicles via the internet, which provides certain services to the users. IoV identifies exact patterns, traffic flow, and routes for users, reducing unwanted accidents and delays in reaching a specific location. Ensuring service security is an important task to perform in IoV [1]. Every vehicle is connected, which shares data from one user to another. Various problems, such as data loss, mishandling, and threats, occur during communication and interaction processes [2]. Proper authentication policies and techniques are provided to users, which ensure their safety from attackers. An effective decentralized authentication scheme is used for IoV. A consensus algorithm based on blockchain technology is used in a decentralized authentication scheme [3]. The actual behaviors of individuals and the data sharing process are analyzed, yielding useful data for security policies. The decentralized scheme improves performance and reduces malicious attacks in IoV. An efficient authentication scheme over blockchain (EASBF) is also used for ensuring the safety of users in IoV systems. EASBF schemes exchange critical keys required for authentication, reducing the complexity of service-providing systems. EASBF identifies attacks and their causes that occur during interaction services. EASBF improves the security and privacy level of users from third-party members [4, 5].

Physically Unclonable Functions (PUF) is one-of-a-kind physical entities that serve as fortresses against unauthorized access are at the center of IoV service security. The PUF-based protocols and policies are used for IoV service security systems [6]. PUF is a hardware fingerprint generator that generates fingerprints for users. PUF provides relevant information during authentication and authorization processes. A two-factor authentication protocol based on PUF is widely used to ensure user safety from attackers [7]. PUF identifies the actual fingerprint details of users, which produce the necessary data for the authentication process. PUF reduces the error ratio in authentication, ‘ensuring user data is protected from third-party members [8]. An authentication and key exchange (AKE) protocol using PUF is also used for IoV networks. The AKE protocol eliminates unwanted data and noises that are presented in fingerprints. PUF detects precise fingerprint details, reducing latency and energy consumption in the authentication process. Security measures include both PUFs and traditional keys. PUFs provide safe device authentication with cryptographic keys generated from hardware variants. However, physical keys protect software and communicate sensitive data securely by generating cryptographic keys using mathematical techniques. During authentication processes, the AKE protocol ensures user safety and privacy. The AKE protocol increases the energy-efficiency range of IoV by providing proper service security schemes to the users [9, 10].

The Internet of Vehicles (IoV) requires mutual authentication methods and schemes. During communication and interaction processes, the mutual authentication protocol provides users a wide range of services. A lightweight mutual authentication protocol is used for IoV [11]. The lightweight properties hold the actual data required for the authentication process [12]. The mutual authentication protocol is commonly used for vehicle-to-vehicle (V2V) communication services [13]. Users are given secret keys to use during the authentication process, which protects their data from hackers. Private keys and details are detected during the authentication process, increasing the accuracy of protecting data from attackers. Private keys and details are detected for the authentication process, increasing the accuracy in ensuring data from the attackers.

The blockchain-based mutual authentication scheme is used for IoV, which detects false intrusions over vehicles [14]. Blockchain technology identifies characteristics and patterns for authentication and authorization, reducing the range of false intrusions in

IoV. The blockchain-based protocol achieves high security and safety, allowing users to access useful services [15].

IoV network performance and responsiveness may suffer due to computational load. Different consensus procedures, such as proof of authority or delegated proof of stake, network partitioning, off-chain solutions, sidechains or state channels, and privacy safeguards, such as zero-knowledge proofs, are all viable options. These adjustments can lessen the burden on computers, make systems more scalable, and ease the strain on networks. These ideas, when implemented, can improve network speed and safety.

PUF, two-factor authentication (2FA), authentication and key exchange (AKE), and mutual authentication are all essential for the security of IoV systems. In addition to improving data security, the one-of-a-kind fingerprints produced by PUFs help lower error rates. For Two-Factor Authentication, you'll need both a password and a fingerprint obtained by a PUF. Due to its ability to filter out redundant information and noise, AKE protocols boost power savings and safety. Mutual authentication offers secret keys to safeguard information, while blockchain-based techniques improve data safety. The efforts of this study take place against the backdrop of this extensive array of security devices. This study introduces a new method using the PUF concept. It is a service security technique that provides unambiguous authentication of V2V and V2I communications. The areas of mutual authentication, synchronization, and de-synchronization are all areas where we have made a significant contribution. In addition, we investigate using federated learning to minimize communication disruptions and spot suspicious cars.

The IoV is a developing field that could significantly improve our daily commutes by providing services like traffic monitoring, route optimization, and instantaneous information sharing. However, the trustworthiness and safety of these services is a significant issue. Data loss, improper management, and malicious attacks are possible outcomes for any IoV system, including vehicles, users, or infrastructure elements. Many security protocols have been designed to improve the reliability and safety of IoV systems in response to these threats. A harmony between user privacy, data integrity, and real-time authentication is required due to the crucial nature of IoV services like real-time traffic updates and accident avoidance.

The contribution of this work is as follows:

- A physically unclonable function-based service security scheme for authenticating vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) interactions on roadside infrastructure.
- Mutual authentication for service authentication and verification through clear classification of synchronization and de-synchronization.
- Identifying suspicious vehicles through activity verification and communication interruption using federated learning.
- Performing a comparative analysis using security-related metrics with existing methods for proving the performance of proposed scheme.

Related works

Jiang et al. [16] designed a three-factor authentication protocol for IoV. PUF are used in the protocol that ensures the privacy and security of users. The designed protocol is a mutual authentication protocol that minimizes the error ratio in the authentication process. The designed protocol identifies the issues that are occurred during authentication and provides an optimal solution to solve the problems. The designed protocol increases the overall performance and efficiency level of IoVs.

Xiong et al. [17] developed an identity-based sign encryption with an equality test scheme (IBSC-ET) for IoV. In this case, classification functions are used to classify the equality provided to perform interaction tasks in IoV. The actual goal of the proposed scheme is to identify equality among the services. Certificate management issues are identified, lowering the computation process's latency and error ratio. Experimental results show that the developed IBSC-ET scheme improves the efficiency and feasibility range of the IoV.

Qureshi et al. [18] introduced a trust and priority-based drone-assisted Internet of Vehicles (TPDA-IoV) for the data routing process. Unique features and patterns are identified by TPDA-IoV which provides necessary information for further processes. Congestion issues and threats that occur during communication and interaction processes are detected. The newly introduced TPDA-IoV reduces the amount of time and energy consumed during the communication process. The introduced TPDA-IoV achieves high performance and reliability levels in IoV-based applications.

Wang et al. [19] proposed a scheme for IoV that used block-streaming service awareness and trusted verification. This scheme uses blockchain technology to build a verification platform for authentication and interaction processes. IoV uses certain devices to collect the edge nodes using sensors. The proposed scheme is a security scheme that protects user's confidential information. The proposed scheme ensures the privacy and security level of user's data from third parties, which maximizes the robustness of IoV.

Tian et al. [20] proposed a reputation framework for identifying the denial of traffic service in the IoV. Roadside units (RSUs) are set up along roadsides to provide the right information for different processes. The proposed vehicle cash (Vcash) scheme verifies the event using a verification process. The proposed scheme increases speed and reduces traffic during the communication process. Compared with other schemes, the proposed Vcash scheme improves the performance and effectiveness level of IoVs.

Yang et al. [21] designed a blockchain-based anonymous authentication scheme for the IoV. The proposed scheme's main aim is to ensure users' safety and security from attackers. Public–private keys are provided to users for the authentication process. The proposed scheme reduces both the time and energy consumption ratios in the computation process. The proposed scheme increases the authentication process's accuracy, enhancing the efficiency and feasibility range of IoVs.

Bagga et al. [22] developed a blockchain-based patch authentication protocol for the IoV. The developed protocol is a two-factor authentication protocol that secures the personal data of users from third-party members. An analysis technique is implemented here for addressing the problems and issues that are presented in the IoV. A key agreement scheme is also used here that provides important key values to the users for the authentication process. Experimental results show that the proposed protocol increases the overall effectiveness and reliability level of IoV.

Houmer et al. [23] introduced a secure authentication scheme for 5G-based Vehicle-to-Everything (V2X) communication systems. The actual aim of the introduced scheme is to provide high-security services to the users. Important key values and patterns are recognized during the authentication process, reducing the computation latency.

The introduced scheme improves the safety and security of user's data, which increases the performance and reduces the computational cost of V2X systems.

Jiang et al. [24] proposed a self-checking authentication scheme (SAES) for Vehicular ad hoc networks (VANET). VANET analyzes the characteristics which identify the necessary features which are presented among vehicles and roadside units (RSU). The proposed SAES scheme improves the overall privacy and security of VANET, which increases system efficiency and performance.

Wang et al. [25] designed an efficient multi-server authentication and key agreement protocol for the IoV. The main goal of the proposed protocol is to improve the safety and privacy level of users in communication services. Key values and passwords are shared with the users for the authentication process. Key values contain the actual data, which secures the data from third-parties. The proposed protocol provides effective solutions to problems that improve the effectiveness and feasibility of IoV systems.

Shen et al. [26] developed a secure and efficient blockchain-assisted authentication (SEA) scheme for edge-integrated IoV. Users must provide frequent authentication information in order to gain access to the device or vehicles. The proposed SEA scheme identifies services that have been paused or terminated due to threats and problems. SEA provides optimal solutions to problems, increasing the efficiency range of IoV. When compared with other schemes, the developed SEA scheme maximizes the overall security and privacy level of users in IoVs.

Xi et al. [27] proposed a zero-knowledge proof (ZKP)-based anonymous mutual authentication scheme for the IoV. The scheme that detects traces and issues in IoVs also employs elliptic curve cryptography (ECC). ZKP offers users a fast reconnection technique, which increases the authentication process's feasibility range. User verification keys and features are provided to ensure user safety and security. The proposed scheme improves the performance and effectiveness level of authentication, which reduces the latency in IoV.

Zhang et al. [28] designed a secure many-to-many authentication and key agreement (SMAKA) scheme for VANET. Cloud service providers (CSP) collect the data required for the authentication process. The main aim of the proposed SMAKA scheme is to improve the services provided to the users. CSP detects the anonymous messages that are received by users and alerts the cloud server to prevent problems for those users. Experimental results show that the designed SMAKA scheme ensures the privacy and security of users.

Xie et al. [29] proposed a security enhancement scheme for real-time, parallel in-vehicle applications. A controller area network with a flexible data rate (CAN-FD) is used here for the authentication process. CAN-FD analyzes the messages that are shared between individuals to produce feasible data for further processing. Message authentication codes (MAC) are added to messages to improve application performance. The proposed scheme achieves high efficiency and effectiveness in providing services to the users. In Table 1, the summary of the above works with the advantages and disadvantages is presented.

Proposed service-categorized security scheme

The design goal of the service-categorized security scheme is to maximize the mutual authentication in the IoV communication and information exchange by reducing adversaries or unidentified third parties along the roadside environment in smart cities. The open and closed infrastructures based IoV communication is processed using self-sustaining authentication. The security method or authentication is to grip a communication and information exchange, for which a variety of suspicious activities and adversaries occur to be controlled and mitigated for secure and handling sensitive guidance and communication information. The proposed scheme can provide authentication for IoV vehicle communication and sensitive information exchange between the sender and receiver in all the levels of communication sessions of smart cities. The proposed scheme is presented in Fig. 1.

The function of SCSS using PUF is to provide secure communication and information exchange. The PUF is used for identifying compromised and uncompromised communication devices based on vehicle service and sensitive information guidance. Information collected from the IoV communication and information exchange or distributed to all the sessions. The compromised and uncompromised communication devices are connected in smart cities through IoV. Mutual authentication for communication and information exchange is administered to reduce anonymous third parties or adversaries. The functions of compromised and uncompromised communication devices in the IoV are used for communication, information exchange, and authentication verification. Monitoring suspicious activities and adversaries using PUF is analyzed using a federated learning process. Improved security and authentication procedures for the Internet of Things motivate adoption of federated learning, a client-service mode method. It enables training machine learning models over multiple distributed devices while keeping data at the device level [30, 31]. Evidence shows that education can reduce the time it takes to complete the various steps in the authentication process. Federated learning can incur additional delay depending on criteria like model complexity, device number, connection overhead, and update frequency. It could make things safer but also make some processes take longer.

IoV communications in smart cities

The communication and information exchange for assisted IoV in smart cities is defined using two types of devices namely compromised and uncompromised communication devices. The compromised communication devices are responsible for information exchange, whereas the uncompromised devices administer information guidance monitoring and other adversary or unidentified third-party detection. The compromised devices communicate with a set of vehicles $IoV = \{1, 2, \ldots iov\}$. These vehicles can collect information from all the roadside infrastructures of smart cities. The above IoV communicate or exchange various quantities of information at different time $T = \{1, 2, \ldots t\}$ interval. Assume F denotes the number of suspicious activities that occurs in smart cities. Based

Table 1 Comparative analysis of related work

Reference	Blockchain	PUF	Security measure	Application	Advantages	Identified issue
Jiang et al. [16]	No	Yes	Multi-factor authentication	IoV	Strong security due to multi-factor authentication	More computational overhead
Xiong et al. [17]	No	No	Identity-based encryption	IoV	Inbuilt equality test of Signcryption	It suffers from trapdoor query
Qureshi et al. [18]	No	No	Trust-based	IoV	Micro-level analysis that instantaneously identifies changes	Slow verification due to varying trust factors
Wang et al. [19]	Yes	No	Identity-based blind signature technology	IoV	Microservices for blockchain	Model limited to 6G technology
Tian et al. [20]	No	No	Trust-based	IoV	Punishment model for malicious vehicles	The real roadmap and traffic scenario are not considered
Yang et al. [21]	Yes	No	Anonyms authentication	IoV	Decentralized operations, Revocation mechanism for malicious vehicles	Transaction latency is high for real IoV systems
Bagga et al. [22]	Yes	No	Group key-based authentication	IoV	Use of big data analytics and machine learning algorithm for the analysis of authentic data	The execution time on the emulated device is high
Houmer et al. [23]	No	No	Secret key-based authentication	IoV	Less execution time	Model limited to 6G technology
Jiang et al. [24]	No	No	Self-checking authentication based on a pseudonym	VANET	Participation of trusted authority in authentication and group signature	Roadside unit deployment cost is high
Wang et al. [25]	No	No	Multi-server-based authentication	IoV	Smart card is used for extra security of keys	Session disconnection requires a long process increasing the complexity
Shen et al. [26]	Yes	No	Key-based and privacy	IoV	Decentralized operations, less complexity	Synchronization lag between heterogeneous services
Xi et al. [27]	No	No	Anonymous mutual authentication	IoV	User traceability is easy and fast reconnection	Overhead in maintaining anonymity
Zhang et al. [28]	No	No	Mutual authentication	IoV	Less verification time for different users	Session disconnection requires a long process increasing the complexity
Xie et al. [29]	No	No	Two-stage method towards security	In-Vehicle Applications	Ease of deployment robustness	Non-parallel in-vehicle applications are not supported

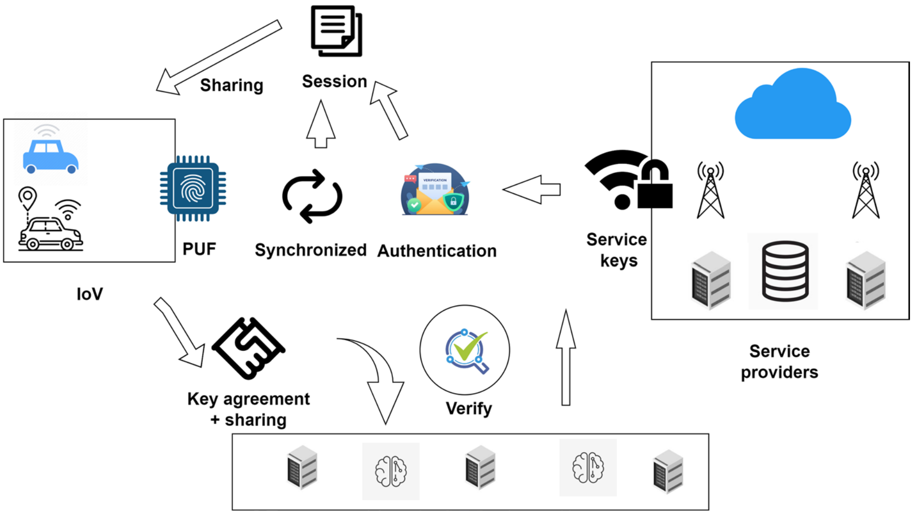


Fig. 1 Proposed SCSS

on the instance, the number of a process performed per unit of time is N^p such that the authenticated communication (Δ_{N^p}) is given as in Eq. (1).

$$\Delta_{N^p} = \begin{cases} \frac{iov \times N^p}{t} \in N^p \forall T, F = 0 \\ A_D \times \frac{iov - F}{N^p \times t} \in \left(N^p, F\right) \forall T, F \neq 0 \end{cases} \tag{1}$$

such that,

$$\left.\begin{array}{c} N^p \forall T = \sum_{i=1}^{iov} \left(N^p\right)_i \\ and \\ \left(N^p, F\right) \forall T = \sum_{i=1}^{iov} \left(N^p\right)_i - A_D \sum_{i=1}^{F} \left(N^p\right)_i \end{array}\right\} \tag{2}$$

where,

$$A_D = \left(\frac{pUn_{thp}}{Un_{thp} + N^p}\right) \tag{3}$$

where the variables A_D and Un_{thp} used to represent the adversary occurrence and unidentified third parties in different sessions. Based on the equation $N^p \forall T$ and $\left(N^p, F\right) \forall T$ condition indicates the synchronized keys for N^p and monitoring de-synchronization at different time intervals$T$. Rates and frequencies can be expressed numerically using the notationN^p. N^p indicates the volume of activities or tasks completed within a specified time frame, and its value may change depending on the exact circumstances stated in the study or research. In the compromised devices, IoV services and informed guidance are analyzed continuously and processed with security and Δ_{N^p} are the additional factors for ensuring digital signatures or passwords. At each time of IoV communication and information exchange in smart cities, security verification is performed for a successful session. From the collected smart city roadside data, the uncompromised communication devices can be classified and provide mutual authentication for each session. The proposed scheme identifies A_D through Q_{SP} and Q_{VC} interactions as either Δ_{NP}

or$sync_K$. This is classified under t(for authenticated) and K(for unauthenticated) based on operation output $(OT)_T$ at $T \cdot$ Therefore adverse communication between successive intervals is reduced to preventing A_D impacts. This is further confirmed using $P_{SP}\forall\ni_T$ and $\ni_{T-1}$ variations. It is to be noted that the non-responding verifications can't be classified under K. Depending on the Q_{SP} response if it is classified under $\ni_T$ then it isUn_{thp}.

The classification of PUF factors between $iov \in IoV$ and F is estimated using the observation of their vehicle-side authentication, access control, and service demands from the IoV in smart cities. In this case,$F > iov$ generates and shares fewer and insufficient keys for the vehicle service and information guidance. The perquisites of the authentication methods are to grip communication without any adversary occurrence and the routine Δ_{N^p} relies on $(iov \times N^p)$ is the condition for synchronized key verification.

$$\left.\begin{array}{c} Sync_K = \sum_{i=1}^{iov} \frac{au^{th}(N^p)_i}{t_i} \\ and \\ \urcorner Sync_t = \frac{\Delta_{N^p}}{(iov-F)} - \left(au^{th}\left(N^p\right) - Un_{thp}\right) \end{array}\right\} \tag{4}$$

In the above equation $Sync_K$ and $\urcorner Sync_t$ represents the synchronized key and de-synchronization time instance for IoV communications in smart cities. From Eqs. (1), (2), (3) and (4), the reliable service-sharing process (R_{SS}) with mutual authentication is verified using synchronized keys for each session at different time intervals T. This verification is performed for computing the condition $F = 0$ and $F \neq 0$ for all T instances using federated learning. The synchronization and de-synchronization process between the service provider and the vehicle is presented in Fig. 2.

The vehicles interact through T with the Service Provider (SP) wherein two processes are performed. The first is the K validity checking for the assigned intervals and the second is the sharing verification. The session is verified for sync/de-sync and SP classification for identified/unidentified. In the sharing verification, the vehicle information is used for F Checking. This is randomly performed throughout the synchronization time for identifying Un_{thp} as shown in Fig. 2. The learning process relies

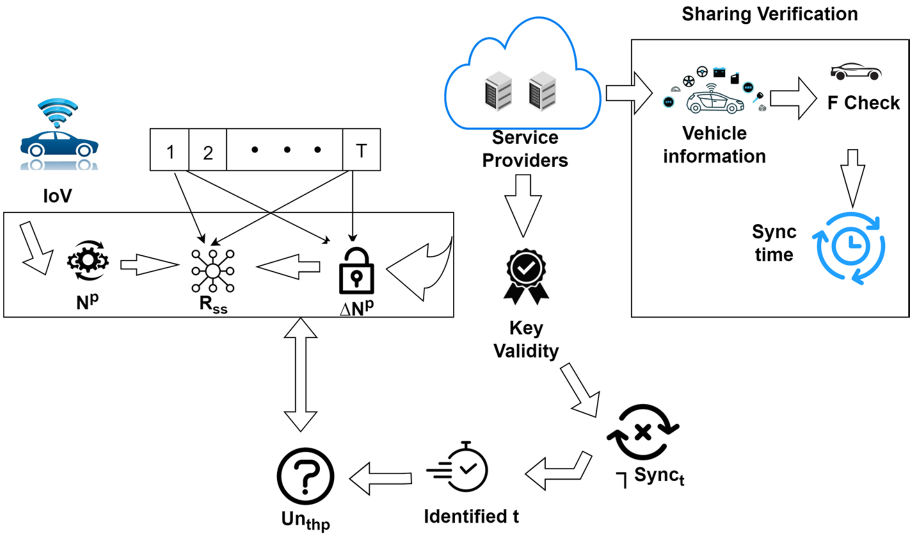


Fig. 2 Synchronization and De-Synchronization Process

on mutual authentication sequences $Sync_K$ and $\urcorner Sync_t$ such that the reliable service-sharing process is determined for all the individual operation outputOT. The linear solution of $Sync_K$ and $\urcorner Sync_t$ an indifferent session is the authentication verification for maximizing the condition$(iov \times N^p)$. The individual operation output OT and final solution $\exists$ are difficult to determine R_{SS}. The input for the communication and information exchange for vehicles in smart cities is Δ_{N^p} for both $N^p \forall T$ and $\left(N^p, F\right) \forall T$ in different sessions.

Assimilating PUF factors based on conditions $F \neq 0$,$\urcorner Sync_t = (iov - F)\Delta_{N^p}$, and $au^{th}\left(N^p\right)$, federated learning guarantees de-synchronization and individual operation via synchronized keys. If service based PUF factors are governed for identifying anonymous third parties and adversaries in the de-synchronization time, it is output in $F = 1$ else $F = 0$. The output of the individual operation in the first authentication $N^p \forall T$ generates a service key and sharing for security whereas $\left(N^p, F\right) \forall T$ segregate output of iov from IoV with $F \neq 0$. For instance, the monitoring de-synchronization and individual operation output and $\exists$ for $N^p \forall T$ is estimated for disconnecting those sessions. The assessments are performed to estimate both the communication devices with Un_{thp} identification and the conditional assessment of $au^{th}\left(N^p\right) = 0$ or $au^{th}\left(N^p\right) = 1$ from the different sessions. Therefore, the sensitive guidance/communication information required for the entire service session in a given time interval T is computed. Based on the above de-synchronization monitoring process,F serves as an input, after the identification of Un_{thp} and A_D in $N^p \forall T$ authentication

$$\left.\begin{array}{c}
(OT)_1 = \urcorner Sync_1 * t_1 + \left(N^p\right)_1 F \\
(OT)_2 = \urcorner Sync_2 * t_2 - Un_{thp_1} + \left(N^p\right)_2 F_1 \\
(OT)_3 = \urcorner Sync_3 * t_3 - Un_{thp_2} + \left(N^p\right)_3 F_2 \\
\vdots \\
(OT)_T = \urcorner Sync_T * t_T - Un_{thp_T} + \left(N^p\right)_T F_T
\end{array}\right\} \tag{5}$$

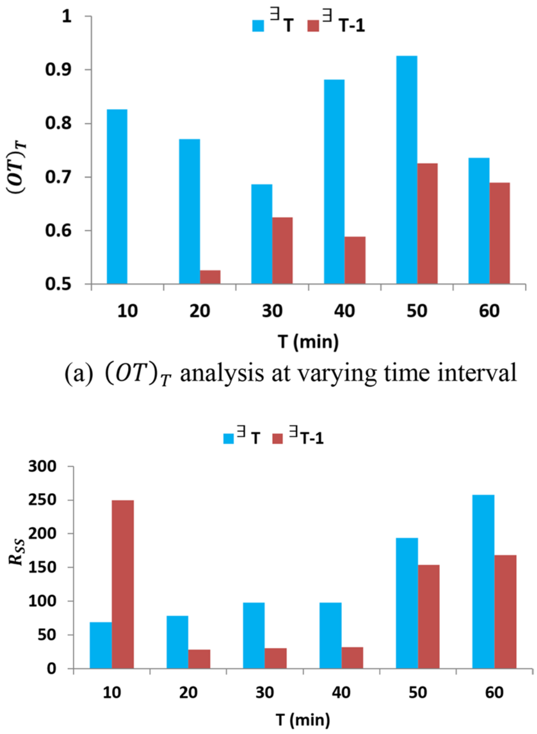
$$\left.\begin{array}{l}
\exists_1 = (OT)_1 = \urcorner Sync_1 * t_1 + \left(N^p\right)_1 F \\
\exists_2 = (OT)_2 - A_{D_1}\left(N^p\right)_1 \\
= \urcorner Sync_2 * t_2 - A_{D_1} + \Delta_{N^p 1} F - Un_{thp_1}\left(N^p\right)_2 \\
\exists_3 = (OT)_3 - A_{D_2}\left(N^p\right)_3 \\
= \urcorner Sync_3 * t_3 - A_{D_2} + \Delta_{N^p 2} F - Un_{thp_2}\left(N^p\right)_3 \\
\vdots \\
\exists_T = (OT)_T - A_{D_T}\left(N^p\right)_{T-1} \\
= \urcorner Sync_T * t_T - A_{D_T} + \Delta_{N^p T} F - Un_{thp_{T-1}}\left(N^p\right)_{T-1}
\end{array}\right\} \tag{6}$$

As per the Eqs. (5) and (6), the linear output is given as $\exists_T = \urcorner Sync_T * t_T - A_{D_T} + \Delta_{N^p T} F - Un_{thp_{T-1}}\left(N^p\right)_{T-1}$. If the condition $F = 0$, then $\exists = 1$ and $\urcorner Sync_T = \Delta_{N^p T}$. Therefore, $\exists = \Delta_{N^p T} * t_T + \Delta_{N^p T} = \Delta_{N^p T}(t_T + 1)$ is the reliable authentication and $R_{SS} = 1$. Hence, the service-sharing process of the such session is refined by 1. The IoV communication stores $\left(R_{SS}, au^{th}\left(N^p\right), IoV\right)$ at each session and the information, exchange determines the synchronized key for authenticating the services. Instead, $\left(N^p, F\right) \forall T$ is the individual operation output with synchronized service key is computed as shown in Eq. (7):

$$\left.\begin{array}{c}(OT)_1 = \Delta_{N^p{}_1}\\ (OT)_2 = \Delta_{N^p{}_2} - F_1 - A_{D_1} au^{th}\left(N^p\right)_1\\ (OT)_3 = \Delta_{N^p{}_3} - F_2 + A_{D_2} au^{th}\left(N^p\right)_2\\ \vdots\\ (OT)_{T-1} = \Delta_{N^p{}_{T-1}} - F_{T-1} - A_{D_{T-1}} au^{th}\left(N^p\right)_{T-1}\end{array}\right\} \tag{7}$$

$$\left.\begin{array}{l}\exists_1 = (OT)_1 = au^{th}\left(N^p\right)\\ \exists_2 = (OT)_2 + Sync_{K_1} - \urcorner Sync_1\\ = au^{th}\left(N^p\right)_2 - A_{D_1} - Un_{thp_1}\left(N^p\right)_1 - \urcorner Sync_1\\ \exists_3 = (OT)_3 + Sync_{K_2} - \urcorner Sync_2\\ = au^{th}\left(N^p\right)_3 - A_{D_2} - Un_{thp_2}\left(N^p\right)_3 - \urcorner Sync_2\\ \vdots\\ \exists_{T-1} = (OT)_{T-1} + Sync_{K_{T-1}} - \urcorner Sync_{T-1}\\ = au^{th}\left(N^p\right)_{T-1} - A_{D_{T-1}} - Un_{thp_{T-1}}\left(N^p\right)_{T-2}\\ -\urcorner Sync_{T-1}\end{array}\right\} \tag{8}$$

Equations (7) and (8) computes the condition $\urcorner Sync = (iov - F)\Delta_{N^p}$ and $A_D = 1$ or $A_D = 0$ in a continuous manner. If $A_D = 0$, then $\exists_{T-1} = \Delta_{N^p} - Un_{thp}N^p - \urcorner Sync$ is the final individual operation output and if $A_D = 1$, then $Un_{thp} = 1$ and hence the session is disconnected. This condition is not applicable for the first estimation as per Eqs. (5) and (6) because it depends on all authenticated service processes in IoV at T. The analyses of $(OT)_T$ and R_{SS} for different T is presented in Fig. 3.



(a) $(OT)_T$ analysis at varying time interval

(b) R_{SS} Analyses at varying time interval

Fig. 3 $(OT)_T$ and R_{SS} Analyses. (**a**) $(OT)_T$ analysis at varying time interval. (**b**) R_{SS} Analyses at varying time interval

The analyses for $(OT)_T$ and R_{SS} for the varying $T(min)$ and $\ni_T$ and $\ni_{T-1}$ is presented in Fig. 3a, b. The $(OT)_T$ is observed under Δ_{NP} for ensuring successful R_{SS}. First, R_{SS} is achieved by P_{SP} and S_K and $MH(sync_t)$ wherein $Tsync_K$ is alone in the interrupting sequence. If the $t = k$ then the A_D is high preventing P_{SP} such that X is varied for preserving $\ni_T$. contrarily $\ni_{T-1}$ is observed for renewing the key sharing process for F detection. Besides, the FL process identifies $de - sync$ for A_D under T and $\ni$ under $(T - 1)$ for preventing au^{th} failures. Therefore, the next communication session is observed for $sync_t$ and $sync_K$ for new SK based security. The 2 to $(T - 1)$ interval and $(1 - T)$ intervals are distinguished for preventing R_{SS} failures. Hence, the reliable service-sharing process, along with compromised and uncompromised communication devices, is observed by the IoV, and hence it is unchanged by third parties. The learning model for de-synchronization verification is illustrated in Fig. 4. The SP performs two different operations by utilizing federated learning paradigms.

The first process is the synchronization verification under two intervals, namely $(1toT)$ and $(2toT - 1)$. Considering $NP\forall\ AD_T$ detection ∀ t, the synchronization is performed. The successive synchronization is $\exists_{T-1}$. The de-synchronization is performed if $AD = 1$ is detected and two distinct training processes are performed, as shown in Fig. 4. In the following IoV communication and information exchange sequence, the service-sharing process and mutual authentication on its previous session determine the security measures for vehicle service and information guidance. If this sequence of vehicle service observation is based on $F > iov$, then the de-synchronization is identified from $iov \in IoV$ is disconnected to prevent suspicious activities and adversaries in the authentication or security method. The generating key is shared for both service providers and vehicles if any alert given by the assisted vehicles in smart cities relies on

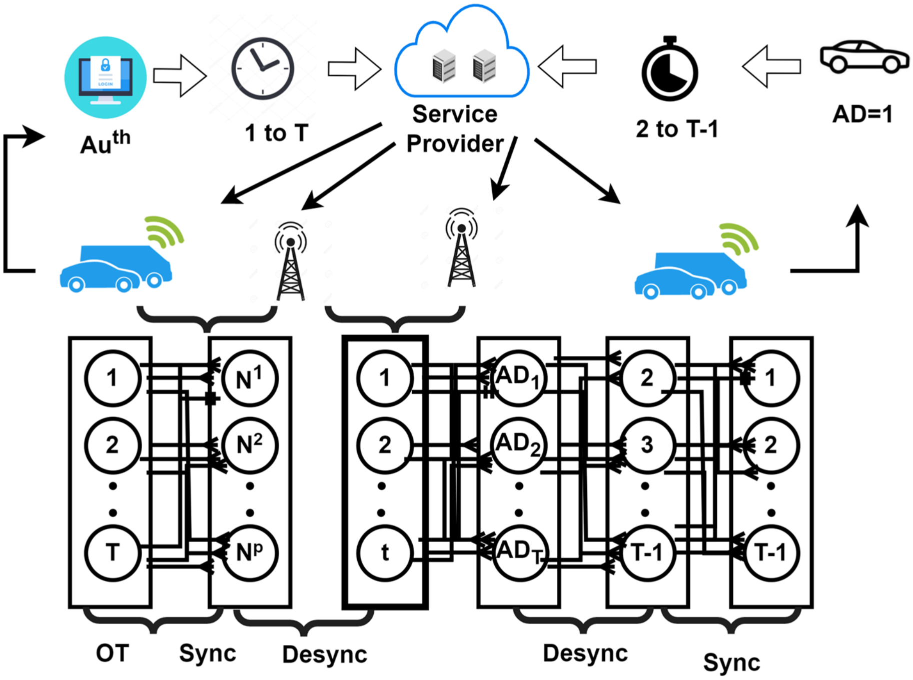


Fig. 4 Learning model for de-Synchronization verification

open and closed infrastructure along the roadside to ensure instant actions to find the unidentified third parties and adversaries. The security in the communication and information exchange from the IoV in smart cities relay on the external service providers and the vehicle communicator is used for deciding on the particular session and is analyzed. This process prevents adversaries and unidentified third parties from collecting incorrect communication and information, whereas the adversary detection ratio is high. The controlled PUF factor ensures de-synchronization and fewer information authentication/security methods within smart cities. However, the chances for external service providers and vehicle communicator information modification in the IoV environment are high. Therefore, end-to-end authentication is provided to secure IoV communications in smart cities.

Mutual authentication for service sharing

In the service-sharing process, mutual authentication follows the communication of uncompromised devices. The uncompromised communication devices rely on the different session, access control, and service demands for disseminating collected IoV information in smart cities. Based on the communication device authentication/security methods administered based on the service-sharing process, information exchange between vehicles and service providers is still vulnerable. This information guidance and vehicle service security is administered based on the service-based PUF factors such as digital signatures or passwords and R_{SS} concurrently. The first level of security is administered to protect information between smart cities and service providers. In this authentication process, the end-to-end security based on the service provider key and vehicle key is exchanged between the uncompromised communication devices and PUF factors. Assume P_{SP} and P_{VC} represent the generated synchronized keys for service providers and vehicle communicators, respectively. The authentication process follows synchronized keys and service keys combination for security. Assume Q_{SP} and Q_{VC} represent the service keys for all the service providers and vehicle communicators. The initial information processing requires synchronized key generation is represented as shown in Eqs. (9), 10.

$$\left.\begin{array}{c} P_{SP} = X * \exists * IoV \\ and \\ P_{VC} = X * S \end{array}\right\} \tag{9}$$

$$\left.\begin{array}{c} Q_{SP} \forall T \; and \; T \forall S \in IoV \\ and \\ Q_{VC} \forall T \; and \; T \forall (S - \exists \times iov) \in (IoV - F) \end{array}\right\} \tag{10}$$

In the above Eqs. (9) and (10),X is the random integer in which the service keys based on X process is fetched for authentication. The above equation estimates the validity of T for either IoV or $(iov - F)$ as identified by the federated learning. Now, the session keys (SK) for IoV communication are generated as shown in Eq. (11):

$$SK = P_{SP} * Q_{VC} * \|Q_{VC} \forall T\| = P_{VC} * Q_{SP} \| |Q_{VC} \forall T| \| \tag{11}$$

This synchronized key and vehicle key are valid only for all $t \in T$ posts in which K is discontinued is analyzed based on X. Now, the mutual authentication is generated as shown in Eqs. (12), (13):

$$MA\left(\neg Sync_t\right) = \left(R_{SS}\|S\|N_p\|X\|K\right) \tag{12}$$

$$Key\,sharing = \left\{\left[P_{SP} \oplus MA\left(\neg Sync_t\right) \oplus X \oplus T\right], iov\right\} \tag{13}$$

The above key generation and sharing rely on the number of $iov \in IoV$ communication and information exchange at each session S in the T interval. These PUF factors and authentication are to be verified on both the sender and receiver end. Here, de-synchronization time is mapped with K for identifying de-synchronization occurrence, hence if time varies; the synchronized key is shared randomly. If a de-synchronization occurrence is identified in any session, then authentication is cut in that particular session, and discontinued the vehicle services. The uncompromised device verifies the current PUF factors in communication and information exchange. The sequence diagram of the mutual authentication process is illustrated in Fig. 5. The shared key is valid only for the session $t \in T$ without being falsified by an adversary; the successful sessions are verified from the current instance to prevent overlapping of the following sessions. In the IoV environment, vehicle service-based authentication is provided to reduce the complexity of communication and information exchange. However, the PUF factor performs security verification. This verification check ensures appropriate service key is shared, as shown in Fig. 5. The IoV information is shared between the sender and receiver devices for communication. Therefore,

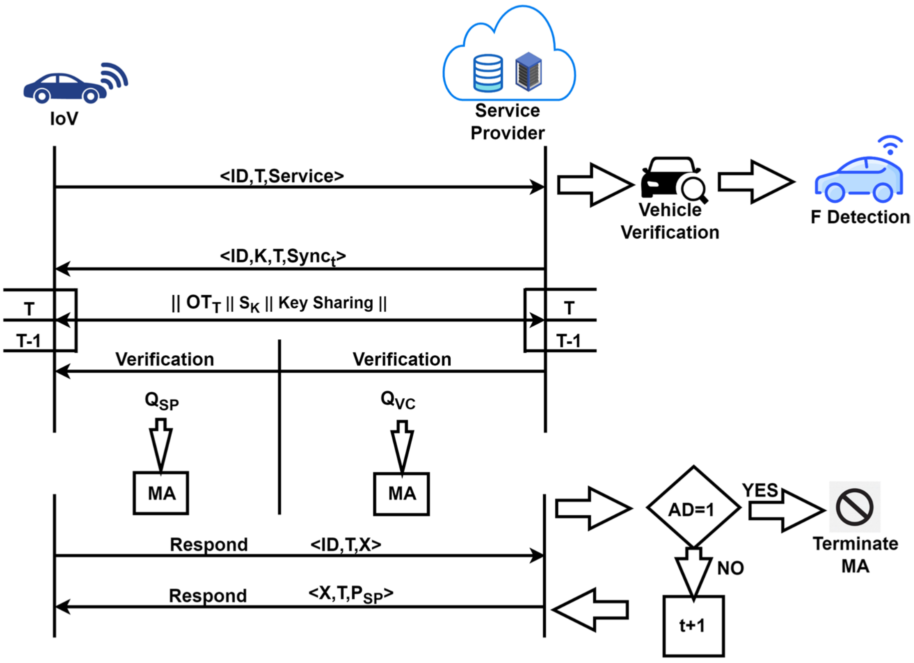
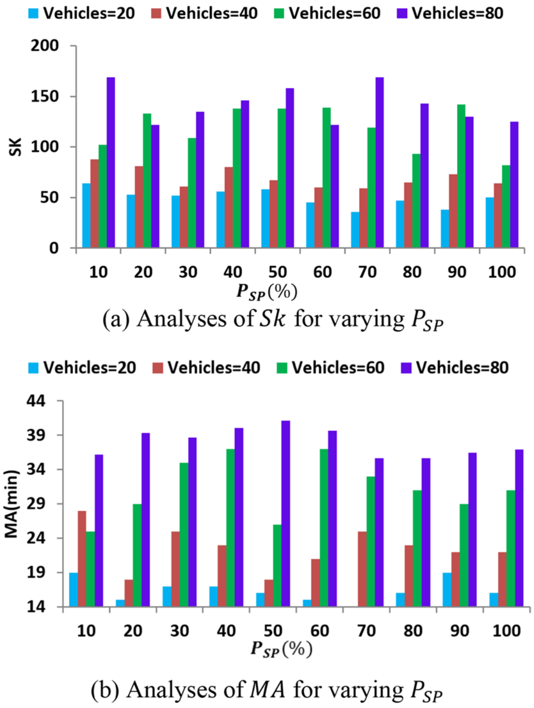


Fig. 5 Sequence diagram of the mutual authentication process

a synchronized key with the PUF factor for security verification ensures additional authentication/security methods for sharing information on both ends.

On both ends, the IoV functions as an uncompromised communication device for sequence,R_{SS} and synchronization or de-synchronization checks using federated learning. In the service-sharing process, each session is verified in the receiving terminal to prevent adversaries and unidentified third parties. This verification helps to reduce the authentication cut and de-synchronization time in the receiving IoV devices. Figure 6 presents the analyses of Sk and MA for the varying P_{SP} ratio.

For varying P_{SP} and S vehicles the SK and $MA(min)$ are analyzed in Fig. 6. The keys shared for Q_{SP} and Q_{VC} are encouraged for varying $sync_t$ for leveraging better outcomes. The verification is performed under T and $(T-1)$ for preventing AD existence and communication termination. Based on the FL process for K validity checking the R_{SS} time is determined. In the further process,$de-sync$ and $sync$ intervals are classified for maximizing MA for the augmenting vehicles. Therefore, the new processes under security and key assignment are performed for the new vehicles. Although PUFs provide robust security mechanisms, it is important to acknowledge that they are still susceptible to attacks. Methods for improving PUF-based systems, such as authentication and encryption of devices, secure key management, monitoring, and detection, are the subject of this research. These techniques aim to increase the difficulty, duration, and overall expense of an attack. Layers of defense, constant surveillance, and precise monitoring are only some of the essentials of a solid security plan.



(a) Analyses of Sk for varying P_{SP}

(b) Analyses of MA for varying P_{SP}

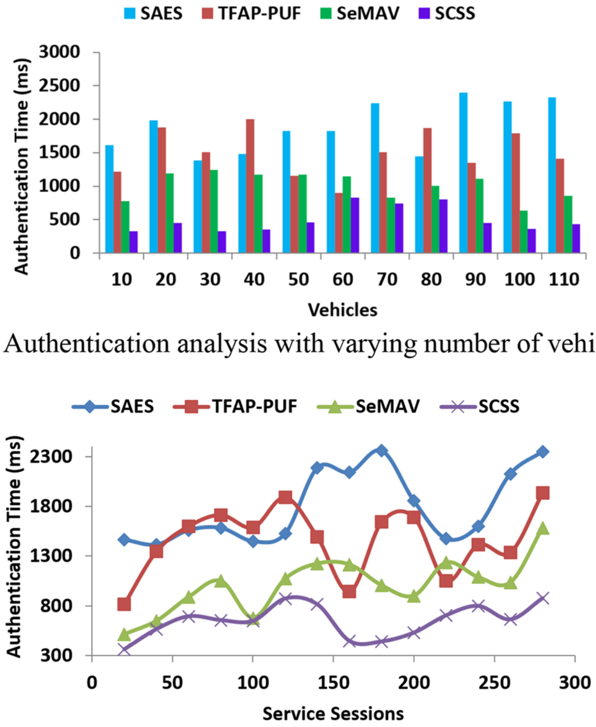
Fig. 6 Analyses of Sk and P_{SP}

Results and discussion

The simulation is carried out using OMNeT++with an open street map covering 21 km Road segment. The simulation creates an electronic model of IoV interactions, testing and evaluating security techniques for implementation in the real world, bridging the gap between theoretical research and actual IoV security. This method sheds light on the usefulness and efficiency of proposed security methods for protecting IoV communication This segment is characterized by 4 major cross-over lanes and 6 traffic junctions. The vehicle count throughout the road segment varies from 10 to 110 communicating with 14 access points. The access points cover a maximum of 250 m range for a vehicle ranging between 20 and 70 km/Hr. Service authentications are provided using elliptic curve cryptography as provided in [27] and the maximum session span is 20 min at on average. The adversary detection ratio, complexity, de-synchronization time, and successful sessions are analyzed using this information authentication time. The variants are vehicles and service sessions (20–280) and the alongside methods are SAES [24], TFAP-PUF [16], and SeMAV [25] are compared.

Authentication time analysis

The adversary and anonymous third-party identification in IoV communications in smart cities are observed from the different sessions for securing the information in both sender and receiver devices through mutual authentication. The authentication analysis for varying number of vehicles and sessions are shown in Fig. 7a, b respectively. In this proposed scheme using PUF factor satisfies less authentication time by computing the



(a) Authentication analysis with varying number of vehicles

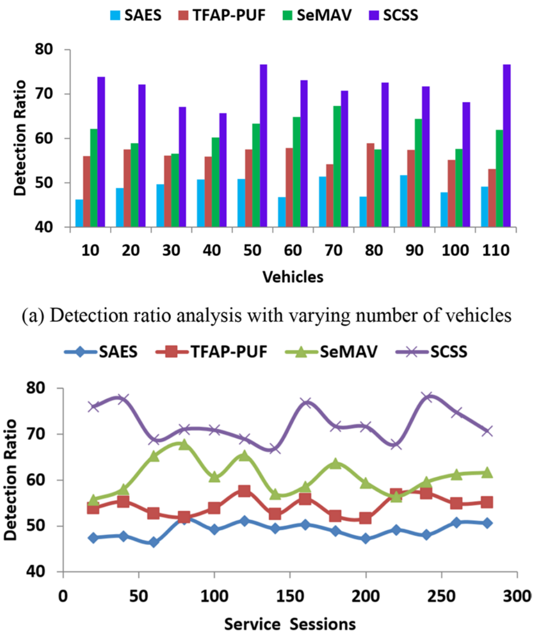
(b) Authentication analysis with varying service session

Fig. 7 Authentication Time Analysis

compromised and uncompromised communication devices. In this process, the de-synchronization occurrence is accurately identified for securing communication from these adversaries and disconnecting the session. The self-sustaining authentication method for the service-sharing process, the condition $N^p\forall T$ and $\left(N^p, F\right)\forall T$ is computed for a successful session. The adversary and unidentified third parties are mitigated depending on the federated learning security check until sensitive guidance/communication information is processed. The different vehicle service observation is preceded using Eqs. (4), (5), (6), (7), (8) and (9) computations. In this proposed securing communication, both sender and receiver end the verification is performed for identifying the adversary detection ratio. Based on this sequence, the authentication time is less compared to the other factors in this article.

Adversary detection ratio

The adversary detection ratio is high in the proposed scheme based on assisted vehicles communication and information exchange in smart cities relying on open and closed infrastructures along the roadside is observed for identifying de-synchronization occurrence as depicted in Fig. 8. In this proposed scheme satisfies less unidentified third parties by checking the security verification using federated learning. In this sequential process for adversary detection using PUF factors in different time intervals for secure communication, $iov \in IoV$, and F is computed until identifies de-synchronization occurrence from the available vehicle service and information guidance. Service needs and access control are essential for mutual authentication in smart cities. Verification of the PUF factor at both the sender and the receiver ends aids in the detection of unauthorized users. Sharing service keys facilitates the authentication of vehicle-guiding services and other sensitive data. Hence, the adversary detection is computed using federated



(a) Detection ratio analysis with varying number of vehicles

(b) Detection ratio analysis with varying service session

Fig. 8 Adversary Detection Ratio Analysis

learning based on different sessions, and de-synchronization identification is high in this proposed scheme.

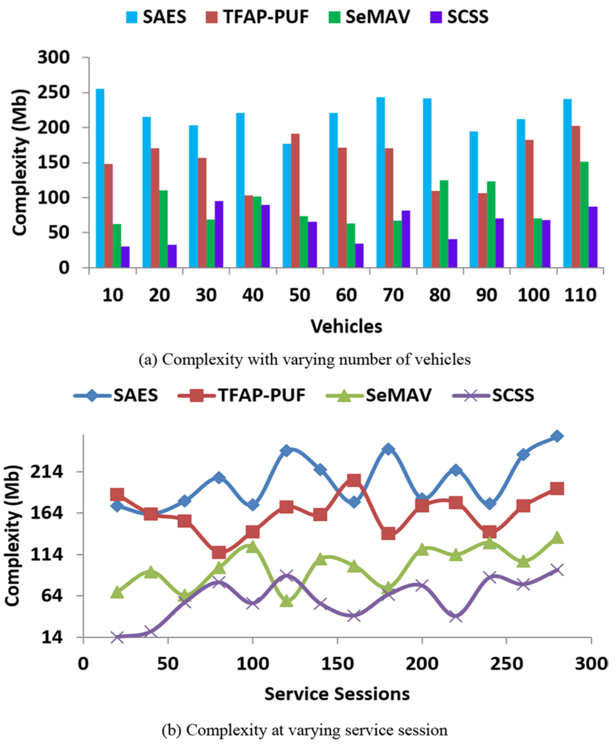
Space complexity

In Fig. 9, the space complexity identified in the proposed scheme is considerably less, with the PUF monitoring de-synchronization and individual operation output for secure communication and information exchange. In this instance, the adversary detection in the first session is observed for improving the service security verification with the PUF monitoring process for the individual operation output. This process is performed using federated learning and security methods to grip communication and helps to map the de-synchronization time for accurate IoV key generation and sharing through federated learning verification. Post this key generation, the synchronized key and service key are provided for the individuals for preventing complexity and authentication time.

The different vehicle services in each session differs that can be identified using mutual authentication as the first individual operation output with PUF factor. The service key is authenticated using the learning process for adversary detection from the different sessions along the roadside. This mutual authentication helps reduce the adversary and unidentified third parties with the PUF factor in all the sessions, which is less complex in this proposed scheme.

De-synchronization time

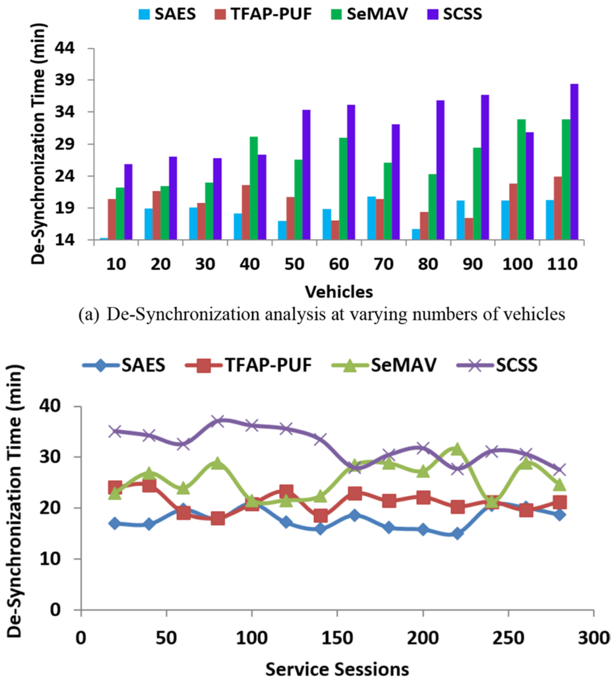
Figure 10 represents the secure communications on both the sender and receiver devices with mutual authentication for identifying suspicious activities, respectively.



(a) Complexity with varying number of vehicles

(b) Complexity at varying service session

Fig. 9 Complexity Analysis



(a) De-Synchronization analysis at varying numbers of vehicles

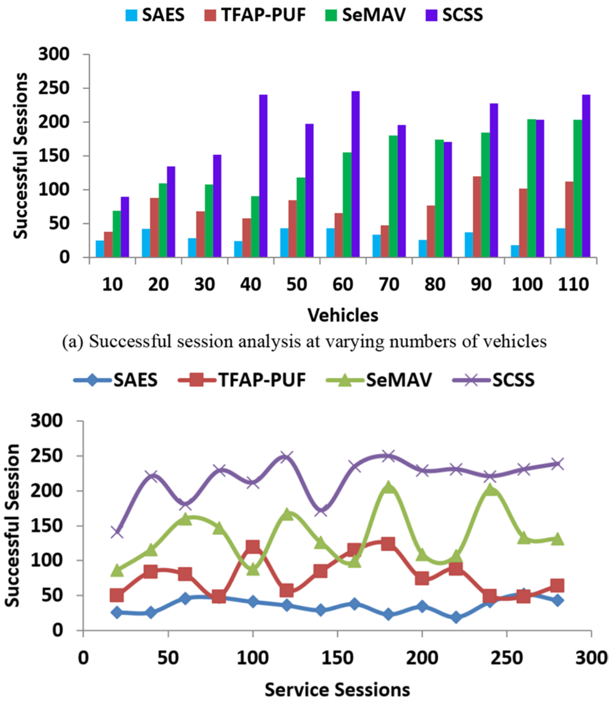
(b) De-Synchronization analysis with varying service sessions

Fig. 10 De-Synchronization time analysis

The proposed scheme maximizes adversary detection by identifying de-synchronization through the PUF factor by the federated learning check. The first de-synchronization occurrence is identified at the service provider and the vehicle communicator in IoV; the session is disconnected. From the instance, compromised and uncompromised communication devices estimate the vehicle-side authentication, access control, and service demand. The individual operation output and final solution satisfy highly secure communication due to classifying such de-synchronization occurred sessions in smart cities. Therefore, the final decision is modeled to identify adversaries and anonymous third parties in IoV as a better finding. The adversary identification from the communication vehicle's information is secured by the service keys using mutual authentication. Detecting such an adversary maximizes the IoV communication and successful sessions such that the high de-synchronization time achieves using the PUF factor in the proposed scheme.

Successful session

In Fig. 11, the service key generation and sharing for mutual authentication detect the de-synchronization occurrence at the service provider and vehicle for disconnecting the session. Secure communication and information exchange are performed for precise individual operation output based on the authentication. Both the sender and receiver devices are secured through service keys performed at different time intervals. The service-sharing process with mutual authentication is performed using a synchronized key by the federated learning verification for maximizing successful sessions. The federated learning outputs in continuous adversary detection with information guidance and a new session are processed for vehicle service. Based on the authentication/security



(a) Successful session analysis at varying numbers of vehicles

(b) Successful session analysis at varying numbers of sessions

Fig. 11 Successful session analysis.

Table 2 Performance analysis

Metrics	SAES		TFAP-PUF		SeMAV		Proposed SCSS	
	Vehicles	Service sessions	Vehicles	Service sessions	Vehicles	Service sessions	Vehicles	Service sessions
Authentication time (ms)	2322.8	2353.1	1412.6	1934.2	851.8	1583.6	431.999	877.274
Detection ratio	49.1	50.62	53.14	55.13	61.95	61.63	76.663	70.666
Complexity (Mb)	241.2	257.01	202.25	193.92	151.15	134.82	87.493	95.65
De-synchronization time (ms)	20.25	18.75	23.91	21.26	32.87	24.68	38.402	27.508
Successful sessions	43	43	112	64	204	131	241	239

methods, the sensitive information handling associated with the IoV communications is analyzed and secured to satisfy both the condition of $N^p \forall T$ and $\left(N^p, F\right) \forall T$ for identifying the de-synchronization occurrence. The adversary and anonymous third parties are identified using a federated learning process and achieve successful sessions from the different IoV, preventing adversary. Both sender and receiver devices with self-sustaining authentication methods satisfy highly successful sessions for identifying suspicious activities using the proposed PUF factor scheme. The comparative analysis summary with the findings is presented in Table 2 for the vehicles and service sessions.

The proposed scheme maximizes detection ratio, de-synchronization time, and successful sessions by 10.97, 11.05, and 8.39%, respectively. The authentication time and complexity are confined by 11.96 and 9.31%, respectively (for Vehicles). The proposed scheme maximizes detection ratio, de-synchronization time, and successful sessions by 14.87, 7.2, and 11.13%, respectively. The authentication time and complexity are confined by 9.19 and 8.5%, respectively (for Service Sessions).

Conclusion

Internet of vehicles relies on neighbors and roadside infrastructures for services and interactions. The possibilities for unauthorized infrastructure access and false services are high due to the open nature of the environment. To address this issue, this article presented a service-categorized security scheme using a physically unclonable function. Using the PUF, the communicating terminals are authenticated to prevent session failures. The adversaries are detected using synchronization verification and process failures. In the entire process, federated learning is employed for verifying synchronization and linear outputs of secure sessions and service sharing. The authentication is performed using lightweight key sharing and random integer-based generation. The session keys are mutually verified by the vehicle and the service providers throughout the interaction until an interruption occurs. The key-sharing process is referenced using identified third parties other than the suspicious vehicle. In the learning update, the adversary detection and de-synchronization verification are performed before the mutual authentication breakdown. This enhances the request processing with authenticated session interaction and information sharing. Security mechanisms and authentication protocols for the IoV have seen substantial improvements in areas including detection ratio, performance effectiveness, latency, energy consumption, and privacy protection since their introduction. An increased detection ratio of 10.97% identifies 11% more possible threats, and a performance efficiency increase of 15.32% enables faster processing, less waiting time, and longer battery life. As a bonus, these enhancements lower maintenance expenses. In the future process, the decentralized blockchain paradigm for improving authentication performance is planned to be incorporated. There are benefits to bolstering security, data integrity, and privacy by incorporating decentralized blockchain in IoV security schemes. Still, there are drawbacks to consider, such as scalability, latency, energy consumption, compliance, and user experience. This incorporation is expected to handle multi-server authentication confining the delay and service integrity.

Acknowledgements

Authors are thankful to Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia for supporting this research.

Author contributions

NBH and ASA have done the state-of-art literature and research gasp. MZK and MSH have formulated the problem statement and performed simulation. MAK have reviewed the simulation and editing of complete manuscript.

Funding

This research was funded by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R234), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Availability of data and materials

No dataset was used.

Declarations

Ethics approval and consent to participate

This article does not contain any studies with human or animal subjects.

Consent for publication

All authors have given consent for publication to this journal.

Competing interests

We declare that there's no financial/personal interest or belief that could affect their objectivity, or if there is, stating the source and nature of that potential competing. And we also declare that there are no potential competing interests.

Received: 4 August 2023 Accepted: 14 December 2023
Published online: 21 December 2023

References

1. Yao Y, Shu F, Li Z, Cheng X, Wu L. Secure transmission scheme based on joint radar and communication in mobile vehicular networks. IEEE Trans Intell Transp Syst. 2023. https://doi.org/10.1109/TITS.2023.3271452.
2. Cao B, Sun Z, Zhang J, Gu Y. Resource allocation in 5G IoV architecture based on SDN and fog-cloud computing. IEEE Trans Intell Transp Syst. 2021;22(6):3832–40. https://doi.org/10.1109/TITS.2020.3048844.
3. Li C, Dong M, Xin X, Li J, Chen X, Ota K. Efficient privacy-preserving in IoMT with blockchain and lightweight secret sharing. IEEE Internet Things J. 2023. https://doi.org/10.1109/JIOT.2023.3296595.
4. Dai X, Xiao Z, Jiang H, Lui JCS. UAV-assisted task offloading in vehicular edge computing networks. IEEE Trans Mob Comput. 2023. https://doi.org/10.1109/TMC.2023.3259394.
5. Ma J, Hu J. Safe consensus control of cooperative-competitive multi-agent systems via differential privacy. Kybernetika. 2022;58(3):426–39. https://doi.org/10.14736/kyb-2022-3-0426.
6. Wang J, Shao Y, Ge Y, Yu R. Physical-layer authentication based on adaptive Kalman filter for V2X communication. Veh Commun. 2020;26:100281. https://doi.org/10.1016/j.vehcom.2020.100281.
7. Ahmim I, Ghoualmi-Zine N, Ahmim A, Ahmim M. Security analysis on "three-factor authentication protocol using physical unclonable function for IoV." Int J Inf Secur. 2022;21(5):1019–26. https://doi.org/10.1007/s10207-022-00595-6.
8. Aghabagherloo A, Delavar M, Mohajeri J, Salmasizadeh M, Preneel B. An efficient and physically secure privacy-preserving authentication scheme for vehicular Ad-hoc NETworks (VANETs). IEEE Access. 2022;10:93831–44. https://doi.org/10.1109/access.2022.3203580.
9. Tian C, Jiang Q, Li T, Zhang J, Xi N, Ma J. Reliable PUF-based mutual authentication protocol for UAVs towards multi-domain environment. Comput Netw. 2022;218:109421. https://doi.org/10.1016/j.comnet.2022.109421.
10. Cao B, Zhang J, Liu X, Sun Z, Cao W, Nowak RM, Lv Z. Edge-cloud resource scheduling in space–air–ground-integrated networks for internet of vehicles. IEEE Internet Things J. 2022;9(8):5765–72. https://doi.org/10.1109/JIOT.2021.3065583.
11. Yao Y, Zhao J, Li Z, Cheng X, Wu L. Jamming and eavesdropping defense scheme based on deep reinforcement learning in autonomous vehicle networks. IEEE Trans Inf Forensics Secur. 2023;18:1211–24. https://doi.org/10.1109/TIFS.2023.3236788.
12. Cao B, Zhao J, Gu Y, Fan S, Yang P. Security-aware industrial wireless sensor network deployment optimization. IEEE Trans Industr Inf. 2020;16(8):5309–16. https://doi.org/10.1109/TII.2019.2961340.
13. Dai X, Xiao Z, Jiang H, Chen H, Min G, Dustdar S, Cao J. A learning-based approach for vehicle-to-vehicle computation offloading. IEEE Internet Things J. 2023;10(8):7244–58. https://doi.org/10.1109/JIOT.2022.3228811.
14. Min H, Fang Y, Wu X, Lei X, Chen S, Teixeira R, Zhao X. A fault diagnosis framework for autonomous vehicles with sensor self-diagnosis. Expert Syst Appl. 2023. https://doi.org/10.1016/j.eswa.2023.120002.
15. Zhang X, Fang S, Shen Y, Yuan X, Lu Z. Hierarchical velocity optimization for connected automated vehicles with cellular vehicle-to-everything communication at continuous signalized intersections. IEEE Trans Intell Transp Syst. 2023. https://doi.org/10.1109/TITS.2023.3274580.
16. Jiang Q, Zhang X, Zhang N, Tian Y, Ma X, Ma J. Three-factor authentication protocol using physical unclonable function for IoV. Comput Commun. 2021;173:45–55. https://doi.org/10.1016/j.comcom.2021.03.022.
17. Xiong H, Hou Y, Huang X, Zhao Y. Secure message classification services through identity-based signcryption with equality test towards the internet of vehicles. Veh Commun. 2020;26:100264. https://doi.org/10.1016/j.vehcom.2020.100264.
18. Qureshi KN, Alhudhaif A, Shah AA, Majeed S, Jeon G. Trust and priority-based drone assisted routing and mobility and service-oriented solution for the internet of vehicles networks. J Inform Secur Appl. 2021;59:102864. https://doi.org/10.1016/j.jisa.2021.102864.
19. Wang Y, Tian Y, Hei X, Zhu L, Ji W. A novel IoV block-streaming service awareness and trusted verification scheme in 6G. IEEE Trans Veh Technol. 2021;70(6):5197–210. https://doi.org/10.1109/tvt.2021.3063783.
20. Tian Z, Gao X, Su S, Qiu J. Vcash: a novel reputation framework for identifying denial of traffic service in internet of connected vehicles. IEEE Internet Things J. 2020;7(5):3901–9. https://doi.org/10.1109/jiot.2019.2951620.
21. Yang H, Li Y. A blockchain-based anonymous authentication scheme for internet of vehicles. Procedia Comput Sci. 2022;201:413–20. https://doi.org/10.1016/j.procs.2022.03.109.
22. Bagga P, Sutrala AK, Das AK, Vijayakumar P. Blockchain-based batch authentication protocol for internet of vehicles. J Syst Architect. 2021;113:101877. https://doi.org/10.1016/j.sysarc.2020.101877.
23. Houmer M, Ouaissa M, Ouaissa M. Secure authentication scheme for 5G-based V2X communications. Procedia Computer Science. 2022;198:276–81. https://doi.org/10.1016/j.procs.2021.12.240.

24. Jiang H, Hua L, Wahab L. SAES: a self-checking authentication scheme with higher efficiency and security for VANET. Peer-to-Peer Netw Appl. 2020;14(2):528–40. https://doi.org/10.1007/s12083-020-00997-0.
25. Wang J, Wu L, Wang H, Choo KKR, Wang L, He D. A secure and efficient multiserver authentication and key agreement protocol for internet of vehicles. IEEE Internet Things J. 2022;9(23):24398–416. https://doi.org/10.1109/jiot.2022.3188731.
26. Shen M, Lu H, Wang F, Liu H, Zhu L. Secure and efficient blockchain-assisted authentication for edge-integrated internet-of-vehicles. IEEE Trans Veh Technol. 2022;71(11):12250–63. https://doi.org/10.1109/tvt.2022.3194008.
27. Xi N, Li W, Jing L, Ma J. ZAMA: a ZKP-based anonymous mutual authentication scheme for the IoV. IEEE Internet Things J. 2022;9(22):22903–13. https://doi.org/10.1109/jiot.2022.3186921.
28. Zhang J, Zhong H, Cui J, Xu Y, Liu L. SMAKA: secure many-to-many authentication and key agreement scheme for vehicular networks. IEEE Trans Inf Forensics Secur. 2020;16:1810–24.
29. Xie G, Yang LT, Wu W, Zeng K, Xiao X, Li R. Security enhancement for real-time parallel in-vehicle applications by CAN FD message authentication. IEEE Trans Intell Transp Syst. 2020;22(8):5038–49.
30. Mou J, Gao K, Duan P, Li J, Garg A, Sharma R. A machine learning approach for energy-efficient intelligent transportation scheduling problem in a real-world dynamic circumstances. IEEE Trans Intell Transp Syst. 2022. https://doi.org/10.1109/TITS.2022.3183215.
31. Fu Y, Li C, Yu FR, Luan TH, Zhao P. An incentive mechanism of incorporating supervision game for federated learning in autonomous driving. IEEE Trans Intell Transp Syst. 2023. https://doi.org/10.1109/TITS.2023.3297996.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.