Iran Journal of Computer Science (2025) 8:2345–2355
https://doi.org/10.1007/s42044-025-00318-9

RESEARCH

SO-ITS: a secure offloading scheme for intelligent transportation systems in federated fog-cloud

Yashar Salami[1]

Received: 9 May 2025 / Accepted: 6 August 2025 / Published online: 13 August 2025

Abstract
Intelligent driving technologies have significantly reduced traffic congestion and road accidents, enhancing overall safety by enabling vehicles to communicate with their surroundings, thus keeping drivers informed of traffic conditions and critical events. Adequate data security demands mutual authentication for secure exchanges and robust offloading procedures to guard against potential attacks. This paper presents the SO-ITS scheme, tailored for safe data offloading in intelligent driving systems. The scheme's robustness is validated using the AVISPA tool, confirming its resilience to known threats. Comparative analysis with existing schemes assesses communication overhead, computational cost, and bit complexity. At the same time, performance is evaluated through NS-3 simulations, measuring PDR, throughput, and EDD across various scenarios. Results demonstrate that the SO-ITS scheme provides strong security, low communication overhead, and moderate computational complexity, establishing it as a promising solution for secure intelligent transportation systems.

Keywords Offloading · Authentication · Fog · Federated

1 Introduction

Today, the rapid evolution of cities into innovative urban ecosystems places vehicles at the heart of this transformation [1, 2]. Among the pillars of this development, intelligent transportation systems stand out as a critical enabler, with the Internet of Vehicles emerging as one of its most dynamic and impactful domains [3] By leveraging internet connectivity, the IoV allows vehicles to interact with external entities, such as infrastructure components, seamlessly [4], roadside units [5, 6], mobile devices, applications, services, etc.) [7]. His connectivity supports various applications, including dynamic routing, efficient parking management, enhanced safety measures, and real-time positioning through GPS technologies. The strength of IoV lies in its deep integration with smart infrastructure, RSUs, and advanced sensor networks, enabling a cohesive and intelligent transportation environment [8, 9]. Building upon this immutable trust management, blockchain consensus mechanisms can facilitate secure key distribution and dynamic access control among IoV nodes [10, 11].

However, as intelligent driving systems rely on continuous data exchange, ensuring secure and trustworthy communication becomes essential. Before any information transfer occurs, mutual authentication between senders and receivers is crucial. Establishing secure authentication remains one of the primary challenges in maintaining the safety, reliability, secure offloading, and resilience of communication within IoV ecosystems. Mun et al. [7] proposed an improved secure anonymous authentication scheme for roaming services in global mobility networks, utilizing symmetric encryption and hashing. However, their scheme is susceptible to Rainbow table (RT) attacks. In contrast, Zhao et al. introduced a more secure and efficient anonymous authentication scheme for the same purpose [12]. In 2014, a method relying on asymmetric encryption and hashing was proposed, but it remains vulnerable to RT attacks. Similarly, Mohit et al. [13] designed an authentication protocol for a wireless sensor network-based innovative vehicular system, which uses hashing but is also susceptible to RT attacks. Ying et al.[14] In 2017, an anonymous and lightweight authentication protocol for secure vehicular networks was introduced. This approach relies on asymmetric encryption and hashing techniques. However, it remains susceptible to (RT) attacks. In 2019,

✉ Yashar Salami
yashar.salami@kapadokya.edu.tr

[1] Faculty of Computer and Information Technologies, Cappadocia University, Ürgüp, Nevşehir, Turkey

Table 1 Comparison of related work

Works	RT Attacks	Fog Node	Authentication	Secure offloading	Symmetric	Asymmetric	Smart driving	Intersection
[12]	O	Δ	Δ	Δ	O	Δ	O	O
[13]	O	Δ	Δ	O	O	O	O	O
[14]	O	Δ	Δ	O	Δ	O	O	O
[24]	O	Δ	Δ	O	Δ	O	O	O
[15]	O	Δ	Δ	O	O	O	O	O
[16]	Δ	Δ	Δ	O	O	O	Δ	O
[17]	Δ	Δ	Δ	Δ	O	O	O	O
[18]	O	Δ	Δ	O	Δ	O	O	O
[19]	Δ	Δ	Δ	O	Δ	O	Δ	O
[20]	Δ	Δ	Δ	O	O	Δ	Δ	O
[21]	Δ	Δ	Δ	O	Δ	O	O	O
[22]	O	Δ	Δ	O	O	Δ	Δ	O
[23]	Δ	Δ	Δ	O	O	Δ	Δ	O
SO-ITS	Δ	Δ	Δ	Δ	O	Δ	Δ	Δ

Δ Supported, *O* not supported

Chen et al. [10] proposed a secure authentication protocol for the Internet of Vehicles, utilizing symmetric encryption and hashing. However, it is susceptible to RT attacks. Vasudev et al. introduced a lightweight mutual authentication protocol for V2V communication in the Internet of Vehicles, addressing similar challenges [15]. However, in 2020, it was vulnerable to an RT attack. Salami et al. published a paper in 2024, the Secure Offloading Scheme for IoT-Based [16]. However, this scheme did not support smart vehicles. In response, Yashar et al. proposed a model for a secure data offloading approach tailored for the Internet of Vehicles, yet this scheme also faced limitations in supporting intelligent vehicles.[17]. Mun et al. [18] proposed a scheme for secure anonymous authentication in roaming services for global mobility networks. In 2020, Khajehvand [19] proposed a secure mutual authentication scheme and key exchange protocol in fog-based IoV (SMAK-IOV). However, this scheme could not support secure offloading at intersections, as it primarily focused on authentication and key exchange without addressing the specific challenges of load management in dynamic intersection environments. In 2023, Zeinali et al. [20] introduced SAIFC, a secure authentication scheme for IoV based on fog-cloud federation. Nevertheless, this scheme could not support secure offloading at intersections, as it lacked mechanisms to handle the high variability and real-time demands of intersection-based load management. In 2021, Vahid et al. [21] presented CE-SKE, a cost-effective secure key exchange scheme in fog federation for IoV. However, this scheme could not support secure offloading at intersections, as its design prioritized cost efficiency and key exchange security over the complexities of traffic-aware load distribution. In 2019, Wazid et al. [22] Developed AKM-IoV, an authenticated key management protocol for fog computing-based IoV deployment. Despite its strengths, this scheme could not support secure offloading at intersections, as it did not adequately address the real-time load balancing requirements in such scenarios. In 2024, [23] proposed LSMAK-IOV, a lightweight secure mutual authentication and key exchange scheme in fog-based IoV. However, this scheme could not support secure offloading at intersections, as its lightweight design overlooked the specific challenges of managing load in high-traffic intersection environments. However, this scheme could not fully support secure offloading, as its primary focus was on authentication security, and it lacked sufficient consideration for network secure offloading Intersection challenges. Table 1 presents a comparison of related works.

1.1 Contribution paper

- This paper proposes a secure mutual authentication scheme for secure data offloading in vehicle-to-vehicle communications, enhancing the security of vehicular networks.
- The SO-ITS scheme utilizes asymmetric cryptography to safeguard the confidentiality and integrity of exchanged messages.
- Security analysis substantiates that the scheme is resilient against known attacks prevalent in vehicular environments.

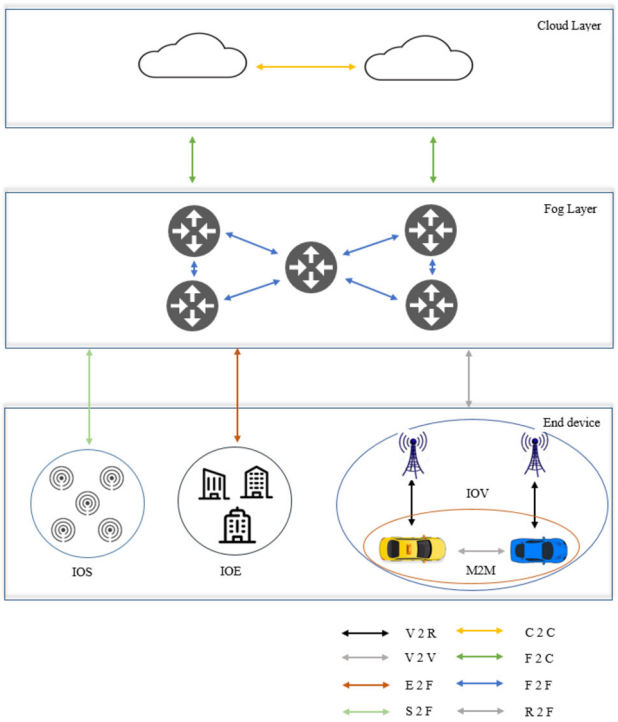

Fig. 1 Network model

- The AVISPA tool is employed to validate the protocol's security, which is complemented by a comparative analysis with existing schemes that assesses computational cost, communication overhead, and bit complexity.
- Furthermore, the scheme is simulated using the NS3 network simulator and evaluated through key performance metrics across diverse scenarios, including PDR, throughput, and EDD.

1.2 Organization paper

The remainder of this paper is organized as follows: Sect. 2 outlines the problem statement and the network model underpinning the SO-ITS. Section 3 outlines the design of the SO-ITS authentication scheme. Section 4 provides a security analysis along with the corresponding results. Section 5 presents a performance evaluation and compares the security requirements of the proposed approach with those of existing methods. Finally, Sect. 6 concludes the paper and discusses potential directions for future research.

2 Network model and problem statement

This section elaborates on the network model and its fundamental assumptions, then defines the main problem and its significance. Figure 1 illustrates the system architecture, depicting the interactions among end devices, the fog layer, and the cloud. In this framework, the cloud layer communicates with the fog layer and interacts with various end devices. The end layer encompasses domains such as the Internet of Sensors (IoS), the Internet of Energy (IoE), the Internet of Vehicles (IoV), and machine-to-machine (M2M) communications. End devices can exchange data directly or offload intensive tasks to the fog layer when higher computational power is required. Data storage in the cloud ensures efficient access and long-term preservation of information. A key requirement for secure data transmission is the deployment of a robust authentication mechanism between the source and the destination. In vehicle-to-vehicle communications, designing an authentication mechanism that can withstand common security threats presents a significant challenge. Considering that limited computational resources constrain vehicles in the end layer, computation offloading becomes inevitable; hence, there is a pressing need for a secure offloading mechanism among vehicles. This paper proposes and presents a secure method to address this challenge.

2.1 Assumptions

The SO-ITS network model is based on the following assumptions:

- Perfect time synchronization is assumed among all vehicles and RSUs (fog nodes).
- Mutual trust is established between the fog layer and the cloud.
- Mutual authentication and trust exist between every pair of fog nodes, including RSUs.
- The fog infrastructure is presumed secure and immune to compromise.
- The cloud environment is assumed secure and free of vulnerabilities.
- RSUs are considered secure and fully reliable.
- Fog nodes, RSUs, and the cloud do not disclose any sensitive data.
- All vehicles are pre-registered with the RSU, fog, and cloud layers.
- Vehicles have no prior knowledge or trust relationships with one another.
- The communication channel is insecure and vulnerable to interception or tampering.

2.2 Adversarial model

The proposed network model is analyzed using the Dolev-Yao adversary model, which allows the attacker to intercept, modify, and inject messages between legitimate entities.

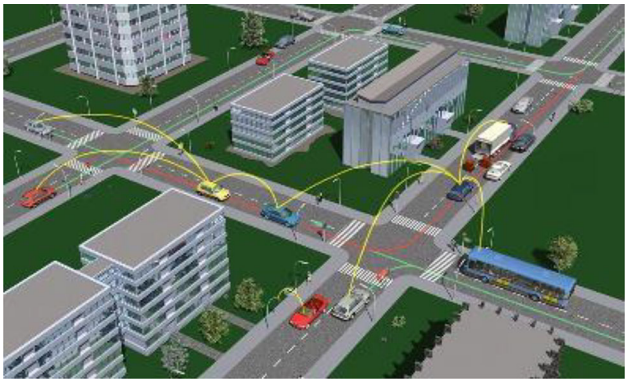

Fig. 2 Communication of cars at the intersection

This framework considers passive eavesdropping, aimed at extracting sensitive information, and active attacks that disrupt or manipulate communications. The security analysis evaluates the system's resistance to common threats, including impersonation, replay, and MITM. Both formal methods and simulation-based tests are conducted under various adversarial scenarios to validate the scheme's robustness.

2.3 Problem statement

Intelligent driving technologies have significantly enhanced road safety, resulting in a substantial reduction in traffic accidents. Central to these systems is the ability of vehicles to seamlessly exchange data with other vehicles and their surrounding environment. Secure communication at intersections, where precise and timely data sharing is critical for safe driving decisions, is paramount, particularly considering the necessity of secure data offloading. To achieve this, vehicles must first mutually authenticate to establish a secure channel for communication and secure data offloading at intersections. Figure 2 shows the vehicle-to-vehicle communication process at an intersection.

However, authentication in intelligent driving systems is susceptible to various threats, including replay attacks [16] and man-in-the-middle attacks (MITM) [17], as well as impersonation attacks and RT attacks [18]. Robust authentication mechanisms are essential to secure vehicular communication and data offloading at intersections, as they are vulnerable to these vulnerabilities. While many existing approaches rely on hash functions to minimize computational overhead, these functions are inherently susceptible to RT attacks. In contrast, the authentication scheme SO-ITS in this paper eliminates the use of hash functions. Our approach significantly enhances security by addressing this vulnerability, offering robust protection against RT attacks and other prevalent threats in vehicular communication and secure data offloading systems.

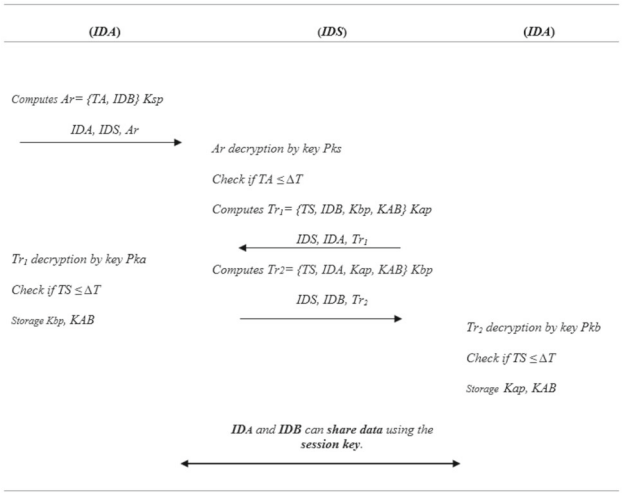

Fig. 3 SO-ITS scheme

Table 2 Show notations used in this SO-ITS

No	Notations	Description
1	Vehicles	v
2	Public key	puk
3	Private key	pvk
4	IDA	ID v(A)
5	IDB	ID v(B)
6	IDS	ID Fog Node
7	Kap	puk of v (A)
8	Kbp	puk of v (B)
9	Ksp	puk of Fog Node
10	Pka	Pvk of v(A)
11	Pkb	Pvk of v(B)
12	Pks	Pvk of Fog Node
13	KAB	Session keys v(A) and v(B)
14	TA	Timestamp of v (A)
15	TS	Timestamp of fog node
16	ΔT	Expiration time

3 SO-ITS

This section presents the SO-ITS scheme, as illustrated in Fig. 3.

3.1 Notations

The list of Notations used in this SO-ITS is presented in Table 2.

3.2 Initialization and registration phase

As stipulated in Sect. 2, each vehicle is pre-registered with the Roadside Unit (RSU), fog layer, and cloud. The Trusted Third Party (TTP), embodied by the fog node, oversees the management and storage of all public keys within the network, ensuring secure and centralized data handling.

3.3 Login and authentication phase

LA1: In the initial phase, entity A computes the authentication request as Ar = {TA, IDB} {K{sp}}, where TA denotes the timestamp and IDB is the identifier of entity B. Subsequently, A transmits Ar along with IDB and IDS to the trusted third party (TTP), denoted as S. LA2: Upon reception, the TTP S decrypts Ar using its private key and verifies the validity of the timestamp by ensuring TA $\leq \Delta$T, where ΔT represents the allowable time window. If the verification succeeds, S prepares two encrypted messages: (i) it encrypts {TS, IDB, K{bp}, K{AB}} using A's public key and dispatches it to A (identified by IDA) and S itself as transaction Tr1; and (ii) it encrypts {TS, IDA, K{ap}, K{AB}} with B's public key and sends it to B (identified by IDB) and S as transaction Tr2. LA3: Upon receiving Tr1, entity A decrypts it using its private key and authenticates the timestamp by confirming TS $\leq \Delta$T. Following successful validation, A securely stores Kbp and KAB to establish a secure communication channel with B.

LA4: Similarly, upon receiving Tr2, entity B decrypts the message with its private key and verifies the timestamp condition TS $\leq \Delta$T. If the condition is valid, B stores Kap and KAB to enable secure communication with A. Figure 4 shows the flowchart of the SO-ITS design.

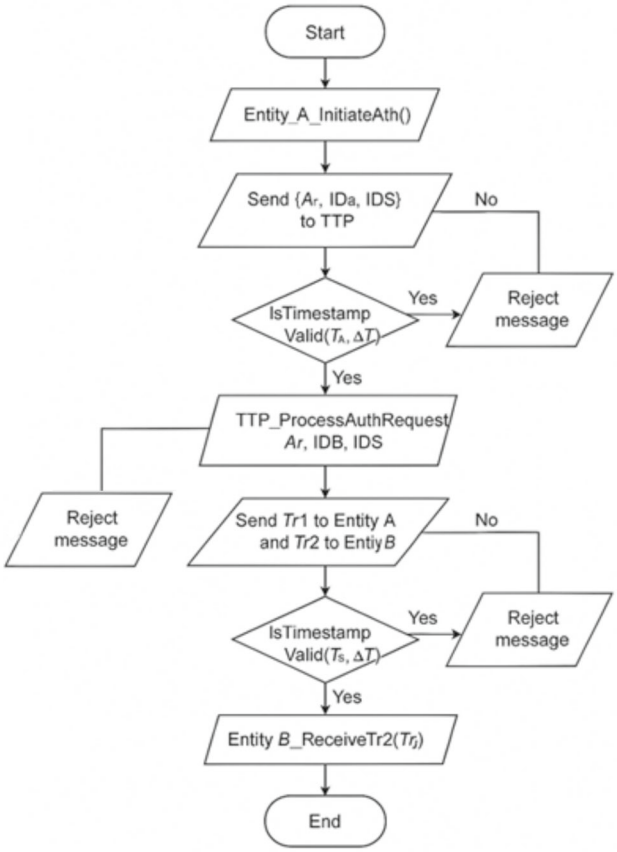

Fig. 4 Flowchart SO-ITS scheme

4 Security formal analysis

This section presents the security analysis of the SO-ITS scheme using the AVISPA tool and discusses the corresponding results. One widely adopted approach for security verification is the formal analysis of authentication protocols. The AVISPA. It is a powerful and practical tool designed for this purpose. It enables the automated validation of security properties in authentication protocols. [25, 26]. AVISPA offers four distinct back-ends for comprehensive protocol analysis: (i) the OFMC [27], which performs symbolic model checking; (ii) the CL-ATSE [28], which uses constraint-solving techniques for attack detection; (iii) the SATMC [29] Which applies SAT-solving methods to protocol verification, and (iv) the TA4SP [30] Which leverages tree automata techniques for scalable analysis.

4.1 Analysis of simulation results

The robustness of the SO-ITS scheme against replay attacks, MITM attacks, impersonation attacks, and other potential threats has been evaluated using the OFMC and CL-AtSe verification tools, as detailed in Sect. 2. Figures 5 and 6 show the simulation outcomes obtained from these tools. The results from OFMC indicate that the verification process explored two nodes with a search depth of 1 ply and completed within 0.10 s. Similarly, the CL-AtSe tool analyzed four distinct states with a translation time of 0.04 s. These simulation outcomes confirm that the SO-ITS scheme successfully passed the security checks of OFMC and CL-AtSe, demonstrating its resilience against the analyzed attack vectors.

5 Performance analysis

In this section, the performance of the SO-ITS scheme is evaluated and compared against existing protocols presented in the [11–18, 26–30] computational cost and fulfillment of security requirements.

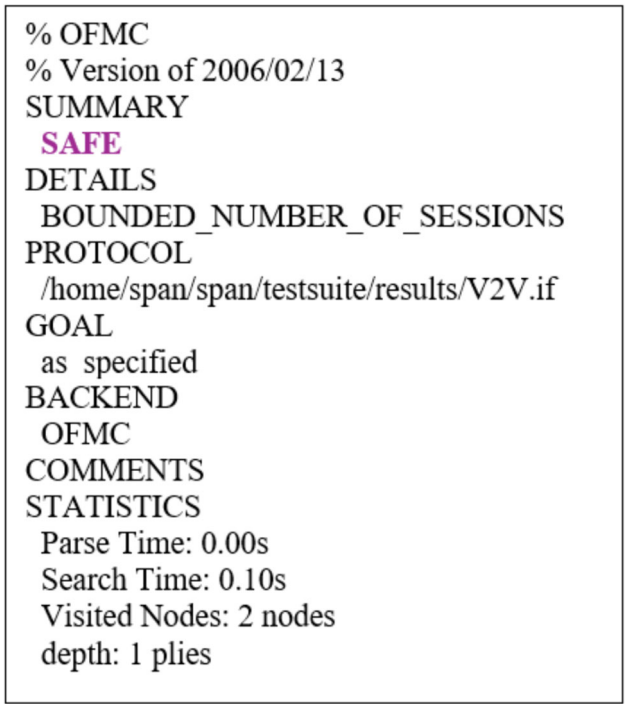

Fig. 5 Results of OFMC

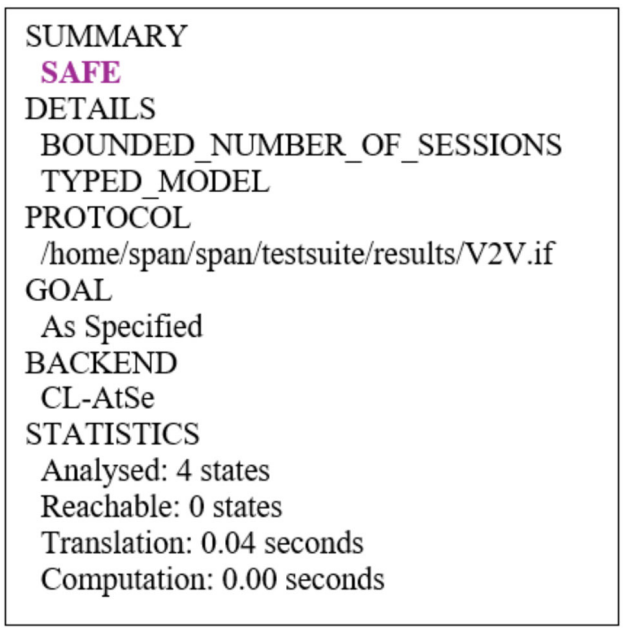

Fig. 6 Results of CL-ATSe

5.1 Computation cost

Table 3 provides a comparative analysis of the computational cost associated with the SO-ITS scheme and those reported in [11–18, 26–30]. The following symbols are defined to perform the analysis: Thf is the execution number of a hash operation; Tecmf is the execution number of an ECC point multiplication operation; Pef is the execution number of public-key encryption; Pdf is the execution number of public-key decryption; Sef is the execution number of symmetric-key encryption; Sdf is the execution number of symmetric-key decryption; Pmf is the execution number of point multiplication; and Eof is the execution number of the exponential operation.

The computational cost analysis reveals that the proposed protocol offers distinct characteristics compared to existing schemes. Specifically, Mun et al. reported the lowest computation cost of 0.0360 ms [18]. This is closely followed by the scheme in [14], which achieves 0.0340 ms [14], and by the protocol of Mohit et al., at 0.0400 ms [12]. Ying et al. also demonstrate a relatively low processing overhead of 0.5785 ms [13]. In contrast, Chen et al. incur a higher computation cost of 2.0980 ms [17], while Zhao et al. present 12.3216 ms [11]. Other lightweight schemes, such as those in [15] and [27], report costs of 16.0209 ms [15] and 17.8770 ms [27], respectively. Heavier protocols—including those in [16, 28], and [30]—register costs of 25.5975 ms [16], 23.5900 ms [28], and 46.2000 ms [30], respectively, whereas the scheme in [29] achieves 9.2536 ms [29], and the design in [26] records the highest cost of 69.3000 ms [26].

In our SO-ITS scheme, public-key cryptography techniques have been employed to ensure robust security. Unlike some previous works, hash functions—vulnerable to replay and tampering attacks—have been deliberately omitted in favor of stronger cryptographic primitives. As a result, while the proposed scheme achieves superior security guarantees, it exhibits a higher processing cost (26.4378 ms) when compared to the most lightweight protocols. Figure 7 illustrates a detailed comparison of the computation costs across the referenced protocols and the SO-ITS scheme. Although our protocol incurs relatively higher computational overhead, this trade-off is justified by its enhanced resilience against a broader spectrum of cryptographic attacks, including those targeting hash-based systems.

5.2 Communication cost and total bits

Our analysis indicates that the protocol proposed by Zhao et al. incurs the highest communication cost among the compared schemes, with 11 messages [11]. This is followed by the protocols of Mun et al. and Mohit et al., each exhibiting a communication cost of 9 messages [12, 18]. In contrast, the protocols developed by Ying et al., Chen et al., and Vasudev et al. demonstrate a moderate communication cost, each with four messages [13, 14, 17]. Scheme [26] uses 8 messages [26], while Scheme [27] requires 7 messages [27]. Both Schemes [29] and [30] use 6 messages [29, 30]. The heaviest message overheads belong to Scheme [15] with 24 messages [15] and Scheme [16] with 25 messages [16]. The

Table 3 Comparison of computation cost

Schemes	Thf	Tecmf	Pef	Pdf	Sef n	Sdf	Pmf	Eof	Total cost	TC (ms)
[18]	8 Thf	0Tecm	0Pe	0Pd	1Se	1Sd	0Pm	0Eo	8 Th + 1Se + 1Sd	0.036
[12]	10 Thf	0Tecm	1Pe	1Pd	0Se	0Sd	5Pm	0Eo	10 Th + 1Pe + 1Pd + 5Pm	12.3216
[13]	20Thf	0Tecmf	0Pef	0Pdf	0Sef	0Sdf	0Pmf	0Eof	20 Thf	0.04
[14]	14Thf	0Tecmf	0Pef	0Pdf	2Sef	2Sdf	0Pmf	1.5Eof	14Thf + + 2Sef + 2Sdf + 1.5 Eof	0.5785
[24]	12Thf	0Tecmf	0Pef	0Pdf	2Sef	2Sdf	0Pmf	6Eof	12Thf + 2Sef + 2Sdf + 6 Eof	2.098
[15]	17Thf	0Tecmf	0Pef	0Pdf	0Sef	0Sdf	0Pmf	0Eof	17Thf	0.034
[16]	29Thf	0Tecmf	0Pef	0Pdf	0Sef	0Sdf	0Pmf	6Eof	29Thf + 6Eof	16.0209
[17]	61Thf	18Tecmf	0Pef	0Pdf	0Sef	0Sdf	0Pmf	0Eof	61Thf + 1 8Tecm	25.5975
[19]	0Thf	0Tecmf	9Pef	9Pdf	0Sef	0Sdf	0Pmf	0Eof	9Pef + 9Pdf	69.3
[20]	30Thf	8Tecmf	0Pef	9Pdf	0Sef	0Sdf	0Pmf	0Eof	30Thf + 8Tecm	17.877
[21]	7Thf	0Tecmf	3Pef	3Pdf	0Sef	0Sdf	0Pmf	0Eof	7Th + 3Pe + 3Pd	23.59
[22]	35Thf	4Tecmf	0Pef	0Pdf	0Sef	0Sdf	0Pmf	0Eof	35Thf + 4 Tecm	9.2536
[23]	0Thf	0Tecmf	6LPe	6LPd	0Sef	0Sdf	0Pmf	0Eof	6LPe + 6LPd	46.2
SO-ITS	0Thf	0Tecmf	3Pef	3Pdf	0Sef	0Sdf	0Pmf	0Eof	3Pef + 3Pdf	26.4378

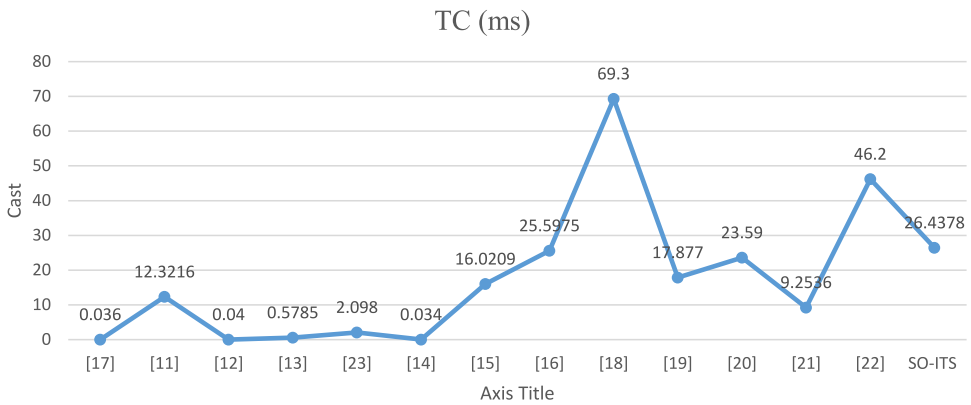

Fig. 7 Computation cost

proposed SO-ITS scheme achieves the lowest communication overhead, with a total of just 3 messages. This reduction in message count reflects the efficiency of our design, making it particularly suitable for resource-constrained environments where minimizing round-trips is critical. Figure 8 provides a comparative illustration of the message counts across existing protocols and the SO-ITS scheme, highlighting the superior efficiency of our approach.

Our analysis of message sizes (in bits) reveals that the protocol proposed by Mohit et al. achieves the lowest transmitted-bit overhead, at just 1,280 bits [12]. This is followed by Scheme [27] at 1,760 bits [27] and Ying et al. at 1,952 bits [13]. The protocol developed by Vasudev et al. has a slightly higher communication size of 2,496 bits [14], while Chen et al. reported 3,024 bits [17]. The proposed SO-ITS scheme demonstrates a message size of 3,072 bits, which remains lower than those of Scheme [29] (3,392 bits [29]) and Mun et al. (3,808 bits [18]) and Zhao et al. (5,536 bits [11]). Heavier message sizes include Scheme [30] at 6272 bits [30], Scheme [15] at 8,900 bits [15], Scheme [26] at 9,344 bits [26], and Scheme [16] at 13,120 bits [16]. This balance of moderate bit-length and strong security properties underscores the suitability of SO-ITS for applications where both bandwidth efficiency and cryptographic strength are required. Figure 9 presents a graphical comparison of the message sizes among the reviewed protocols and the SO-ITS scheme, and Table 4 provides a detailed tabulation of both communication costs and message sizes across all protocols.

5.3 Comparison of security requirements

Table 5 presents a comparative analysis of nineteen security requirements (SO-ITS1–SO-ITS19) across the proposed SO-ITS scheme and thirteen existing protocols. The first group of schemes—[16, 26–30] and [15]—uniformly satisfy the core security requirements from replay resistance through TTP-based design (SO-ITS1–SO-ITS17), yet only a subset ([26, 28–30]) support secure offloading (SO-ITS18)

Fig. 8 Communication costs

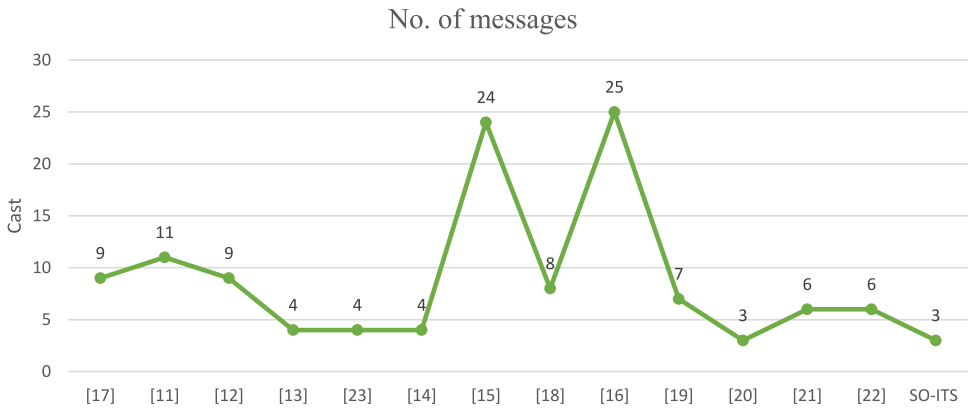

Fig. 9 Communication bits

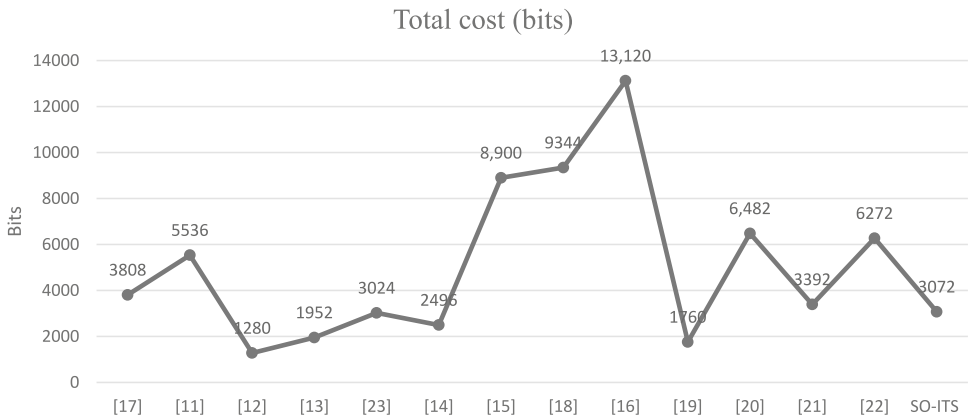

Table 4 Comparison of communication cost and the number of bits

Schemes	No. of messages	Total cost (in bits)
[18]	9	3808
[12]	11	5536
[13]	9	1280
[14]	4	1952
[24]	4	3024
[15]	4	2496
[16]	24	8,900
[19]	8	9344
[17]	25	13,120
[20]	7	1760
[21]	3	6,482
[22]	6	3392
[23]	6	6272
SO-ITS	3	3072

and none provide Intelligent Transportation Systems functionality (SO-ITS19). By contrast, the protocols in [14]–[18] exhibit additional gaps: they are vulnerable to replay attacks (SO-ITS1) and/or RT attacks (SO-ITS13), and fail to support advanced features including key exchange (SO-ITS14), formal verification by OFMC (SO-ITS15) and CL-AtSe (SO-ITS16), as well as secure offloading (SO-ITS18).In contrast, the proposed SO-ITS scheme demonstrates comprehensive resilience against all active and passive threats—replay, MITM, insider, stolen-verifier, impersonation, brute-force, offline-guessing and RT attacks (SO-ITS1–SO-ITS13)—and fully supports key exchange (SO-ITS14), formal verification (SO-ITS15, SO-ITS16), TTP-based design (SO-ITS17), secure offloading (SO-ITS18) and Intelligent Transportation Systems functionality (SO-ITS19). This comprehensive coverage underscores the SO-ITS scheme's superior security posture, uniquely integrating all nineteen requirements within a cohesive architectural scheme. For reference, the security features are defined as follows:

SO-ITS1: Replay attack; SO-ITS2: MITM attack; SO-ITS3: Insider attack; SO-ITS4: Stolen-verifier attack; SO-ITS5: Impersonation attack; SO-ITS6: Brute-force attack; SO-ITS7: Offline password guessing attack; SO-ITS8: Device anonymity; SO-ITS9: Mutual authentication; SO-ITS10: Session key agreement; SO-ITS11: Forward secrecy; SO-ITS12: Confidentiality; SO-ITS13: RT resistance; SO-ITS14: Key exchange; SO-ITS15: Verified by OFMC; SO-ITS16: Verified by CL-ATSE; SO-ITS17: TTP-based design, SO-ITS18: Secure Offloading,, SO-ITS19: intelligent transportation systems.

Table 5 Comparison of security requirements

Schemes														
SO-ITS	[23]	[22]	[21]	[20]	[17]	[19]	[16]	[15]	[24]	[14]	[13]	[12]	[18]	Security requirements
Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	O	O	Δ	O	O	Δ	SO-ITS1
Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	O	Δ	Δ	SO-ITS2
Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	SO-ITS3
Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	SO-ITS4
Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	SO-ITS5
Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	SO-ITS6
Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	SO-ITS7
Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	SO-ITS8
Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	SO-ITS9
Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	SO-ITS10
Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	SO-ITS11
Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	SO-ITS12
Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	O	O	O	O	O	O	SO-ITS13
Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	O	O	O	O	O	O	SO-ITS14
Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	O	Δ	O	O	O	O	SO-ITS15
Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	O	O	O	O	O	O	SO-ITS16
Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	O	Δ	Δ	Δ	Δ	Δ	SO-ITS17
Δ	Δ	Δ	O	O	Δ	O	O	O	O	O	O	O	O	SO-ITS18
Δ	O	O	O	O	O	O	O	O	O	O	O	O	O	SO-ITS19

6 Simulation results and analysis

This section validates the proposed scheme's performance through network simulations conducted using the NS-3.29 simulator on the Ubuntu 20.04.1 operating system. The simulation experiments were carried out on a Dell Inspiron 5110 system equipped with an Intel Core i5-2410 M processor running at 2.30 GHz, 4 GB of RAM, and a 1 TB hard disk drive (HDD).[31].

6.1 Simulation environment and settings

The simulation was executed for a total duration of 200 s. A fleet of 30 vehicles was deployed, while the number of RSUs was varied across three scenarios with counts of 5, 10, and 15, respectively. Additional simulation settings include stationary vehicle mobility (0 m/s), the Friis propagation loss model, a transmission power of 7.5 dBm, IEEE 802.11 as the Medium Access Control (MAC) protocol, IEEE 802.11p for vehicular wireless communication, and AODV as the routing protocol. The simulation environment covered a 300 × 1500 m area, designed to emulate a realistic intersection scenario.

6.2 Simulation results

The performance of the SO-ITS scheme was evaluated using the NS-3 simulator across three distinct configurations, varying the number of RSUs at 5, 10, and 15, in a vehicular intersection scenario with 30 vehicles. The analysis focused on three key performance metrics: PDR, throughput, and EED.

PDR: The results indicate that the 10-RSU configuration achieved the highest PDR, approximately 0.9, reflecting an optimal balance between network coverage and traffic load. The PDR decreased to around 0.86 with 15 RSUs, likely due to increased interference or contention in the denser network. The 5-RSU setup recorded the lowest PDR at approximately 0.84, suggesting insufficient coverage and a higher packet loss rate. Figure 10 shows PDR results.

Throughput: The 15-RSU configuration demonstrated the highest throughput, reaching approximately 5000 Kbps, indicating its superior capacity to handle large data volumes (Fig. 10). The 10-RSU scenario followed with a throughput of about 4000 Kbps, while the 5-RSU configuration lagged at around 1000 Kbps, highlighting its limitation in supporting high traffic loads. Figure 11 shows the Throughput results.

EED: The lowest delay was observed in the 5-RSU configuration, at approximately 20 million milliseconds, attributed

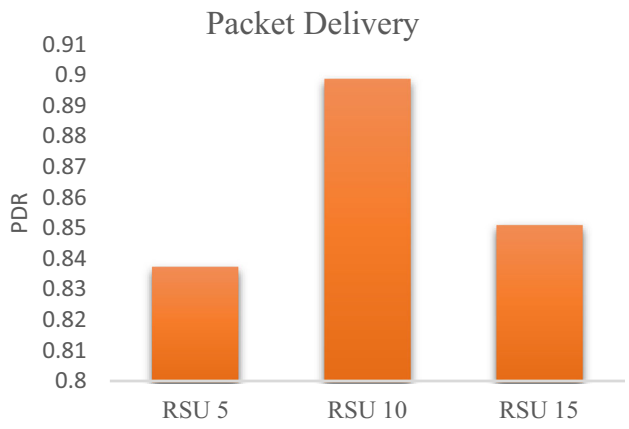

Fig. 10 Packet delivery

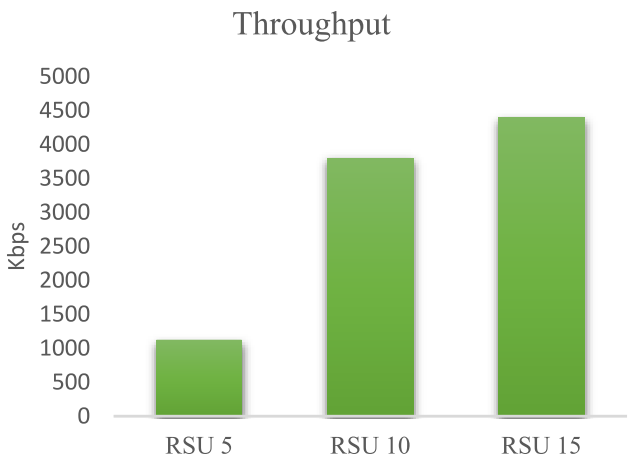

Fig. 11 Throughput

to fewer transmission hops and reduced contention in a sparser network. The delay increased to about 30 million milliseconds with 10 RSUs and peaked at nearly 50 million with 15 RSUs, likely due to higher coordination overhead and potential bottlenecks in the denser setup. Figure 12 shows EED results.

Based on the simulation outcomes, the 15-RSU configuration is deemed the most suitable for dense vehicular environments, offering the highest throughput and a satisfactory PDR despite the elevated latency. The 10-RSU setup provides a balanced performance with reliable delivery and moderate throughput at lower latency, while the 5-RSU configuration underperforms in both PDR and throughput, rendering it inadequate for this scenario. Accordingly, the 15-RSU configuration is recommended for optimal network performance, although the 10-RSU setup may be preferred for latency-sensitive applications.

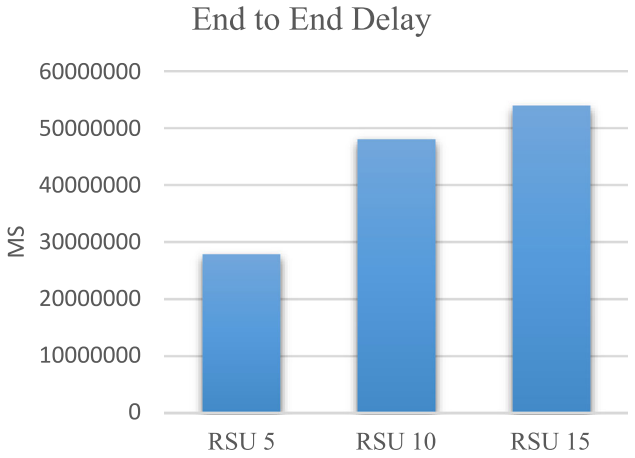

Fig. 12 End-to-end delay

7 Conclusion

This study has introduced a novel and secure authentication scheme tailored for intelligent driving systems, utilizing public-key cryptography to ensure robust protection against security threats. Formal verification using the AVISPA tool confirms the scheme's resilience against a wide range of known attack vectors. Performance comparisons demonstrate that the proposed solution minimizes communication overhead and achieves a balanced computational load, outperforming several existing methods. Additionally, NS3-based simulation results at urban traffic intersections indicate that optimal system performance with 30 vehicles can be sustained by deploying at least 15. Future research will focus on further optimizing the computational efficiency and scalability of the scheme to maintain high security and performance while reducing infrastructure requirements, thereby increasing its feasibility for large-scale, real-world blockchain-based smart transportation deployment.

Author contributions Y.S. wrote the main manuscript text, prepared all figures, and thoroughly revised the entire manuscript. The authors reviewed and approved the final version for publication.

Funding This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Data availability The data used to support this novel scheme are included within the article.

Declarations

Conflicts of interest The authors declare no competing interests.

References

1. Feng, S., Yan, X., Sun, H., Feng, Y., Liu, H.X.: Intelligent driving intelligence test for autonomous vehicles with naturalistic and adversarial environment. Nat. Commun. **12**(1), 1–14 (2021)
2. Salami, Y., Taherkhani, F., Ebazadeh, Y., Nemati, M., Khajehvand, V., Zeinali, E.: Blockchain-based internet of vehicles in green smart city: applications and challenges and solutions. Anthropog. Pollut. **7**(1), 87–96 (2023)
3. 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). https://doi.org/10.1109/TITS.2020.3048844
4. Yu, S., Gong, X., Shi, Q., Wang, X., Chen, X.: EC-SAGINs: edge computing-enhanced space-air-ground integrated networks for internet of vehicles. IEEE Internet Things J. **9**, 5742–5754 (2021)
5. Salami, Y.: SOBT-UF: secure offloading in blockchain infrastructure for intelligent transportation systems using 5G-enabled UAVs within a fog-edge computing federation. In: 2024 19th Iranian conference on intelligent systems (ICIS), pp. 217–222. IEEE, Geneva (2024)
6. Guerna, A., Bitam, S., Calafate, C.T.: AC-RDV: a novel ant colony system for roadside units deployment in vehicular ad hoc networks. Peer-to-Peer Netw. Appl. **14**(2), 627–643 (2021)
7. Manogaran, G., Saravanan, V., Hsu, C.-H.: Information-centric content management framework for software defined internet of vehicles towards application specific services. IEEE Trans. Intell. Transp. Syst. (2021). https://doi.org/10.1109/TITS.2021.3058452
8. Salami, Y., Khajehvand, V.: LSKE: Lightweight secure key exchange scheme in fog federation. Complexity **2021**, 4667586 (2021)
9. Jandial, A., Merdrignac, P., Shagdar, O., Fevrier, L.: Implementation and evaluation of intelligent roadside infrastructure for automated vehicle with I2V communication. In: Vehicular Ad-hoc Networks for smart cities, pp. 3–18. Springer, Berlin (2020)
10. Salami, Y., Hosseini, S.: BSAMS: blockchain-based secure authentication scheme in meteorological systems. Nivar **47**(120–121), 181–197 (2023)
11. Salami, Y., Vahid, K., Zeinali, E.: Efficiency simultaneous key exchange-cryptography extraction from public key in fog-cloud federation-based secure offloading for automatic weather stations observing systems. Nivar **47**(120–121), 153–165 (2023). https://doi.org/10.30467/nivar.2023.416270.1261
12. Zhao, D., Peng, H., Li, L., Yang, Y.: A secure and effective anonymous authentication scheme for roaming service in global mobility networks. Wirel. Pers. Commun. **78**(1), 247–269 (2014). https://doi.org/10.1007/s11277-014-1750-y
13. Mohit, P., Amin, R., Biswas, G.P.: Design of authentication protocol for wireless sensor network-based smart vehicular system. Veh. Commun. **9**(February), 64–71 (2017)
14. Ying, B., Nayak, A.: Anonymous and lightweight authentication for secure vehicular networks. IEEE Trans. Veh. Technol. **66**(12), 10626–10636 (2017)
15. Vasudev, H., Deshpande, V., Das, D., Das, S.K.: A lightweight mutual authentication protocol for V2V communication in internet of vehicles. IEEE Trans. Veh. Technol. **69**(6), 6709–6717 (2020)
16. Salami, Y., Khajehvand, V., Zeinali, E.: SOS-FCI: a secure offloading scheme in fog–cloud-based IoT. J. Supercomput. **80**(1), 570–600 (2024). https://doi.org/10.1007/s11227-023-05499-3
17. Salami, Y., Khajehvand, V., Zeinali, E.: A new secure offloading approach for internet of vehicles in fog-cloud federation. Sci. Rep. **14**(1), 5576 (2024)
18. Mun, H., Han, K., Lee, Y.S., Yeun, C.Y., Choi, H.H.: Enhanced secure anonymous authentication scheme for roaming service in global mobility networks. Math. Comput. Model. **55**(1–2), 214–222 (2012). https://doi.org/10.1016/j.mcm.2011.04.036
19. Salami, Y., Khajehvand, V.: SMAK-IOV: secure mutual authentication scheme and key exchange protocol in fog based IoV. J. Comput. Robot. **13**(1), 11–20 (2020)
20. Salami, Y., Khajehvand, V., Zeinali, E.: SAIFC: a secure authentication scheme for IOV based on fog-cloud federation. Secur. Commun. Networks **1**, 1–19 (2023)
21. Salami, Y., Ebazadeh, Y., Khajehvand, V.: CE-SKE: cost-effective secure key exchange scheme in fog federation. Iran. J. Comput. Sci. **4**(3), 1–13 (2021)
22. Wazid, M., Bagga, P., Das, A.K., Shetty, S., Rodrigues, J.J.P.C., Park, Y.: AKM-IoV: authenticated key management protocol in fog computing-based internet of vehicles deployment. IEEE Internet Things J. **6**(5), 8804–8817 (2019)
23. Salami, Y., Khajehvand, V., Zeinali, E.: LSMAK-IOV: lightweight secure mutual AKE Scheme in fog-based IoV. In: 2024 10th international conference on artificial intelligence and robotics (QICAR), pp. 1–5. IEEE, Geneva (2024)
24. Chen, C.M., Xiang, B., Liu, Y., Wang, K.H.: A secure authentication protocol for internet of vehicles. IEEE Access **7**(c), 12047–12057 (2019)
25. Armando, A., et al.: The AVISPA tool for the automated validation of internet security protocols and applications. In: Etessami, K., Rajamani, S.K. (eds.) Computer aided verification, pp. 281–285. Springer Berlin Heidelberg, Berlin Heidelberg (2005)
26. "Avispa." Available: http://www.avispa-project.org/. Accessed 1 Sept 2017
27. Basin, D., Mödersheim, S., Viganò, L.: An on-the-fly model-checker for security protocol analysis. Lect. Notes Computer Sci. **2808**(3), 253–270 (2003). https://doi.org/10.1007/978-3-540-39650-5_15
28. Turuani, M.: The CL-Atse protocol analyser. In: Pfenning, F. (ed.) Term rewriting and applications, pp. 277–286. Springer, Berlin Heidelberg (2006)
29. Armando, A., Compagna, L.: SATMC: A SAT-based model checker for security protocols. In: Alferes, J.J., Leite, J. (eds.) Logics in artificial intelligence, pp. 730–733. Springer, Berlin Heidelberg (2004)
30. Boichut, Y., Kosmatov, N., Vigneron, L.: Validation of Prouvé protocols using the automatic tool TA4SP. TFIT **6**, 467–480 (2006)
31. "NS3." Available: https://www.nsnam.org. Accessed 1 June 2025