International Journal of Advances in Applied Sciences (IJAAS)
Vol. 15, No. 3, September 2026, pp. 1006~1014
ISSN: 2252-8814, DOI: 10.11591/ijaas.v15.i3.pp1006-1014

Hybrid lightweight encryption and searchable security framework for secure VANET image and text data sharing

Fairouz Sherali, Falah Sarhan
Department of Mathematics, Education College for Girls, Kufa University, Najaf, Iraq

Article Info

Article history:

Received Jul 11, 2025
Revised Jun 3, 2026
Accepted Jun 17, 2026

Keywords:

Bilinear pairing
Cloud computing
Searchable encryption
Spritz stream cipher
Vehicular ad hoc networks

ABSTRACT

The increasing reliance on vehicular ad hoc networks (VANETs) for instantaneous traffic orchestration and data exchange highlights the need for robust, efficient, and privacy preserving security solutions. Classical encryption methods often fail to meet the low-latency and lightweight requirements of vehicular environments. In this study, a hybrid cryptographic framework was designed that integrates searchable encryption (SE) with the Spritz stream cipher, targeting secure keyword-based access to encrypted data. By leveraging bilinear pairing for identity-based key management, the system enables flexible authentication and secure updates. Both text and image data are supported, with minimal computational overhead. Experimental results validate the feasibility of the approach in dynamic, resource-limited vehicular networks.

Corresponding Author:

Falah Sarhan
Department of Mathematics, Education College for Girls, Kufa University
Najaf 00964, Iraq
Email: falahh.sarhan@uokufa.edu.iq

1. INTRODUCTION

Over the past ten years, technology has advanced dramatically, creating new means of information sharing and device and system connectivity. Vehicular ad hoc networks (VANETs) and the internet of things (IoT) are two of the most significant innovations. The IoT encompasses a vast array of internet-connected smart devices, including industrial machines, wearable technology, sensors, and residential systems, that can function with little to no human intervention. VANETs, in contrast, allow vehicles to communicate directly with each other and with nearby infrastructure, aiming to improve traffic flow, reduce collisions, and support autonomous driving [1], [2].

These two technologies are extensively utilized in contemporary domains like automated manufacturing, smart residences, intelligent transportation, and healthcare monitoring. Concerns about data security and safety are growing along with their use. Data in IoT and VANET systems is susceptible to malicious attacks, data theft, and unauthorized access since it is transmitted wirelessly and frequently in public settings. For instance, an attack on a healthcare sensor might jeopardize sensitive patient data, while a security lapse in a smart car communication system could result in risky miscommunications between cars [3].

Encryption is one of the most important ways to safeguard such systems. By converting readable data into a coded format that only trustworthy parties may access or decipher, encryption functions. This procedure is essential for protecting data privacy and making sure it wasn't altered while being transmitted. However, the low processing and storage capacity of many IoT devices makes it challenging to use common encryption technologies. Similar to this, VANET systems need to communicate quickly in real time, which makes elaborate or slow security procedures difficult to implement [4]–[6].

As IoT and VANET systems become more and more used in everyday life and the necessary infrastructure, it is more necessary than ever to make sure they are secure. Constructing encryption mechanisms that are both robust and lightweight is a main issue because classical methods often outperform low-resource devices or impede communication in high-mobility settings like vehicular networks. Therefore, it has become clear that innovative and modern encryption solutions that support high secrecy and performance are in demand.

To address these challenges, this paper introduces a novel secure data sharing framework for VANET environments that combines searchable encryption (SE) with the lightweight Spritz stream cipher. This integration enables privacy-preserving keyword search on encrypted vehicular data without compromising system responsiveness. The proposed solution supports multi-user authentication, dynamic updates, and strong resistance to attacks such as keyword guessing and data inference, making it well-suited for real-time, resource-constrained vehicular communication.

Unlike previous studies, this work uniquely integrates lightweight encryption and efficient search mechanisms within a unified framework tailored specifically for the high-mobility and low-latency requirements of 5G-enabled VANETs. Several studies have addressed secure data sharing in VANET-cloud environments. For instance, Hegde *et al.* [7] suggest a secure, SE method developed for VANET-cloud environments. The authors use a random query trapdoor mechanism and Bloom filters to enable keyword-based search over encrypted vehicular data without compromising privacy. By employing bilinear pairing and hash-based indexing, the scheme ensures both efficiency and resistance against query pattern leakage. It supports dynamic updates, low computation costs, and secure keyword matching.

An improved authentication method for VANETs that satisfies a balance between effectiveness, security, and user privacy is proposed [8]. By offering conditional traceability and defense against forgery and replay attacks, it enhances current methods. For fast authentication appropriate for vehicular settings, the method employs lightweight operations and elliptic curve cryptography. Its superiority in terms of computational and communication overhead is confirmed by performance studies.

Kang *et al.* [9] studied the integration of blockchain technology into vehicular edge computing to allow the secure sharing of vehicle information. It surveys existing solutions to protect data sharing in VANETs, identifies their limitations, and emphasizes how blockchain can provide decentralized authentication, tamper resistance, and efficient data access management, making it a strong candidate for future vehicular networks. Yan *et al.* [10] present a secure access control framework that combines blockchain with attribute-based searchable encryption (ABSE). This design ensures data confidentiality, fine-grained access control, and efficient keyword search over encrypted data. It also supports dynamic updates and resists collusion and keyword-guessing attacks, making it suitable for decentralized environments such as IoT and VANETs.

In their study, Wang *et al.* [6] suggested a lightweight and efficient strong privacy preserving authentication scheme (LESPP), a lightweight and efficient authentication method for secure and private communication in VANETs. This method utilizes self-generated pseudonymous identities and relies on symmetric encryption and message authentication codes (MACs), enabling fast signing and verification without the need for computationally intensive public-key cryptography. Compared to existing public-key-based schemes, LESPP attained a 102 to 103 reduction in computation cost and decreased communication overhead by 41–77.60 while providing resilience against denial-of-service (DoS) attacks. The key management center keeps the ability to reveal real identities if necessary, preserving user privacy and hindering vehicle tracking even when roadside units are compromised.

Recent works between 2022 and 2025 show significant progress in searchable and attribute-based encryption schemes suitable for VANETs. Yan *et al.* [11] present a survey on ABSE, highlighting improvements in computational efficiency, policy hiding, and flexibility in IoT and vehicular contexts [11]. Other research integrates ciphertext-policy attribute-based encryption (CP-ABE) with blockchain and revocable access control for vehicular data sharing, e.g., a dynamic social vehicular network (DSVN) model employing outsourced revocable ciphertext-policy attribute-based encryption (ORCP-ABE) with user attribute revocation and outsourced encryption to reduce overhead [12].

2. PRELIMINARIES

This section outlines the foundational concepts and cryptographic tools used in this research. Understanding the principles of VANET communication, bilinear pairing, the lightweight Spritz cipher, and SE is essential. These principles are important for appreciating the design and security of proposed system.

2.1. Vehicular ad hoc networks

VANETs are a tailored form of mobile ad hoc networks (MANETs), where vehicles fitted with on-board devices (OBUs) interact dynamically with each other and with fixed roadside units (RSUs) to support real-time data exchange, such as traffic alerts, road safety notifications, and information and entertainment services. VANETs are critical components of intelligent transportation systems (ITS) and need

ultra-fast, secure communication as a consequence of their high mobility and dynamic topology. Due to the openness of wireless communication and the security-critical content exchanged, ensuring data integrity, authentication, and privacy is of paramount importance [13]–[15].

Furthermore, the VANET environment requires exacting restrictions on latency and scalability, demanding the use of lightweight encryption techniques that do not compromise real-time responsiveness, even as nodes continuously join, leave, or move between network clusters. In the proposed system, the communication model supports both vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) interactions. V2V is primarily used for direct data exchange, such as accident alerts and traffic updates, while V2I enables vehicles to upload encrypted data to the cloud via roadside units. The scheme is designed to operate under strict latency constraints (typically < 50 ms for safety-critical messages) and can dynamically adapt to node mobility, allowing vehicles to seamlessly join or leave network clusters without disrupting secure communication.

2.2. Searchable encryption

SE allows secure keyword search via encrypted data without decryption, protecting both data confidentiality and query privacy. For instance, in vehicle social networks, dual policy attribute-based SE employs bilinear pairings to enable identity-based access controls and dynamic updates. Furthermore, searchable symmetric encryption (SSE) provides an efficient method for encrypted search in a cloud server (CS) [16]–[19].

Recent advancements have focused on adapting SE to resource-limited settings such as VANET and IoT. Utilizing enhanced cryptographic primitives, lightweight SE techniques decrease computing cost while preserving robust security assurances, specifically against keyword guessing and unauthorized access. Furthermore, new hybrid schemes that integrate SE with stream ciphers, like Spritz, improve performance while conducting encrypted searches across text and multimedia [7], [20], [21].

2.3. Bilinear pairings

Through index trapdoors or ciphertext retrieval, bilinear pairings enable identity-based key generation and SE constructions [22]. This primitive is used to create secure keyword indices in VANET-cloud search strategy [23]. These pairings satisfy the criteria of efficient computability, non-degeneracy, and bilinearity. They are defined over two cryptographic groups, G_1 and G_2, mapping to a target group, G_T [24].

Pairing-based constructions allow efficient and secure authentication in the VANET context, leveraging identity-based cryptography to facilitate key management and decrease infrastructural overhead. Current systems have used bilinear pairings in signcryption algorithms to simultaneously ensure confidentiality and integrity during V2I communications. Further, the integration of pairings in dynamic SE schemes allows real-time updates and scalable keyword search in vehicular clouds while maintaining robust security guarantees such as forward secrecy and user authentication [25], [26].

2.4. Spritz stream cipher

Spritz, a lightweight sponge-based stream cipher, offers efficient encryption and MAC support—perfect for VANET nodes with limited resources. Further, it has better randomness quality than earlier ciphers like RC4 [27], [28]. Because of its permutation-based internal state and byte-oriented design, Spritz is highly suitable for software implementations in embedded vehicular components. Its adaptability allows for both encryption and hashing operations within the same structure, decreasing the need for multiple cryptographic modules. Spritz has lower latency and memory cost than block ciphers, which is essential for real-time VANET communication [29], [30]. Additionally, contemporary studies have revealed that Spritz is resilient to state collision and key recovery attacks, reinforcing its suitability for use in adversarial and dynamic environments [31].

2.5. Image quality and statistical analysis

Evaluating the integrity and robustness of encrypted images relies on well-established metrics such as peak signal-to-noise ratio (PSNR), correlation coefficients, and entropy [32]:

- PSNR is a standard measure used to quantify reconstruction quality. It compares the maximum possible power of a signal (image) versus the power of corrupting noise, expressed in decibels.
- Correlation coefficient analysis determines the level of statistical dependency between adjacent pixels. In a secure, encrypted image, pixel correlation should be near zero—indicating strong diffusion of image data.
- Entropy, especially Shannon entropy, evaluates the randomness of pixel value distributions. Ideal encryption schemes push entropy values toward the maximum (e.g., ~ 8 bits for an 8-bit grayscale image), thereby minimizing information leakage.
- Practical experiments also incorporate noise/crop robustness—e.g., tests involving salt-and-pepper noise and data cut attacks use PSNR to confirm the algorithm's ability to maintain structural fidelity.

3. DETAILS OF THE PROPOSED SCHEME: BLOCKCHAIN-BASED LIGHTWEIGHT NETWORK SECURITY PROTOCOL

Strong security and high-efficiency encryption techniques are essential due to the rapid expansion of networked digital systems, including cloud platforms, mobile and wireless networks, the IoT, VANETs, and healthcare monitoring devices. Encryption techniques frequently encounter a trade-off between processing efficiency and computational cost. Bilinear pairings, for instance, offer strong cryptographic features such as high confidentiality. However, their intensive computational requirements make them unsuitable for encrypting large amounts of data, particularly in environments with limited processing resources. While stream cipher algorithms such as Spritz, a newer version of RC4, support the encryption of large amounts of data, they lack key management and authentication mechanisms.

This paper suggests a hybrid encryption algorithm, named blockchain-based lightweight network security protocol (BLN-SP), that combines lightweight cryptography, secure authentication, and privacy-preserving SE to handle the key challenges of data confidentiality, effective communication, and secure storage in IoT and VANET environments. The BLN-SP framework consists of two encryption layers. The first layer utilizes a lightweight stream cipher (Spritz) to efficiently encrypt both text and image data generated by vehicular nodes. For text data, a direct byte-oriented keystream is applied, while image data is processed in blocks to preserve integrity and minimize latency. The second layer is responsible for secure key management and distribution using bilinear pairing, ensuring that symmetric keys are dynamically generated and refreshed without relying on a centralized authority. On top of these layers, the framework incorporates SE, which enables secure keyword-based search over encrypted vehicular data stored in the cloud. This integration ensures that while data confidentiality is maintained through strong encryption, efficient and privacy-preserving query capabilities are still supported for real-time VANET applications. The proposed system is structured into three functional phases: i) sending vehicle (SV) phase, ii) receiving vehicle (RV) phase, and iii) CS phase. Each vehicle can act as a data sender or receiver depending on its role in the communication scenario. The data flow proceeds as follows.

3.1. Sending phase: sending vehicle (data generation and encryption)

In this phase, the SV collects raw data like speed logs, traffic conditions, accident reports, global positioning system (GPS) coordinates, or road hazard alerts. If the data includes images (e.g., of road conditions or vehicle incidents), the vehicle extracts metadata (such as timestamp, location, vehicle type, or license plate) and generates a set of relevant keywords. The raw data is then encrypted using the Spritz algorithm. The keywords are securely encoded using the index (IDX) algorithm to construct a searchable index. The encrypted data and its index are uploaded to the CS.

Mathematically, SV initiates the scheme by running a key generation (KE-Gen) algorithm, which involves two steps. First: choose an elliptic curve group G of order p and create the following parameters: Q is a random generator of G, a bilinear map e: $G \times G \rightarrow Gy$, two public keys, one for the sender vehicle PK_{SV} and the other for the receiver vehicle PK_{RV} and two secret keys Sk_{SV} and Sk_{RV} for sender and receiver, respectively. Then, compute the shared secret key K_{BLN} for two parties. Second: Initialize the state vector $S = [0,1,2, \ldots 255]$, and build a keystream K_{Spritz} by transforming the shared secret key SV and RV from points on the elliptic curve to bytes. Spritz algorithm absorbs the K_{spritz} in the state vector. Then, (shuffle) swap and mix the state vector values to ensure randomness. Finally, calculate the keystream K_{SPR} based on the state vector S. To protect the sender vehicle's data privacy, SV first uses the file encryption (F-ENC) algorithm to create the searchable index IDX; the algorithm extracts the mentioned keywords from the extracted metadata and then constructs the identifier collection of files containing each keyword. Second, the F-ENC algorithm encrypts the IDX using K_{BLN}, and metadata using K_{SPR} before uploading them to CS.

3.2. Receiving phase: receiving vehicle (search query generation)

In this phase, an RV needing access to specific encrypted information in CS (e.g., recent accidents near its location), RV generates a trapdoor as a search request for the searchable keyword in IDX, using the trapdoor generator algorithm (T-GEN) based on the target keyword. To ensure secure search, each keyword extracted from vehicular metadata is mapped to a unique cryptographic identifier using a hash-based function. The RV then generates a non-reversible trapdoor by encrypting this identifier with its session key and pairing parameters. This prevents the CS from inferring the original keyword and ensures that identical queries remain indistinguishable, mitigating keyword guessing and search-pattern attacks.

3.3. Retrieval phase: cloud server (search query)

In this phase, upon receiving the trapdoor from the RV, the CS uses the searchable index algorithm (SRCH-IDX) algorithm to check the stored searchable indexes and compares each encrypted trapdoor with all encrypted keywords saved in IDX. If the trapdoor matches any keyword in IDX, then CS returns the corresponding encrypted data (e.g., images or sensor logs) to the RV. Finally, RV can decrypt the encrypted

data using the shared secret key derived earlier by the Spritz algorithm K_{SPR}, ensuring end-to-end confidentiality. In this scheme, CS is considered an honest but inquisitive adversary; the server dutifully executes the suggested algorithm but is curious about the keywords and the encrypted file contents. Algorithms 1 to 4 are the details of algorithms KE-Gen, F-ENC, T-GEN, and SRCH-IDX.

Algorithm 1. KE-Gen
A: apply the bilinear pairings
1: generate a prime number p, and select a random generator Q of G,
2: choose an elliptic curve group G of order p,
3: build a bilinear map $G \times G \rightarrow Gy$,
4: pick a random SK_{SV} and SK_{RV},
5: calculate the public keys, $PK_{SV} = Sk_{SV}Q$ and $PK_{RV} = Sk_{RV}Q$.
6: calculate the shared key, K_{BLN}= $e(Pk_{SV}, Sk_{RV}.Q)$= $e(Pk_{RV}, Sk_{SV}.Q)$=$(Q,Q)^{Sk_{SV}Sk_{RV}}$.
B: apply the Spritz algorithm
1: convert K_{BLN} to an array of bytes, K_{Spritz}, and use it as a seed for Spritz cipher,
2: build a state array with 256 elements, S = [0,1,…,255],
3: absorb the elements of K_{Spritz} into the state array S by adding each byte to the current element in S,
4: shuffle the elements of S,
6: generate keystream K_{SPR},
7: return K_{SPR}.

Algorithm 2. F-ENC
1: SV creates the searchable index IDX for all searchable keywords,
2: SV encrypts the IDX, XOR the text of IDX with K_{BLN} and uploads it to CS,
3: SV encrypts the data, XOR the text with keystream K_{SPR} and uploads it to CS.

Algorithm 3. T-GEN
1: RV selects the trapdoors,
2: encrypts the trapdoors using K_{BLN}
3: send to the CS.

Algorithm 4. SRCH-IDX
1: CS tests the stored searchable indexes and compares each encrypted trapdoor with all encrypted keywords saved in IDX,
2: CS retrieves all files corresponding to the trapdoors.

4. THREAT MODEL

The system assumes an honest-but-curious CS that executes operations correctly but attempts to infer sensitive information such as keywords or message contents. Potential adversaries may include external attackers who attempt to intercept vehicular messages, inject false data, or perform replay and Sybil attacks. Internal adversaries, such as compromised vehicles or RSUs, may attempt to misuse valid credentials to access unauthorized data. Attack surfaces include wireless communication channels, cloud storage, and keyword search requests. The proposed BLN-SP scheme mitigates these threats by employing bilinear-based mutual authentication, non-reversible trapdoors, session-based symmetric keys, and timestamped tokens to prevent replay attacks. This layered security model ensures resilience against keyword guessing, data inference, impersonation, and traffic analysis attacks.

5. RESULTS AND DISCUSSION

This section presents a wide evaluation of the proposed encryption technique, integrating Spritz and bilinear pairing within a VANET context. Multiple metrics are used to assess the performance, involving authentication delay, encryption time, and image quality indicators. To prove the efficiency and practicality of the proposed method, results are compared against classic encryption standards. Advanced encryption standard (AES) is a pertinent baseline for comparison among these, since it is often used to secure uploaded data in cloud environments [33]. In contrast, the suggested technique assumes using the lightweight Spritz cipher, where the initial key is securely derived through bilinear pairing. This combination focuses on reducing the computational overhead while preserving strong security, particularly suited for the resource-constrained and latency-sensitive nature of VANETs.

5.1. Text data encryption time analysis

Table 1 depicts the encryption time consumed for various message lengths using the proposed method. AES encryption times are also given for comparison. Even though AES is faster (e.g., 2.7 ms for 128 bytes vs. 5.4 ms for the hybrid technique), it does not allow more sophisticated features like multi-user authentication and SE [34]. Table 1 illustrates that while the suggested method has a small overhead in comparison to AES, it allows for tighter key management and SE.

Table 1. Text encryption time comparison

Message size (bytes)	BLN-SP (ms)	AES (ms)
128	5.4	2.7
256	6.4	2.5
512	7	3.3
1,024	9.7	4.2
2,048	12.4	6.7

5.2. Image encryption time and quality analysis

Table 2 demonstrates the consumed encryption times for images of different resolutions and sizes. The results show that encryption time rises with image size, reaching around 32.9 ms for a 400 KB image and ~ 7.5 ms for a 10 KB image. The proposed method adds cost from pairing procedures in contrast to AES, which is much faster for image encryption. Using standard image security measures, Table 3 assesses the statistical integrity and visual quality of encrypted images using BLN-SP. The PSNR values show effective visual distortion. High entropy and low correlation demonstrate strong confusion and diffusion effects, confirming image encryption robustness.

Table 2. Image encryption time comparison

Image type	Size (approx.)	BLN-SP (ms)	AES (ms)
Small grayscale icon	10 KB	8.4	4.2
Medium grayscale image	25 KB	11.6	6.6
Small color image	40 KB	13.8	7.5
Medium-color image	120 KB	19.6	11.6
Large color image	400 KB	33.7	18.5

Table 3. Encrypted image quality metrics

Image type	PSNR (dB)	Correlation coefficient	Entropy (bits)
Grayscale (10 KB)	7.6	0.016	7.80
Color (40 KB)	6.2	0.014	7.92
Color (400 KB)	6.3	0.007	7.93

5.3. Security discussion

Regarding security, the proposed technique ensures robust security against a number of different common attacks, such as keyword guessing attacks (KGA), chosen keyword attacks (CKA), and data inference attacks. These protections are not inherently supported by AES-based systems unless augmented with additional protocols. The combination of Spritz with bilinear pairing strengthens the encryption scheme and ensures that both content and metadata remain secure.

5.4. Search efficiency and keyword privacy

The suggested method allows secure and efficient keyword search via encrypted data. To maintain data privacy, users can search without exposing the keywords or search patterns. SE enables real-time access to relevant vehicular data while preserving privacy, which is quite useful in emergency communication and traffic updates in VANET systems.

5.5. Storage overhead and scalability

The novel BLN-SP system presents a comprehensive approach for vehicular networks, efficiently handling the trade-off between superior performance and storage efficiency. Although its SE, employing bilinear pairing, fundamentally requires modestly higher memory usage than basic AES, this overhead is merited. The superior capabilities it empowers—such as enabling multiple clients and dynamic data updates.

Importantly, the scheme is designed for scalability. As depicted in Figure 1, memory overhead increases in a near-linear manner with the number of records, maintaining stable performance as the network

expands. Notably, its innovative dual-layer and integrated design make it significantly efficient. BLN-SP ultimately reduces total memory overhead by 25-30% compared to a traditional AES-based VANET scheme. This unified approach delivers robust security and scalability with minimal storage cost.

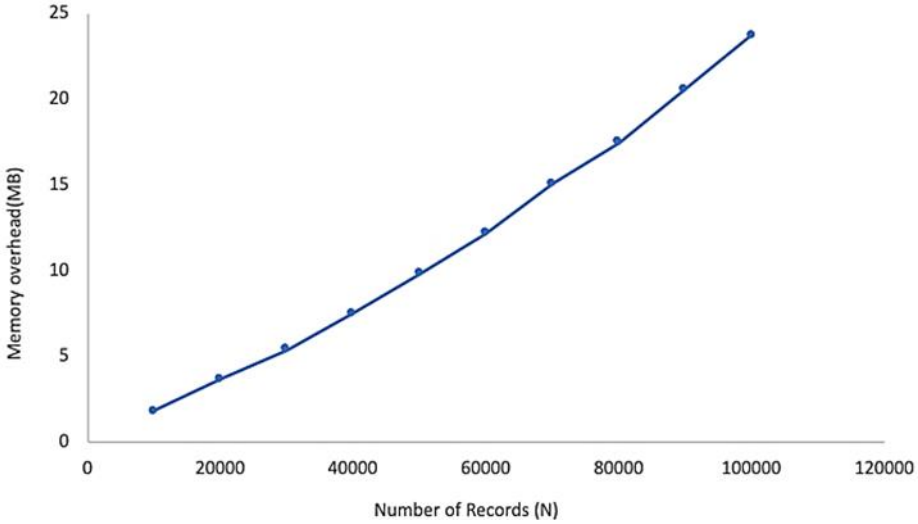

Figure 1. Memory overhead vs number of records (BLN-SP framework)

5.6. Authentication strength evaluation

To ensure that only authorized nodes (vehicles and RSUs) are able to communicate and exchange data, authentication is essential in VANETs. As Table 4 illustrates, weak authentication can result in attacks such as message tampering, impersonation, and Sybil attacks. These attacks can jeopardize traffic safety. Table 5 summarizes the authentication-related performance of the proposed scheme in a simulated VANET network of over 200 vehicles.

5.7. Comparative analysis of AES-based methods

Although AES has a shorter encryption time, it is devoid of more sophisticated properties like forward secrecy, SE, and decentralized multi-user authentication. Performance and feature richness are traded off in the proposed system. This trade-off makes sense in dynamic VANET settings.

Table 4. Key security properties supported

	Supported by BLN-SP	Mechanism
- Resistance against Sybil attack	Yes	Unique, non-forgeable identities formed by pairing-based public keys
- Scalability	High	-
- Anonymity Support	Optional	Pseudonym generation using symmetric Spritz keys
- Forward Secrecy	Yes	New keys are generated for each session based on “number used once.”
- Resistance against replay attack	Yes	Session tokens and timestamps ensure secure, fresh communication
- Mutual Authentication	Yes	Bilinear pairing enables identity-driven key generation.

Table 5. Authentication metrics

Metric	Value	Notes
Time of authentication for each vehicle	~ 3.7 ms	Involves identity and session key verification
Rate of successful authentication	> 99.2%	Assessed in a high-density VANET scenario
False acceptance rate (FAR)	< 0.5%	Under impersonation attempts
Overhead key update	~ 1.7 ms	Lightweight because of Spritz key generation

6. CONCLUSION

This paper revealed how to make a lightweight and secure way to share data in VANET environments by combining bilinear-based SE with the Spritz stream cipher. The proposed BLN-SP scheme maintains strict privacy rules while ensuring effective keyword search over encrypted vehicle data. The performance study showed low encryption and authentication delays, as well as strong resilience to common

cryptographic threats. PSNR, entropy, and correlation measures were used in image-based evaluation to further confirm the robustness of proposed method. The proposed scheme demonstrated better adaptability to resource-constrained vehicular nodes than conventional AES-based schemes. Although BLN-SP provides strong security and efficiency, it doesn't work well with large vehicular networks where nodes move around a lot. It is still a challenge to make it resistant to collusion attacks and work well in real time when there is a lot of traffic. Subsequent studies will focus on adaptive key update strategies and edge-assisted computation to enhance scalability, responsiveness, and resilience against mobility-based threats.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Fairouz Sherali	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓			✓
Falah Sarhan	✓	✓	✓	✓	✓	✓	✓		✓	✓		✓	✓	✓

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author, [FS], upon reasonable request.

REFERENCES

[1] A. Dutta, L. M. S. Campoverde, M. Tropea, and F. De Rango, "A comprehensive review of recent developments in VANET for Traffic, safety & remote monitoring applications," *Journal of Network and Systems Management*, vol. 32, no. 4, pp. 1–37, Oct. 2024, doi: 10.1007/s10922-024-09853-5.

[2] A. Rahman *et al.*, "DistB-VNET: distributed cluster-based blockchain vehicular ad-hoc networks through SDN-NFV for smart city," *2024 27th International Conference on Computer and Information Technology, ICCIT 2024*. pp. 3372–3377, Dec. 2024, doi: 10.1109/ICCIT64611.2024.11022025.

[3] S. Sharma and B. Kaushik, "A survey on internet of vehicles: applications, security issues & solutions," *Vehicular Communications*, vol. 20, Dec. 2019, doi: 10.1016/j.vehcom.2019.100182.

[4] K. U. Sarker, "A systematic review on lightweight security algorithms for a sustainable IoT infrastructure," *Discover Internet of Things*, vol. 5, no. 1, pp. 1–20, Dec. 2025, doi: 10.1007/s43926-025-00150-4.

[5] T. K. Venkatasamy, M. J. Hossen, G. Ramasamy, and N. H. B. A. Aziz, "Intrusion detection system for V2X communication in VANET networks using machine learning-based cryptographic protocols," *Scientific Reports*, vol. 14, no. 1, pp. 1–18, Dec. 2024, doi: 10.1038/s41598-024-82313-x.

[6] M. Wang, D. Liu, L. Zhu, Y. Xu, and F. Wang, "LESPP: lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication," *Computing*, vol. 98, no. 7, pp. 685–708, Jul. 2016, doi: 10.1007/s00607-014-0393-x.

[7] N. Hegde, S. S. Manvi, and H. S. Lallie, "Secure search scheme for encrypted data in the VANET cloud with random query trapdoor," *Information Security Journal*, vol. 32, no. 5, pp. 383–400, Sep. 2023, doi: 10.1080/19393555.2022.2081636.

[8] S. Khan, A. Raza, and S. O. Hwang, "An enhanced privacy preserving, secure and efficient authentication protocol for VANET," *Computers, Materials and Continua*, vol. 71, no. 2, pp. 3703–3719, 2022, doi: 10.32604/cmc.2022.023476.

[9] J. Kang *et al.*, "Blockchain for Secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4660–4670, Jun. 2019, doi: 10.1109/JIOT.2018.2875542.

[10] L. Yan, L. Ge, Z. Wang, G. Zhang, J. Xu, and Z. Hu, "Access control scheme based on blockchain and attribute-based searchable encryption in cloud environment," *Journal of Cloud Computing*, vol. 12, no. 1, 2023, doi: 10.1186/s13677-023-00444-4.

[11] L. Yan *et al.*, "Attribute-based searchable encryption: a survey," *Electronics*, vol. 13, no. 9, 2024, doi: 10.3390/electronics13091621.

[12] X. Chen, Y. Chen, X. Wang, X. Zhu, and K. Fang, "DSVN: a flexible and secure data-sharing model for VANET based on blockchain," *Applied Sciences*, vol. 13, no. 1, 2023, doi: 10.3390/app13010217.

[13] L. Wu *et al.*, "An efficient privacy-preserving mutual authentication scheme for secure V2V communication in vehicular ad hoc network," *IEEE Access*, vol. 7, pp. 55050–55063, 2019, doi: 10.1109/ACCESS.2019.2911924.

[14] A. Y. Dak, S. Yahya, and M. Kassim, "A literature survey on security challenges in VANETs," *International Journal of Computer Theory and Engineering*, vol. 4, no. 6, pp. 1007–1010, Dec. 2012, doi: 10.7763/ijcte.2012.v4.627.
[15] S. Wang, Z. Fan, Y. Su, B. Zheng, Z. Liu, and Y. Dai, "A lightweight, efficient, and physically secure key agreement authentication protocol for vehicular networks," *Electronics*, vol. 13, no. 8, 2024, doi: 10.3390/electronics13081418.
[16] T. Peng *et al.*, "An efficient conjunctive keyword searchable encryption for cloud-based IoT systems," *Digital Communications and Networks*, vol. 11, no. 4, pp. 1293–1304, Mar. 2025, doi: 10.1016/j.dcan.2025.03.002.
[17] Z. Shang, S. Oya, A. Peter, and F. Kerschbaum, "Obfuscated access and search patterns in searchable encryption," in *28th Annual Network and Distributed System Security Symposium, NDSS 2021*, 2021, pp. 1–18, doi: 10.14722/ndss.2021.23041.
[18] X. Liu, P. Liu, B. Yang, and Y. Chen, "One multi-receiver certificateless searchable public key encryption scheme for IoMT assisted by LLM," *Journal of Information Security and Applications*, vol. 90, May 2025, doi: 10.1016/j.jisa.2025.104011.
[19] F. Sherali and F. Sarhan, "Searchable encryption based on a chaotic system and AES algorithm," *International Journal of Advances in Applied Sciences*, vol. 14, no. 3, pp. 975–984, 2025, doi: 10.11591/ijaas.v14.i3.pp975-984.
[20] P. Manickam, K. Shankar, E. Perumal, M. Ilayaraja, and K. Sathesh Kumar, "Secure data transmission through reliable vehicles in VANET using optimal lightweight cryptography," in *Advanced Sciences and Technologies for Security Applications*, 2019, pp. 193–204, doi: 10.1007/978-3-030-16837-7_9.
[21] R. Wang, Z. Zhang, P. Zhang, C. Wu, and Z. Yang, "Efficient encrypted semantic search method toward internet of vehicles," *Journal of Supercomputing*, vol. 81, no. 4, pp. 1–35, Mar. 2025, doi: 10.1007/s11227-025-06981-w.
[22] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in Cryptology — CRYPTO 2001*, Berlin, Heidelberg: Springer, 2001, pp. 213–229, doi: 10.1007/3-540-44647-8_13.
[23] F. Sherali and S. Falah, "An efficient two-factor user authentication and key exchange protocol for telecare medical information system," *International Journal of Mathematics and Computer Science*, vol. 15, no. 4, pp. 1015–1027, 2020.
[24] M. Al-Qutayri, C. Yeun, and F. Al-Hawi, "Security and privacy of intelligent VANETs," in *Computational Intelligence and Modern Heuristics*, IntechOpen, 2010, doi: 10.5772/7815.
[25] I. Ali, Y. Chen, M. Faisal, and M. Li, "Authentication scheme for vehicle-to-infrastructure communications using bilinear pairing," in *Efficient and Provably Secure Schemes for Vehicular Ad-Hoc Networks*, Singapore: Springer, 2022, pp. 43–65, doi: 10.1007/978-981-16-8586-6_3.
[26] I. Ali, Y. Chen, M. Faisal, and M. Li, "Bilinear pairing-based signcryption scheme for secure heterogeneous vehicle-to-infrastructure communications in VANETs," in *Efficient and Provably Secure Schemes for Vehicular Ad-Hoc Networks*, Singapore: Springer, 2022, pp. 147–173, doi: 10.1007/978-981-16-8586-6_7.
[27] R. L. Rivest and J. C. N. Schuldt, "Spritz—a spongy RC4-like stream cipher and hash function." people.csail.mit.edu, 2014. [Online]. Available: http://people.csail.mit.edu/rivest/pubs/RS14.pdf
[28] R. Roșie, "Randomness of spritz via dieharder testing," 2015, *arXiv:1502.01763*.
[29] O. Alfandi, A. Bochem, A. Kellner, C. Göge, and D. Hogrefe, "Secure and authenticated data communication in wireless sensor networks," *Sensors*, vol. 15, no. 8, pp. 19560–19582, Aug. 2015, doi: 10.3390/s150819560.
[30] M. Khan, H. Dagenborg, and D. Johansen, "Performance evaluation of lightweight stream ciphers for real-time video feed encryption on ARM processor," *Future Internet*, vol. 16, no. 8, 2024, doi: 10.3390/fi16080261.
[31] S. Banik and T. Isobe, "Cryptanalysis of the full Spritz stream cipher," in *Fast Software Encryption (FSE 2016)*, Berlin, Heidelberg: Springer, pp. 63–77, doi: 10.1007/978-3-662-52993-5_4.
[32] P. Sarosh, S. A. Parah, and G. M. Bhat, "An efficient image encryption scheme for healthcare applications," *Multimedia Tools and Applications*, vol. 81, no. 5, pp. 7253–7270, Feb. 2022, doi: 10.1007/s11042-021-11812-0.
[33] F. Sherali, "A new approach for enhancing AES-based data encryption using ECC," *International Journal of Mathematics and Computer Science*, vol. 19, no. 1, pp. 229–235, 2024.
[34] D. L. Evans, P. J. Bond, and K. H. Brown, *Advanced encryption standard (AES)*, Gaithersburg, Maryland: Federal Information Processing Standards Publication (FIPS), 2023, doi: 10.6028/NIST.FIPS.197-upd1.

BIOGRAPHIES OF AUTHORS

Fairouz Sherali is a professor in the Department of Mathematics, Kufa University, Iraq. She received her Ph.D. in Information Security from Huazhong University in 2017. Her main teaching and research interests include developing searchable encryption algorithms in cloud computing. She has published several research articles in International Journals of Mathematics and Computer Science. She can be contacted at email: fairoozm.jaafar@uokufa.edu.iq.

Falah Sarhan is a professor at the Department of Mathematics, Kufa University, Iraq. He received his Ph.D. in numerical analysis from Huazhong University in 2017. His main teaching and research interests include numerical analysis and applied mathematics. He has published several research articles in International Journals of Mathematics and Computer Science. He can be contacted at email: falahh.sarhan@uokufa.edu.iq.