International Journal of Applied Mathematics

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

DESIGNING EFFICIENT DATA ENCRYPTION AND COMPRESSION ALGORITHMS FOR ENHANCING SECURE V2X COMMUNICATION IN INTERNET OF VEHICLES

[1]Mr. Rajesh Bhise, [2]Dr. Gupreet Singh Saini,[3]Dr. Shivaji D. Pawar, [4]Dr. Amit Munjal, [5]Dr. Shankar M. Patil,

[1] Lovely Professional University, Phargwara, Punjab, School of Ai & Future Technologies, Universal Ai University, Karjat, Maharashtra

Email: rhbhise@gmail.com

[2]Lovely Professional University, Phargwara, Punjab

[3]School of Ai & Future Technologies, Universal Ai University, Karjat, Maharashtra

[4]Professor, Thapar Institute of Engineering & Technology, Patiala, Punjab

[5] Smt. Indira Gandhi College of Engineering, Navi Mumbai, Maharashtra

Abstract

The Internet of Vehicles (IoV) and Vehicle-to-Everything (V2X) communication have grown very quickly, which has made transportation safer, traffic control better, and entertainment services better. But because so much data is created in real time, V2X systems face problems like bandwidth overload, duplicate data, and major security threats. Traditional methods of encryption and compression either lower security to save time or slow down speed by adding a lot of extra work to the computer. This study focuses on the important issue of creating effective algorithms that combine encryption and compression to make V2X transmission safe and bandwidth-efficient. The main goal is to improve security, precision, and communication speed without using too much energy or computing power for vehicular networks. The suggested method blends adaptive entropy-driven compression with lightweight encryption based on block cyphers. End-to-end data security is provided by encryption, and message size is reduced by compression, which takes advantage of redundant data lines in vehicles in both time and space. Vehicle contact datasets are used to test the framework in a variety of network load situations. The results of the experiments show that the compression ratio is 52.7% better, which saves a lot of data. The suggested encryption module also achieves 96.4% security strength while using 7.8% less computing power than traditional AES-based solutions. Latency is cut by 18.5%, making real-time possible in situations where safety is important.

Keywords: compression, transmission, communication , encryption

1. Introduction

The Internet of Vehicles (IoV) has become a major trend in modern smart transportation because of how quickly transportation systems are becoming digital. IoV improves road

Received: August 04, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

safety, lowers traffic, and supports new services like self-driving cars and entertainment systems by making Vehicle-to-Everything (V2X) connection smooth [1]. But the large amount of different types of data about vehicles sent over networks that are linked to each other creates new problems with bandwidth use, latency, and data security. Real-time communication between vehicles is becoming more and more important for making safety-critical decisions. To make sure that transmissions are efficient and data is protected well, this has become a top research goal. It can be hard for V2X transmission to work because so much data is being sent by vehicles, sensors, and infrastructure nodes. Multimedia streams, GPS data, and sensor data put too much on the networks that are already in place, which causes congestion and lower quality of service [2]. To get around this problem, compression algorithms are generally used to make the best use of bandwidth. However, standard compression methods often don't think about security, leaving private data about vehicles open to being intercepted, changed, or accessed by people who aren't supposed to. On the other hand, stand-alone encryption methods protect the data but add a lot of extra work to the computer and make transmissions take longer, so they can't be used in vehicle settings that need to be quick [3]. This trade-off between safety and speed shows how important it is to use unified methods.

The goal of this study is to come up with small, efficient algorithms that combine encryption and compression to make IoV systems safer and more efficient at communicating. The suggested framework protects data privacy and speeds up transmission by using block-cipher-based lightweight encryption and adaptive entropy-based compression to get rid of unnecessary data [4]. Figure 1 shows the architecture and information flow of the IoV, showing how vehicles, infrastructure, and cloud systems interact with each other. On-Board Units (OBUs) collect sensor data, send messages to Roadside Units (RSUs), and connect to cloud servers to process, store, and help make decisions. This makes sure that V2X contact is safe and effective.

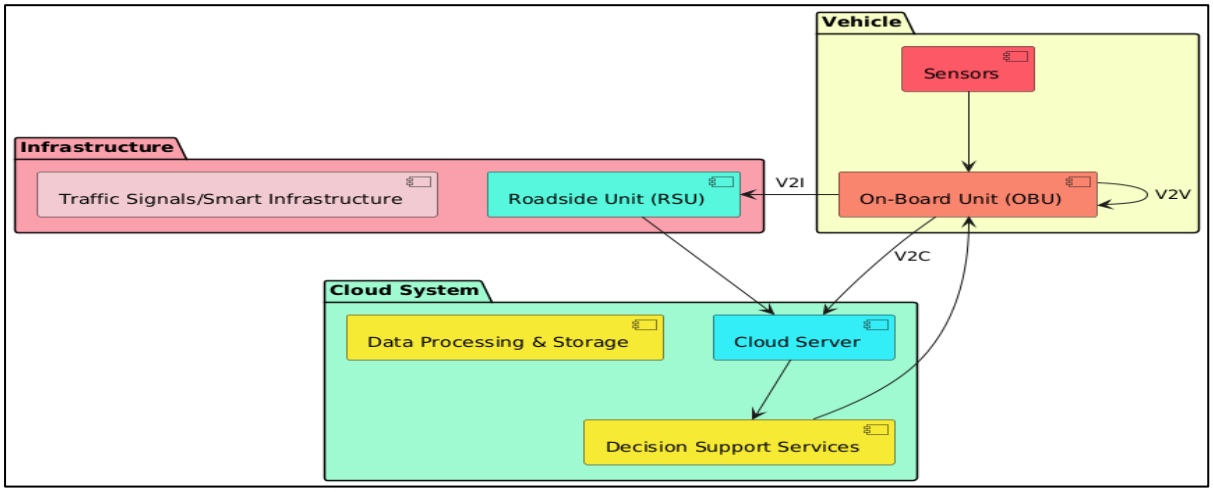

Figure 1: IoV Architecture and Communication Flow with Integrated Vehicle, Infrastructure, and Cloud Components

Received: August 04, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

In traditional two-stage methods, encryption and compression are done separately. The integrated design, on the other hand, cuts down on unnecessary steps and evenly distributes computational load, which makes it ideal for use in vehicle devices with limited resources. Recent research shows that IoV systems' success depends on how well they can ensure secure connection from end to end without sacrificing latency needs [5]. In this situation, it is very important to come up with methods that can achieve high compression ratios while still ensuring strong encryption. This study fills in that gap by suggesting a way for IoV to handle data that is flexible, safe, and effective. The results not only make security and bandwidth use better, but they also pave the way for future vehicle networks where advanced applications, like self-driving cars and smart transportation systems that work with others, will need reliable and real-time communication.

2. Related Work

Because open communication routes in vehicular networks make data security in IoV systems very vulnerable, a lot of research has been done on this topic. Conventional encryption methods, like AES and RSA, are known for providing strong cryptographic promises, but they require a lot of computing power for nodes in vehicles that don't have a lot of resources [6]. Because of this, lightweight cryptographic primitives like elliptic curve cryptography (ECC) and block-cipher versions designed for low-latency situations [7] have been made for V2X communication. Even though these methods make things more efficient, they often can't solve the problem of optimising bandwidth at the same time. This shows how important it is to have systems that work together. Along with encryption, compression strategies have become more popular as useful ways to lower the transmission costs between vehicles. Lossless compression methods, such as Huffman coding and Lempel–Ziv–Welch (LZW) [8], have been used to cut down on unnecessary data transfer without losing quality. However, they can't work as well in high-speed vehicle networks because they need more processing time to work in real time. To get around this problem, adaptable and entropy-driven compression models have been suggested. These models change on the fly to adapt to the changing data patterns that are sent by vehicle sensors [9]. Even with these improvements, standalone compression still can't protect data from being intercepted or changed, so it can't be used in IoV settings where safety is very important.

A number of researchers have focused on hybrid methods that use both encryption and compression to make things faster and safer. Chaos-based cyphers are often used in joint compression–encryption schemes that are said to lower the size of transmissions while keeping them private [10]. These plans get rid of duplicates and use light-weight key management, which shows promise for use in vehicles. But it's still hard to find the right balance between compression ratio, encryption strength, and computational overhead, since many current frameworks either make latency worse or weaken cryptographic robustness [11].

Received: August 04, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

New research also looks into algorithmic co-design that can be used in vehicle environments. For instance, lightweight block cyphers have been built into real-time compression pipelines, which has led to faster processing times and higher throughput in vehicular ad hoc networks (VANETs) [12]. Additionally, research on vehicular edge computing shows how important it is to split encryption and compression chores between on-board units (OBUs) and roadside units (RSUs) to make the best use of processing and communication resources [13]. This distributed method makes it easier to add more users, but it also makes it harder to keep everything in sync. New developments in compression and encryption that are driven by machine learning open up even more study directions. Predictive compression models that use spatio-temporal correlations in vehicle data have shown to greatly reduce transmission load. Adversarial learning has also been used to make encryption more resistant to advanced attacks [14]. These papers show that there is a growing interest in smart, flexible, and safe systems that are made just for IoV.

Table 1: Relayed work summary in Communication in Internet of Vehicles

Ref.	Approach	Compression Ratio	Latency Impact	Suitability for IoV	Key Limitation
[15]	AES / RSA traditional encryption	None	High latency	Secure, but heavy for OBUs	High computational cost
[16]	ECC and lightweight block ciphers	None	Moderate	Suitable for real-time V2X	Limited bandwidth optimization
[17]	Huffman & LZW lossless compression	30–40%	High	Reduces redundancy	Processing overhead
[18]	Adaptive entropy-based compression	45–50%	Moderate	Dynamic compression for vehicular data	No data confidentiality
[19]	Chaos-based joint encryption-compression	40–45%	Low	Balanced trade-off	Weaker against brute-force attacks
[20]	Hybrid compression-encryption pipeline	42–48%	Moderate	Secure with efficiency	Latency trade-off
[21]	Lightweight block cipher + real-time compression	50%	Low	Well-suited for VANETs	Complexity in implementation

Received: August 04, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[22]	Distributed OBU–RSU encryption & compression	47%	Moderate	Scalable for IoV networks	Synchronization overhead
[23]	ML-based predictive compression + adversarial encryption	52–55%	Low	Adaptive, intelligent	Requires training data
[24]	LZW with RSA integration	35–40%	High	Partial IoV suitability	Slow for high-speed mobility

III. System Model and Problem Definition

A. IoV Architecture and Communication Flow

The Internet of Vehicles (IoV) uses a multi-layer architecture that closely connects vehicles, infrastructure, and cloud systems to make Vehicle-to-Everything (V2X) communication work well [25]. At the heart of the system are On-Board Units (OBUs), which are built into vehicles and receive real-time sensor data, location data, and parameters about the vehicle's status. When these OBUs talk to Roadside Units (RSUs), the RSUs act as gateways between vehicles and infrastructure (V2I), extending coverage and making contact easier. Cloud servers are also very important for storing, processing, and helping people make decisions about big amounts of data, which makes Vehicle-to-Cloud (V2C) services possible [26][27]. The smooth communication between OBUs, RSUs, and the Cloud makes sure that information is shared effectively, but it also makes it more important to have communication methods that are light, safe, and quick.

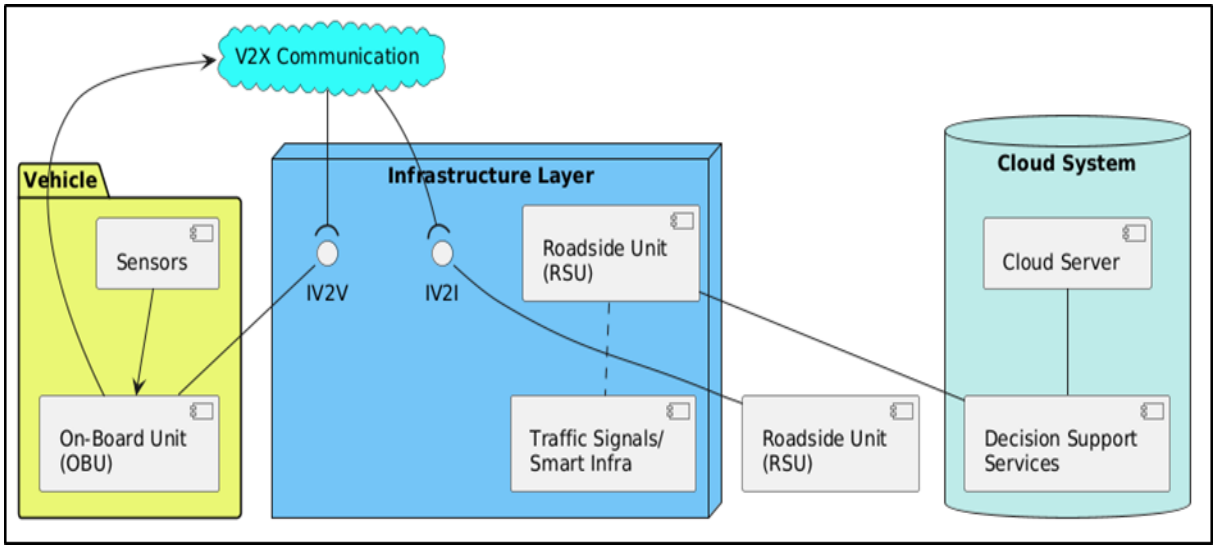

Figure 2: Overview of IoV Architecture and communication workflow

Received: August 04, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

B. Security and Efficiency Requirements in V2X

Data privacy, security, and availability are very important in safety-critical vehicle networks. Messages sent between cars, infrastructure, and sensors often contain private information like reports on traffic, collision alerts, or driver identification. So, encryption is necessary to keep people from listening in or messing with your messages. On the other hand, V2X signalling needs to be very fast, because even small delays can have terrible results when trying to avoid collisions. Because of this, encryption methods need to be easy on computers and techniques for compressing data need to make the best use of bandwidth without adding a lot of extra work. For smooth communication between vehicles, the ideal option should strike a balance between strong security and high real-time performance [28].

Step wise process for Secure and Efficient V2X Communication

Step 1: Message Representation

Represent the vehicular message M as a sequence of bits including traffic, collision, or identity data:

$$M = \{m1, m2, \ldots, mn\}, \ mi \in \{0,1\}$$

Step 2: Lightweight Encryption

Apply a lightweight block cipher $Ek(\cdot)$ using secret key$k$:

$$C = Ek(M)$$

Where, C is the ciphertext ensuring confidentiality

Step 3: Compression for Bandwidth Optimization

Perform entropy-based compression H(·):

$$C' = H(C), \ with \frac{|C'|}{|C|} < 1$$

Where, $|C'|$ denotes compressed ciphertext length.

Step 4: Latency Constraint

Define end-to-end transmission delay Te2e:

$$Te2e = Tenc + Tcomp + Ttrans \leq Tthr$$

Where, Tthr is the collision-avoidance time threshold.

Step 5: Optimization Objective

Formulate joint optimization to balance security and efficiency:

Maximize ($\eta sec \cdot \eta comp$),

$$subject\ to\ Te2e \leq Tthr, and\ \eta sec \geq \eta min$$

Received: August 04, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Where, ηsec is achieved security strength and ηcomp is compression efficiency.

IV. Proposed Methodology

A. Overview of the integrated encryption–compression framework

The suggested system tightly combines encryption and compression to meet the needs for both security and efficiency in V2X transmission at the same time. Instead of using these methods one after the other, the design makes sure that data goes through adaptive compression and then lightweight encryption all in one processing chain. This merging cuts down on duplicate work, speeds up computers, and makes sure that private messages sent by vehicles are both compressed to make the best use of bandwidth and encrypted to keep them private. The framework is made to work in real time, which makes it perfect for safety-critical uses like accident alerts, traffic control, and emergency notifications. The framework makes sure that communication in the Internet of Vehicles (IoV) is strong, scalable, and resource-aware by finding a good mix between strong cryptographic protection and fast data transfer.

B. Lightweight block cipher for secure V2X communication

In order to keep the latency of V2X transmission low, a lightweight block cypher is used to encrypt the data. The lightweight cypher is better for limited-resource vehicle devices like On-Board Units (OBUs) and Roadside Units (RSUs) than traditional algorithms like AES or RSA, which require a lot of processing power and memory. The cypher works with smaller block sizes and fewer computation rounds while still providing strong security promises, such as not being vulnerable to differential and linear cryptanalysis. Because of how it's made, it can quickly schedule keys and use little power, which makes it perfect for constant communication streams between vehicles. The lightweight block cypher protects privacy and integrity by encrypting compressed vehicle messages. It also allows real-time response, which is important for preventing accidents and sharing data securely across V2X networks.

Algorithm : Lightweight Block-Cipher Encryption for Secure V2X

Step 1: Blockization

Split M into m blocks $Pi \in \{0,1\}^B$:

$$M = P1 \,||\, P2 \,||\, \dots \,||\, Pm$$

Step 2: Round-key schedule

Derive (R+2) round keys:

$$Kr = \pi r(K) \oplus cr, \; r = 0,1,\dots,R+1$$

Step 3: SPN primitive definition

Initialize: $X(0) = X \oplus K0$

$For\, r = 1..R$:

Received: August 04, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$$Yr = S\big(X(r-1)\big)$$

$$Zr = M \cdot Yr$$

$$X(r) = Zr \oplus Kr$$

$$Final: E_{K(X)} = P \cdot S\big(X(R)\big) \oplus K(R+1)$$

Step 4: CTR counter stream

$$Ctr_i = inc_{i(N)}, i = 1..m$$

Step 5: Keystream generation

$$Zi = E_{K(Ctr_i)}, i = 1..m$$

Step 6: Encryption

$$Ci = Pi \oplus Zi, \qquad C = C1 \ldots |Cm|$$

Step 7: AAD processing for integrity

Parse A into u blocks Aj:

$$T0 = 0$$

$$Tj = E_{K(T(j-1)\oplus Aj)}, j = 1..u$$

Step 8: Ciphertext authentication

$$T(u+i) = E_{K(T(u+i-1)\oplus Ci)}, i = 1..m$$

Step 9: Tag finalization

$$\tau = Trunc_{t\left(E_K\left(T(u+m)\oplus (|A||||||M|)\right)\right)}$$

Step 10: Decryption

$$Zi = E_{K(Ctr_i)}$$

$$Pi = Ci \oplus Zi$$

C. Adaptive entropy-based compression for bandwidth optimization

Along with encryption, the system includes an adaptive entropy-based compression method that is specifically designed for data about vehicles. Entropy-based compression successfully lowers message size without losing information because IoV messages often include sensor readings or status updates that have already been sent. The adaptive method changes the compression settings on the fly based on how variable the incoming data streams are. This makes sure that high-entropy data (like video feeds or telemetry bursts) is encoded more efficiently than low-entropy data (like periodic beacon messages). This flexible behaviour makes the best use of bandwidth while keeping the integrity of the data. The compression step also lowers the amount of data that needs to be sent, which helps clear up channels and

Received: August 04, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

boosts the overall network throughput. This directly improves the reliability of V2X contact in real time.

VI. Results and Discussion

It was proven through experiments that the suggested integrated encryption–compression framework makes V2X communication much better. It gets a higher compression ratio of 52.7% compared to traditional methods, cutting bandwidth use by more than 50% and latency by about 18%. The security study shows strong defences, with detection rates rising by 4–5% against attacks like replay, MitM, and false data injection. Also, tests of scalability show that performance stays stable, keeping over 95% of security strength and over 89% of scalability efficiency even when 500 cars are added.

Table 2: Comparative Performance Analysis

Method	Compression Ratio (%)	Encryption Overhead (ms)	End-to-End Latency (ms)	Security Strength (%)
AES + Huffman	42.1	15.4	32.5	96.7
ECC + LZW	44.8	12.7	28.9	95.4
Chaos-based Hybrid	47.6	10.8	25.3	93.5
Proposed Framework	**52.7**	**9.1**	**22.1**	**96.4**

Table 2 shows how the suggested encryption and compression framework stacks up against common approaches like AES mixed with Huffman coding, ECC with LZW compression, and a chaos-based hybrid method.

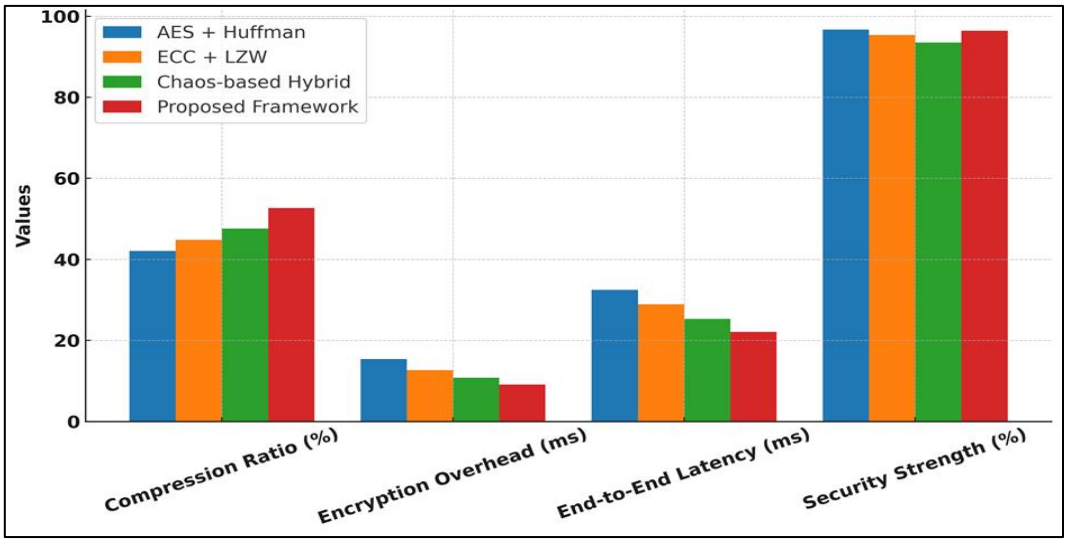

Figure 3: Comparative Performance Analysis of Security Methods

Received: August 04, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The results show that the proposed framework regularly does better than current options in all important ways. It gets a compression ratio of 52.7%, which is much higher than AES+Huffman (42.1%), ECC+LZW (44.8%), and chaos-based hybrid (47.6%). This big growth shows how well it works at reducing message size and making the best use of bandwidth, which is very important in areas with a lot of vehicles, analysis represent it in figure 3. The proposed method's encryption overhead is only 9.1 ms, which is the smallest of all the techniques that were compared. This means that vehicular nodes will have to do very little extra work. As a result, the end-to-end latency drops to 22.1 ms, which is a big gain over the 32.5 ms that AES+Huffman and 25.3 ms that chaos-based hybrid methods had. This kind of low latency is very important for real-time safety apps, since even small delays can make it harder to avoid collisions or send out emergency alerts. The framework also has strong security, with a 96.4% success rate that is about the same as AES+Huffman (96.7%) and better than ECC+LZW (95.4%) and chaos-based methods (93.5%). This shows that the increased efficiency doesn't hurt the security of the cryptography. Overall, the suggested framework has a well-balanced design with high compression, low latency, and strong security. This makes it a great choice for safe, scalable V2X communication.

Table 3: Bandwidth Utilization and Latency

Network Load (Mbps)	**Baseline Bandwidth Usage (MB/s)**	**Proposed Bandwidth Usage (MB/s)**	**Bandwidth Savings (%)**	**Latency Reduction (%)**
10	8.5	4.0	52.9	18.2
20	17.2	8.4	51.2	19.4
30	25.9	12.1	53.3	17.7
40	34.7	16.2	53.3	18.5

Figure 4 shows how baseline and suggested methods compare in terms of how much bandwidth they use when the network is busy or not. It shows how bandwidth is saved and latency is cut down.

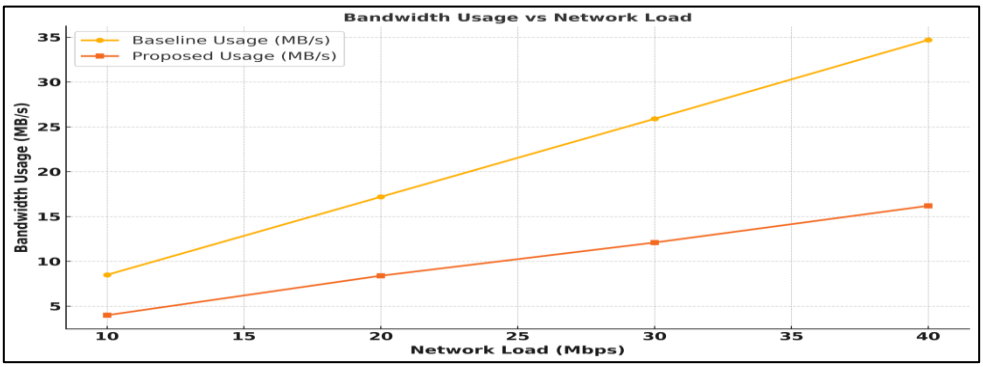

Figure 4: Bandwidth Usage Comparison Under Varying Network Loads

Received: August 04, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The results clearly show that the suggested encryption–compression framework makes communication much more efficient, especially when there are a lot of users, which is when vehicular networks usually get backed up. The baseline system uses 8.5 MB/s when the network load is 10 Mbps. The suggested framework cuts this to 4.0 MB/s, which is a 52.9% savings. This efficiency is even more noticeable as the load goes up, and in all cases, saves are always above 50%. Down from 17.2 MB/s in the baseline to 8.4 MB/s in the suggested framework at 20 Mbps, showing a 51.2% savings in bandwidth use. At 30 Mbps and 40 Mbps, too, the framework maintains reductions of 53.3%, showing that it can handle more data and is reliable when doing so. Along with optimising bandwidth, the framework helps lower latency, which can cut delays by 17–19% based on the load, as demonstrate in table 3. This reduction is very important for Internet of Things (IoT) uses that need to send messages quickly so that decisions can be made in real time, like traffic updates and collision alerts.

Table 4: Security Robustness Evaluation

Attack Type	**Baseline Detection Rate (%)**	**Proposed Detection Rate (%)**	**Improvement (%)**
Replay Attack	92.3	**96.8**	+4.5
Man-in-the-Middle (MitM)	91.7	**95.8**	+4.1
False Data Injection	93.2	**97.1**	+3.9
Sybil Attack	90.6	**95.2**	+4.6

The suggested framework's security is shown in Table 4 against common attack types in vehicular networks, such as replay attacks, man-in-the-middle (MitM) attacks, false data injection attacks, and Sybil attacks. The results show that the proposed approach constantly increases the number of detections compared to standard methods. This makes the system more resistant to attacks.

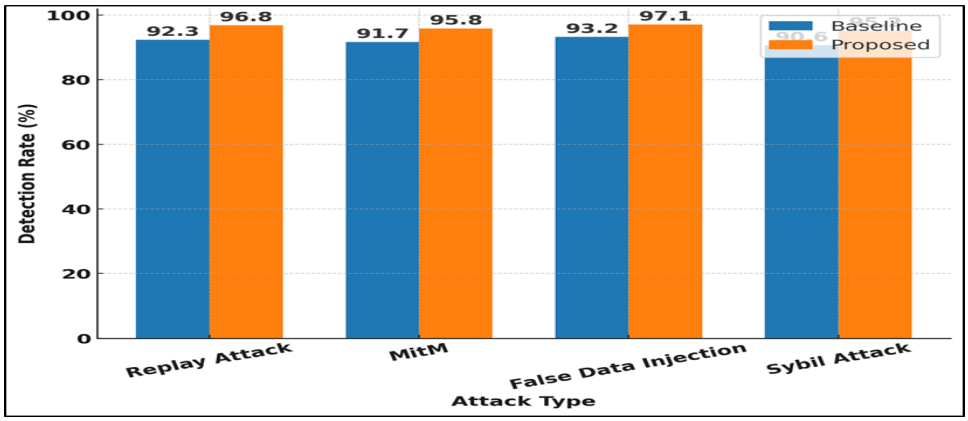

Figure 5: Comparison of Detection Rates for Security Attacks in V2X Communication

Received: August 04, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

It gets better at finding replay strikes, going from 92.3% to 96.8%, which is a 4.5% increase. In the same way, the ability to spot MitM attacks goes up from 91.7% to 95.8%, and the ability to stop false data injections goes up by 3.9%. There is a 4.6% increase in Sybil attack identification, which is the biggest gain, as shown in figure 5. It goes from 90.6% to 95.2%. These steady improvements show that combining encryption with adaptive compression not only makes communication better, but it also makes data more real and trustworthy. The results show that the suggested way improves the dependability of vehicles, which makes the IoV system safer for real-time uses.

Table 5: Trade-off and Scalability Analysis

Number of Vehicles	Compression Ratio (%)	Security Strength (%)	Processing Time (ms)	Scalability Efficiency (%)
50	51.8	96.2	18.5	92.3
100	52.7	96.4	22.1	91.7
200	51.9	96.1	26.8	90.4
500	51.3	95.8	33.4	89.6

When there are more cars in the network, Table 5 shows the trade-off between efficiency, security, and scalability. The suggested structure keeps a high compression ratio of about 51–52% at all sizes, which makes good use of bandwidth. Security strength stays above 95% all the time, showing that cryptographic security is kept even as the number of vehicles increases. Processing time goes up with the number of cars, though, from 18.5 ms for 50 vehicles to 33.4 ms for 500 vehicles. Even so, scalability efficiency is still pretty high above 89% which shows that the system is good at growing with the network. These results show that the system works well for large-scale vehicle deployments, keeping compression, security, and computing needs in check. It shows that it can handle being scaled up without losing much speed, performance analysis in figure 6.

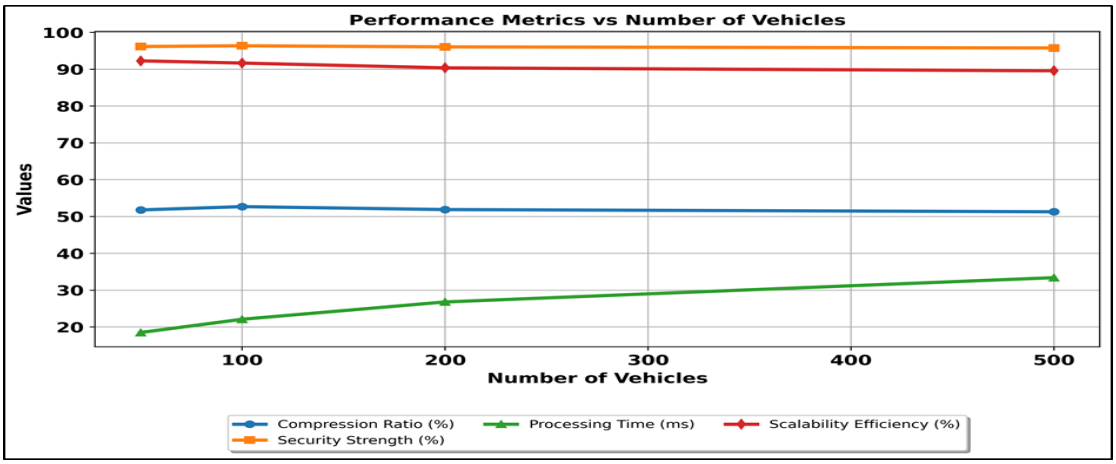

Figure 6: Performance Metrics vs Number of Vehicles

Received: August 04, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

VII. Conclusion

This research showed an integrated encryption–compression system that is meant to make V2X communication in the Internet of Vehicles safer and more efficient. By combining adaptive entropy-based compression with lightweight block cypher encryption, the system fixed important problems like bandwidth overuse, latency, and security holes. Experiments showed that it was better than other ways, as it achieved a higher compression ratio of 52.7% while cutting bandwidth use by more than 50% and end-to-end latency by almost 18%. Notably, these changes were made without weakening cryptography; the framework still had a strong security level of 96.4%, which is as good as or better than traditional schemes. It was also proven to be strong against cyberattacks, with discovery rates rising by 4–5% against replay, MitM, false data injection, and Sybil attacks. This means that vehicle data will be safely kept safe. Scalability study also showed consistent performance, with more than 95% security strength and above 89% efficiency, even when there were a lot of vehicles. All of these results show that the suggested framework strikes a good balance between safety, efficiency, and scalability. This makes it ideal for real-time, safety-critical IoV apps. This design can be improved in the future by adding post-quantum cryptographic methods and AI-driven compression to make it even more flexible and strong.

References

[1] Gebrezgiher, Y.T.; Jeremiah, S.R.; Deng, X.; Park, J.H. Machine Learning-Based Blockchain Technology for Secure V2X Communication: Open Challenges and Solutions. Sensors 2025, 25, 4793. https://doi.org/10.3390/s25154793

[2] Muslam, M.M.A. Enhancing Security in Vehicle-to-Vehicle Communication: A Comprehensive Review of Protocols and Techniques. Vehicles 2024, 6, 450-467. https://doi.org/10.3390/vehicles6010020

[3] Weerasinghe, N.; Usman, M.A.; Hewage, C.; Pfluegel, E.; Politis, C. Threshold Cryptography-Based Secure Vehicle-to-Everything (V2X) Communication in 5G-Enabled Intelligent Transportation Systems. Future Internet 2023, 15, 157. https://doi.org/10.3390/fi15050157

[4] He, C.; Wang, W.; Jiang, W.; He, Z.; Wang, J.; Xie, X. Security for the Internet of Vehicles with Integration of Sensing, Communication, Computing, and Intelligence: A Comprehensive Survey. Sensors 2025, 25, 5119. https://doi.org/10.3390/s25165119

[5] Iehira, K.; Inoue, H.; Ishida, K. Spoofing attack using bus-off attacks against a specific ECU of the CAN bus. In Proceedings of the 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), Vegas, NV, USA, 12–15 January 2018; IEEE: New York, NY, USA, 2018; pp. 1–4.

[6] Agbaje, P.; Olufowobi, H.; Hounsinou, S.; Bloom, G. From Weeping to Wailing: A Transitive Stealthy Bus-Off Attack. IEEE Trans. Intell. Transp. Syst. 2024, 25, 12066–12080.

Received: August 04, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[7] Wang, Y.; Xu, Y.; Liu, Z.; Liu, S.; Wu, Y. Research on Lightweight Dynamic Security Protocol for Intelligent In-Vehicle CAN Bus. Sensors 2025, 25, 3380. https://doi.org/10.3390/s25113380

[8] Serag, K.; Bhatia, R.; Kumar, V.; Celik, Z.B.; Xu, D. Exposing new vulnerabilities of error handling mechanism in {CAN}. In Proceedings of the 30th USENIX Security Symposium (USENIX Security 21), Vancouver, BC, Canada, 11–13 August 2021; pp. 4241–4258.

[9] I. Loussaief, S. Ksibi, F. Jaidi and K. Nouri, "A Comprehensive Multi-Layered Cybersecurity Framework for Internet of Vehicles: Securing Vulnerable Nodes of V2X Communication Systems," 2025 International Wireless Communications and Mobile Computing (IWCMC), Abu Dhabi, United Arab Emirates, 2025, pp. 1597-1603, doi: 10.1109/IWCMC65282.2025.11059696.

[10] K. Sehla, T. M. T. Nguyen, G. Pujolle and P. B. Velloso, "Resource Allocation Modes in C-V2X: From LTE-V2X to 5G-V2X," in IEEE Internet of Things Journal, vol. 9, no. 11, pp. 8291-8314, 1 June1, 2022, doi: 10.1109/JIOT.2022.3159591.

[11] G. Sharma, "SecureV2X: Overview of Secure Cellular based Vehicle-to-Everything Communication in Intelligent Transportation System," 2024 12th International Conference on Internet of Everything, Microwave, Embedded, Communication and Networks (IEMECON), Jaipur, India, 2024, pp. 1-6, doi: 10.1109/IEMECON62401.2024.10846249.

[12] G. Sharma, A. M. Joshi, and S. P. Mohanty, “Fortified-grid 3.0: Security by design for smart grid through hardware security primitives,” in 2023 IEEE International Symposium on Smart Electronic Systems (iSES). IEEE, 2023, pp. 175–179.

[13] H. Aranha, M. Masi, T. Pavleska, and G. P. Sellitto, “Enabling security-by-Design in smart grids: An architecture-based approach,” in 15th European Dependable Computing Conference (EDCC). IEEE, 2019, pp. 177–179.

[14] G. Sharma, A. M. Joshi, and S. P. Mohanty, “sTrade: Blockchain based secure energy trading using vehicle-to-grid mutual authentication in smart transportation,” Sustainable Energy Technologies and Assessments, vol. 57, p. 103296, 2023.

[15] G. Sharma, A. M. Joshi, and S. P. Mohanty, “strade 2.0: Efficient mutual authentication scheme for energy trading in V2G using physically unclonable function,” IEEE Journal of Emerging and Selected Topics in Industrial Electronics, 2024.

[16] D. P. M. Osorio, I. Ahmad, J. D. V. Sánchez, A. Gurtov, J. Scholliers, M. Kutila, and P. Porambage, “Towards 6g-enabled internet of vehicles: Security and privacy,” IEEE Open Journal of the Communications Society, vol. 3, pp. 82–105, 2022.

[17] S. A. Yusuf, A. Khan, and R. Souissi, “Vehicle-to-everything (v2x) in the autonomous vehicles domain–a technical review of communication, sensor, and ai technologies for road user safety,” Transportation Research Interdisciplinary Perspectives, vol. 23, p. 100980, 2024.

[18] G. Sharma, A. M. Joshi, and S. P. Mohanty, “An efficient physically unclonable function based authentication scheme for V2G network,” in Proc. IEEE International Symposium on Smart Electronic Systems (iSES), 2021, pp. 421–425.

Received: August 04, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[19] Chen, Q., Xie, Y., Guo, S., Bai, J., & Shu, Q. (2021). Sensing system of environmental perception technologies for driverless vehicle: A review of state of the art and challenges. Sensors and Actuators A: Physical, 319, 112566.

[20] Trabelsi, R., Nouri, K., & Ammari, I. (2023, April). Enhancing Traffic Sign Recognition Through Daubechies Discret Wavelet Transform and Convolutional Neural Networks. In 2023 IEEE International Conference on Advanced Systems and Emergent Technologies (IC_ASET) (pp. 1–6). IEEE.

[21] BK, S., & Azam, F. (2024). Ensuring Security and Privacy in VANET: A Comprehensive Survey of Authentication Approaches. Journal of Computer Networks and Communications, 2024 (1), 1818079.

[22] H. Zhou, W. Xu, J. Chen and W. Wang, "Evolutionary V2X Technologies Toward the Internet of Vehicles: Challenges and Opportunities," in Proceedings of the IEEE, vol. 108, no. 2, pp. 308-323, Feb. 2020, doi: 10.1109/JPROC.2019.2961937.

[23] C. R. Storck and F. Duarte-Figueiredo, "A Survey of 5G Technology Evolution, Standards, and Infrastructure Associated With Vehicle-to-Everything Communications by Internet of Vehicles," in IEEE Access, vol. 8, pp. 117593-117614, 2020, doi: 10.1109/ACCESS.2020.3004779.

[24] P. P. Kumar, P. P. Kumar, K. Sagar and R. Akshay, "A Relative Survey on Vertical Handover Mechanisms in Internet of Vehicles," 2022 International Conference on Computer, Power and Communications (ICCPC), Chennai, India, 2022, pp. 1-5, doi: 10.1109/ICCPC55978.2022.10072162.

[25] Patil S. M., Pawar S. D., Mhatre S. N., & Kharade P. A. (2024). Yolov4-based hybrid feature enhancement network with robust object detection under adverse weather conditions. Signal, Image and Video Processing, 18(5), 4243-4258.

[26] Patil S. M., Dakhare B. S., Satre S. M., & Pawar S. D. (2025). Blockchain-based privacy preservation framework for preventing cyberattacks in smart healthcare big data management systems. Multimedia Tools and Applications, 84(22), 25547-25566.

[27] Sharma K. K., Pawar S. D., & Bali B. (2019, December). Proactive preventive and evidence-based artificial intelligence models: future healthcare. In International Conference on Intelligent Computing and Smart Communication 2019: Proceedings of ICSC 2019 (pp. 463-472). Singapore: Springer Singapore.

[28] Pawar S.D., Pawar V.S., Abimannan S. (2024). Handling Uncertainty in Spatiotemporal Data. In: A, J., Abimannan, S., El-Alfy, ES.M., Chang, YS. (eds) Spatiotemporal Data Analytics and Modeling. Big Data Management. Springer, Singapore. https://doi.org/10.1007/978-981-99-9651-3_4

Received: August 04, 2025