Optimising Data Integrity in VANETs: An Innovative Method to Minimize Replay and Tampering Attacks

R. Prema[1], Prasanna Ranjith Christodoss[2], S. Silvia Priscila[3(✉)], G. Gowthami[4], M. Sakthivanitha[5], F. Mohamed Ilyas[6], V. Vishwa Priya[7], and Ms. Jomila Ramesh[8]

[1] Department of Computer Science, New Horizon College, Kasturinagar, Bangalore 560043, India

[2] Department of Computing, Mathematics and Physics, One University Ave, Mechanicsburg, PA 17055, United States
prchristodoss@messiah.edu

[3] Department of Computer Science, Bharath Institute of Higher Education and Research, Chennai, Tamil Nadu, India
silviaprisila.cbcs.cs@bharathuniv.ac.in

[4] Department of Computer Science, St Francis De Sales College (Autonomous), Electronic City, Bangalore 100, Karnataka, India
Gowthamigunasekar@sfscollege.in

[5] Department of Computer Applications, Vels Institute of Science Technology and Advanced Studies, Chennai, Tamil Nadu, India

[6] Information Systems Management, The New College (Autonomous), Chennai, Tamil Nadu, India
hodbis@thenewcollege.edu.in

[7] Department of Computer Science and Information Technology, Vels Institute of Science Technology and Advanced Studies Chennai, Chennai, India

[8] Centre for Computer Science and Information Technology [CCSIT], University of Calicut, Kodungallur, India

Abstract. The possibility of VANET risk to replay and manipulation attacks, which may compromise the security of safety-critical signals, creates a major threat to road safety. Most of the cryptographic methods are used in current security measures, which are either computationally costly or at risk of attacks. By using hash chains and digital signatures in combination to prevent replay and manipulation attacks, and in this research, we provide a unique method for improving the security of data in VANET. We plan to reduce communication delay and processing overhead to ensure message integrity and authenticity is there. Test outcomes demonstrate how well our method identifies and stops replay and manipulation incidents of assault. Our proposed method provides a practical way to protect VANET and ensure the reliability of applications that are essential for safety.

Keywords: Cryptographic methods · Digital signatures · Replay · Security · Safety critical signals · Tampering attacks · VANET

R. Sridaran and S. Priti (Eds.): AI-FCDAC 2025, CCIS 2866, pp. 75–86, 2026.
https://doi.org/10.1007/978-3-032-17300-3_6

1 Introduction

In the future, Mobile Ad Hoc Networks (MANETs) and Vehicular Ad Hoc Networks (VANETs) will both be useful for Intelligent Transportation Systems. VANET is a type of Mobile Ad Hoc Network (MANET) [3]. Nowadays, the death rate should be higher because of traffic accidents; it may be addressed with VANET, which may enhance road safety and passenger comfort. As the usage of private transportation is growing, VANETs are a way to provide passengers with dynamic services and information, such as alerting them to situations of emergency or streamlining routes to destinations [1].

VANETs are a type of ad hoc network that uses vehicles as communication units and has a minimal infrastructure [3]. Due to the behaviour of drivers, high mobility, and mobility limits, these networks differ considerably from general MANETs in that they rely on the automobiles themselves to provide network performance [3]. VANET enable Peer-to-Peer (P2P) or multi-hop communication, facilitating applications such as traffic monitoring, collision avoidance, and weather forecasting [4, 5].

We can apply VANET for various applications, from comfort-related ones like broadcasting details about the goods and services to safety-critical ones like emergency response systems [4, 5]. The alternative name for VANET is Vehicle-to-Vehicle communications (V2V) or Inter-Vehicle Communications (IVC), which have the potential to completely change how we travel [4, 5]. One of the main uses for VANETs is in life-or-death medical emergencies where transmission of data is essential, yet infrastructure is insufficient.

However, new issues and challenges also arise when combined with these beneficial VANET applications [2]. In order to guarantee the reliability, safety, and effectiveness of VANETs as they expand further, it is critical to address these issues and create solutions. In this regard, it is essential to understand the features, uses, and difficulties of VANETs to create practical solutions that enhance road safety along with passenger comfort.

Replay and Tampering: A replay attack is a variation of a security flaw that arises when data is sent over a network and the data is intercepted and maliciously reused. In this attack an unauthorized individual engaged in hacking will capture network traffic and retransmit the original data to the original destination as if the unauthorized individual was the sender. The nature of a replay attack is that the same message will be received by the recipient more than once, which is why this attack is called a replay attack. A common approach used to mitigate replay attacks are timestamps and session keys that validate messages and stop them from being retransmitted by someone without authorization [7].

Replay attack, which implies a real threat to automatic speaker verification technology because it replays a prerecorded voice as a sample [8]. The intentional, malicious change of data, systems or physical things is called a tampering attack. This may undermine the integrity, security or functionality of the specified entity. Improper security, data breaches, system failure, financial losses, reputational damage, all these are the consequences of a tampering attack. The prevention methods for tampering attacks are to implement strong access controls, use encryption and digital signatures, regularly monitor systems and data, and perform security audits and testing [9].

By repeatedly applying a cryptographic hash function provide a set of hash values is known as a hash chain. Each hash value is derived from the previous value, creating a

linked sequence. One-time passwords, digital signatures, and data integrity verification are the various applications of hash chains. They give an encrypted way of creating and confirming a list of values, assuring that any modification can be identified. To verify the authenticity and integrity of data to ensure the secure authentication process, we used a hash chain [10].

A digital signature technique guarantees authenticity, integrity, and non-repudiation by connecting a message to its original sender. By creating a digital signature, the sender confirms they formed or approved the message by cryptographically linking their data to its message. This connection prevents the sender from refusing involvement or authorship, gives an authenticated way to verify the message's origin and assures that it has not been tampered with any other one. In online transactions and data exchange, we used digital signatures based on trust [10]. In the existing paper, they used machine learning algorithms to increase attack detection, keep false positive rates low, and assure anonymity, authentication, and privacy. But the paper does not describe in detail about a particular cryptographic technique used in the proposed security framework for VANETS. Instead of it, they gave more importance to ML-based approaches to improve the security [11].

This research paper aims to concentrate the security of VANETS by securing against replay and tampering attacks. Since VANETs are sensitive to the above kind of attacks, lives could be in risk and the safety dangerous signals could be compromised. The objective of this research is to ensure the message integrity and authenticity while reducing transmission delay and processing cost. This study aims to create a novel method with the combination of hash chains and digital signatures. The purpose of this paper is to provide an effective solution for improving road safety ensuring the availability of safety-critical applications in VANETs.

1.1 Related Works

Huo et al., (2025) talked about how Vehicle-to-vehicle (V2X) communication security has grown more important as linked vehicle communication becomes increasingly complex. Replay attacks present a severe danger to the security of intelligent networked vehicles because they are a common form of network attack. They showed the stability and safety of intelligent connected vehicle communication. And in this paper, they proposed anti-replay attack scheme based on the fusion of hash chain and V2X communication, which combines the special benefits of hash chain technology with a focus on the common replay attack problem in V2X communication [12].

Sinha et al., (2024) evaluate a set of hashing methods used in the blockchain and the supply chain domain to find their effectiveness in previous attacks. To improve security and their overall processes, they proposed a hashing technique that allows a blockchain network. By using this type of method, he got 10–90% performance improvements over the previous methods. The study takes a look at how supply chain management increases lead times overall, with process optimization and technology advancements playing important roles in reducing the duration of some or all of the operations [13]. Roy et al., (2012) made a thorough study of digital signature schemes. And they explored in various domains to get the security level for electronic mechanisms [14].

Rakhra et al., (2024) integration of cryptographic techniques for authentication and non-repudiation is highlighted in this research paper and the depth analysis of digital signature verification processes in cloud computing environments. They described what are all the challenges they met in digital signature schemes, like computational overhead, key management, and risk to various cyber threats within the cloud structure. In this study, they suggested effective key distribution techniques and cutting-edge encryption standards. Using this research, they offer useful techniques to protect electronic transactions in cloud contexts [15]. Iqbal et al., (2024) made a comparative analysis has been done to identify the efficiency of the proposed model. At last, this method improves the performance in terms of security like that they described in their study [16].

Muzakkir et al., (2024) uses a SHA-256 for digital signature tokens, and OpenSSL for valid digital signatures, they start with generating a key pair, and they created the digital signature application in this study. Mainly, they created this application to secure and efficiently authorise document signing. Moreover, they assure the delivery of OTPs through mail for user authentication testing and a strong defence against Man-in-the-Middle attacks, and secure transfer of login data over HTTPS is also described. QR code verification efficiency, authenticity and signature integrity were confirmed by this research analysis [17].

2 Methodology

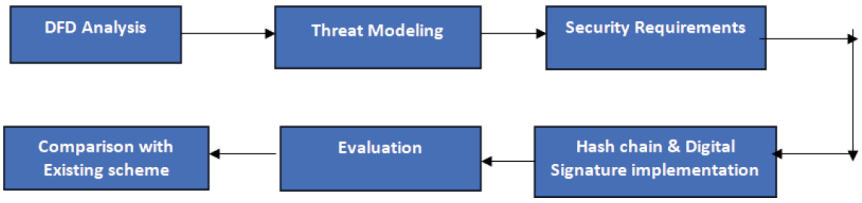

Fig. 1. Data flow diagram for methodology

DFD Analysis: To identify and understand the flow of data within the VANET system is analysed by a DFD analysis (Dataflow Diagram). This analysis helps to identify the problems and weaknesses in the system where security threats like replay and tampering attacks could develop. To protect the authenticity and integrity of the data, we have to analyse the data flow, then we can identify where the data is sent, received, processed and ensure the corresponding security measures are in place. The Data Flow Diagram (DFD) analysis will be used in the proposed security structure to assess the flow of information between vehicles and the infrastructure as well as the received information input and storage system. On examining these data flows, the points of hash chains and digital signatures may be identified to defend the system against the replay and tampering attacks. Moreover, the result of this analysis will be used to design the security framework so that we optimize system performance and ensure the security framework (Fig. 1).

Threat Modeling: The first action in VANETs security setup is to determine the threats to security. A threat modeling approach can be utilized to identify and examine possible targets in the system, e.g. using STRIDE or LINDDUN. Such approaches facilitate the identification of the weaknesses and the possible failure points in VANETs. STRIDE methodology groups threats into six classes of threats: det witness to the spoofing, tampering, repudiation, information disclosure, denial of service (DoS) and elevation of privilege (EoP). Based on it, we can adequately define risks related to vehicle-to-vehicle (V2V) communication, namely, spoofing attacks, and safety messages tampering [18]. The LINDDUN methodology, instead, is anchored on privacy related threats and categorizes these threats in seven ways such as Linkability, Identifiability and Non-Repudiation. Cumulatively, STRIDE and LINDDUN capture many of the possible threats with 34 risks and11 key assets or threat targets being covered [19]. A secure system design of VANET can be made by consequently discovering the potential threats and vulnerabilities. In our proposed system, hash chains and digital signatures provide a system to achieve integrity (and authenticity) of messages and is effective to prevent replay and tampering attacks. The framework offers good security against threats that may occur thus increasing the security level of VANETs [20].

2.1 Security Requirements

Data Integrity: Data integrity plays the vital role in VANETs because vehicles are dependent on accurate and reliable data to make safe decision. Verification of data preserves the integrity of the information being sent to ensure that it is neither tampered with nor adversely affected by unauthorized parties. Observing this principle, VANETs will be able to avoid attacks that will mislead the correctness of safety-affecting information.

Non-repudiation: Non-repudiation is also important in VANETs in that a car cannot deny its involvement in a transaction or a communication. This is a security measure to prevent the cases where electronics vehicles fraudulently claim that they never sent or received a certain message. Non-repudiation allows trust building and accountability between the vehicles and the network by the minimization of the probability of message denial.

Authentication: Authentication is required to prove that the vehicles and infrastructure are authentic. The network can only be accessed by authorised parties who share information amongst themselves. VANETs can help to avoid spoofing, unauthorized access, and other attempts of hacking by authenticating cars and infrastructure, and this way, the trust and reliability of the network are maintained.

2.2 Hash Chain and Digital Signature Implementation

To prevent replay and tampering attacks, the proposed security framework utilises hash chains and digital signatures. A hash chain is a series of hash values formed by hashing the previous hash value multiple times, in a way similar to how a password or code is hashed, in one-way function. Hash chains have numerous uses; one common use is for message integrity/authentication. In order to further protect the communication, the use

of a digital signature is added to the hash chain. Each message is digitally signed with the private key of the sender, and the security of the message can be verified by the receiver using the sender's public key, which provides integrity of the message and authenticity of the sender. Particularly, digital signature algorithms like RSA and hash-based signatures (such as SPHINCS and XMSS) are used to provide the essential security properties with fewer security assumptions. These algorithms are appropriate for applications needing high security because they provide benefits like post-quantum security and fewer security requirements.

A unique message ID, timestamp, message payload, hash chain value, and digital signature are the components message structure in this framework. A digital signature is created using the message payload and the current hash value in the hash chain. The receiver attempts to verify the signature using the sender's public key by computing the hash chain which is achieved by applying the one-way hash function to the previous hash value, and comparing it to the expected value in the hash chain. Here, they assure that any hash chain value or message payload will be identified. This framework can prevent replay attacks is one of its advantages. Replay attacks occur when an unauthorised person retransmits a message to the receiver, which might cause harm or a clash to the system. So here we are going to use timestamps and hash chains, which prevents replay attacks, and the attacker has to create a new hash chain value and digital signature for each message that is replayed. Because of this, the attacker has no possibility to launch a successful replay attack, almost here it is zero.

Moreover, this framework provides high protection against tampering attacks. When an attacker modifies the message by payload or hash chain value, it may harm the system or cause a clash with the system. Any tampering attacks with the message payload or hash chain value will be easily identified by using digital signatures and hash chains. Because of this, an attacker doesn't have a chance to launch their tampering attempt, and it is almost zero. The entire framework's security depends on the one-way hash function and digital signature used. In order for an attacker to produce a new hash chain value, it must not match the expected value, because a hash function should be collision-resistant and preimage-resistant. And choosing message attacks, making it difficult for an attacker to produce a new digital signature, a secure digital signature scheme should be existentially unforgeable.

The framework provides security advantages that are efficient and scalable. The framework's usage of hash chains and digital signatures reduces computing overhead because only one hash operation and digital signature verification are needed for every message. The framework is scalable, because it is used in various applications and domains, like finance, healthcare, and government sectors. The suggested security model can be applied in various ways, to IoT security, secure data storage, and secure communication protocols. Through the deployment of secure communication protocols, the framework attributes that exchanges between two users are secure, and the integrity and authenticity of the messages being conveyed are not violated. Under an IoT landscape, the frame will ensure security in communication between devices and the cloud or other associated devices . There are also adequate data storage security measures that are

deployed to protect the integrity and authenticity of data that is stored in cloud or other storage systems.

A key element in the improvement of the security of the framework is proper key management. There is generation of public and private keys, distribution and secure storage. Key revocation mechanisms make sure that revoked keys are removed in a timely fashion and replaced. Furthermore, there is some future work that may be done to find ways of throwing more efficiency into the framework, framework processes of key revocation, and also integrating the framework to work with other security systems. This framework makes sure that there is an authenticity and integrity to the message and it offers immense protection against replay and tampering. The design is highly scalable and security-oriented; it provides long-term protection via a key management scheme.

In a nutshell, hash chains plus the digital signature provides a solid means of combating replay and tampering attacks. This method can be used on a wide range of applications and domains because of its ability to ensure message integrity, detect manipulation, and prevent replay attacks. The scalability of the framework as well as its effectiveness and security also gives the framework longevity in combating different forms of cyber threats.

Hash Chain Algorithm

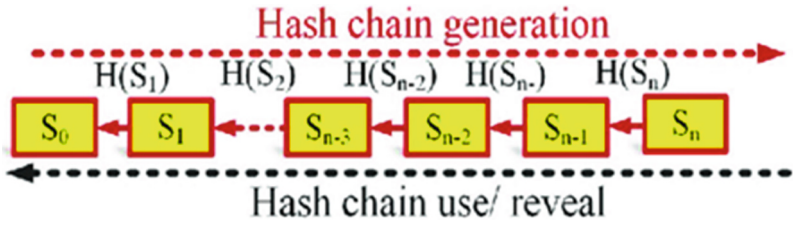

Fig. 2. Hash Chain Generation Image

A hash chain is a cryptographic mechanism, where the sequence of values is created depending on the previous one. The specified method is commonly employed in a variety of authentication systems, entities in blockchain technology, and security protocols because of its high security characteristics (Fig. 2).

Algorithm Steps:

- Select a one-way Hash Function: Choose a secure hash function which is a one way hash like SHA-256 that assures you of cryptographic strength.
- Initialize Hash Chain: Add random number or some initial value to start the chain.
- Calculate the Hash Chain: Using a one-way hash algorithm, each successive value in the chain is calculated by using the previous value as the input to a one-way hash function.
- Repeat: Iteration repeat until the length of the hash chain is reached (Fig. 3).

Fig. 3. How the Hashing Algorithm Works

Digital Signature Generation Algorithm (DSA)- Key Generation

1. Choose Prime Numbers: Select two prime numbers, p and q, where q is a divisor of (p-1).
2. Choose a Generator: Select a generator g, where g = h^(p-1)/q mod p and h is an integer between 1 and (p-1).

3.Private Key: Choose a private key x, where 0 < x < q.
4.Public Key: Compute the public key y = g^x mod p.

Signing

1. Choose a Random Number: Select a random number k, where 0 < k < q.
2. Compute r: Calculate r = (g^k mod p) mod q.
3. Compute s: Calculate s = (k^(−1) * (H(m) + xr)) mod q, where H(m) is the hash of the message m.
4. Signature: The digital signature is (r, s).

Verification

1. Compute w: Calculate w = s^(−1) mod q.
2. Compute u1 and u2: Calculate u1 = H(m) * w mod q and u2 = r * w mod q.
3. Compute v: Calculate v = (g^u1 * y^u2 mod p) mod q.
4. Verify: Check if v = r. If true, the signature is valid.

Verification Algorithm

- Receive Message and Signature: Receive the message m and the digital signature (r, s).
- Verify Signature: To check the signature, use the verification algorithm.
- Check Hash Chain: Verify the hash chain value by applying the one-way hash function to the previous hash value.
- Authenticate: Authenticate the message, if the signature and hash chain are valid.

3 Results and Findings

Calculating the effectiveness and efficiency of the proposed framework for VANET is essential. The computational cost, communication overhead, and security features are evaluated in this study to highlight the framework's possible effects on network security and performance. The above measurements are used to assess whether the framework is suitable for deployment on VANET and to identify the areas for further optimization.

Computational Overhead: It specifies the amount of computing resources (time and processing power) required to finish security operations like digital signature verification and hash chain creation. We evaluate this and we are not overburdening the system, and to make sure the system is effective, so these things are listed in the Table 1.

Table 1. Calculation of Computational Time and Complexity

S.NO	Operation	Computational Time (ms)	Computational Complexity
1.	Hash Chain Generation	0.5	O(n)
2.	Digital Signature Generation	1.2	O(n)
3.	Digital Signature Verification	0.8	O(n)

In the above Table 1, the type of operation and its computational time, along with its complexity, are also mentioned. 0.5 ms they got as computational time and an O(n) complexity value, in the hash chain generation. Then, for the Digital signature generation, 1.2 ms as the computational time and the complexity is O(n). Also, the Digital signature verification operation took 0.8 ms as the computational time with an O(n) complexity value.

Communication Overhead: It describes the extra information sent across the network as a result of security features like digital signatures and hash chain values. To make sure the framework doesn't negatively impact network performance, we assess this and we mentioned in the table below:

Table 2. Shows the Message size with Network latency

S.NO	Message Type	Message Size (bytes)	Network Latency (ms)
1	Message with Hash Chain	256	10
2	Message with Digital Signature	512	15

The size of the Message in bytes and Network latency are listed out in the above Table 2. Two main things are pointed out in the above table: that is, the message with a hash chain and the message with a digital signature. 256 (bytes) is the size of the message for a message with a hash chain; their network latency is 10 ms. And for the digital signature message size is 512 (bytes), with their network latency is 15 ms.

Security: It refers to how well the framework will defend against attacks like replay and tampering. We assess this to make sure the framework offers sufficient security measures.

In the above Table 3, attack types, with their prevention mechanism & effectiveness, are shown. We took two types of attacks we took. For the replay attack, the prevention

Table 3. Attack types with their prevention mechanism & effectiveness

S.NO	Attack Type	Prevention Mechanism	Effectiveness
1	Replay Attack	Hash Chain	High
2	Tampering Attack	Digital Signature	High

mechanism is a hash chain, and the effectiveness should be high. And for the tampering attack, the prevention mechanism is a digital signature, and the effectiveness should be high.

Table 4. Comparison with the different schemes

Scheme	Authentication	Integrity	Non-Repudiation
Proposed Scheme	✓	✓	✓
ECPP	✓	✓	✗
SPECS	✓	✗	✓
RAISE	✓	✓	✓

In the above Table 4, they compared the security features with different schemes. To evaluate the schemes, they used three key things: non-repudiation, which guarantees that a sender cannot deny sending a message; integrity, which guarantees that data cannot be modified or tampered with; and authentication, which confirms the identity of individuals or devices. All three security properties are offered by the Proposed Scheme and RAISE (Robust Authentication Scheme for VANET), while SPECS (Secure and Privacy Enhancing Communications Schemes) lacks Integrity, and ECPP (Efficient Conditional Privacy Preservation) lacks non-repudiation. In terms of security aspects, this comparison illustrates the advantages and disadvantages of each system.

Table 5. Comparison of different schemes with computational overhead & communication overhead

Scheme	Computational Overhead	Communication Overhead
Proposed Scheme	Low	Low
ECPP	Medium	Medium
SPECS	High	High
RAISE	Low	Medium

Table 5 shows how effectively various systems perform in terms of communication and processing overhead. Efficiency in processing power and network consumption is

demonstrated by the Proposed Scheme's low overhead in both categories. SPECS has a large overhead that could impact performance, and ECPP has low overhead in both categories. RAISE is also a high-performance processor since its overhead is low in calculation and middle in communication. Comparing will be necessary in order to judge the effectiveness and performance of each scheme.

4 Conclusion

In summary, has effectively established protection against both replay and tampering attacks in the proposed security architecture of VANETs with the required minimum of computing and communication overheads. In the analytic performance, it is possible to observe how efficient the framework is in the safeguard of VANET. Provision of a potent VANET solution is presented within this framework that is well-armed with security provisions. The comparison between other systems such as ECPP, SPECS, and RAISE shows the security and performance benefits of the system that we propose. In order to make intelligent transportation systems reliable and secure, all things considered, the suggested framework has potential concerning the security of VANET. In future, we need to develop the workability to a larger framework in VANET and integrating it with some more security and verify its efficiency in practice-based conditions. To the further advancement of VANET security and efficiency, to compare and analyze experimental data, we develop a platform on which the VANET security protocol can be tested. Through such a study, we get to guarantee the efficiency and security of intelligent transportation systems.

References

1. Al-Sultan, S., Al-Doori, M.M., Al-Bayatti, A.H., Zedan, H.: A comprehensive survey on vehicular Ad Hoc network. J. Netw. Comput. Appl. **37**, 380–392 (2014). https://doi.org/10.1016/j.jnca.2013.02.036
2. Rehman, S.U., Khan, M.A., Zia, T.A., Zheng, L.: Vehicular Ad-Hoc networks (VANETs)—An overview and challenges. J. Wirel. Netw. Commun. **3**(3), 29–38 (2013). https://doi.org/10.5923/j.jwnc.20130303.02
3. Yousefi, S., Mousavi, M.S., Fathy, M.: Vehicular Ad Hoc Networks (VANETs): Challenges and Perspectives. In: 6th International Conference on ITS Telecommunications, pp. 761–766. IEEE, Chengdu, China (2006). https://doi.org/10.1109/ITST.2006.289012
4. Li, F., Wang, Y.: Routing in vehicular Ad Hoc networks: A survey. IEEE Veh. Technol. Mag. **2**, 12–22 (2007)
5. Yousefi, S., Mousavi, M.S., Fathy, M.: Vehicular Ad Hoc networks (VANETs): Challenges and perspectives. In: 6th International Conference on ITS Telecommunications, pp. 761–766. IEEE, Chengdu, China (2006). https://doi.org/10.1109/ITST.2006.289012
6. Chainlink. What is a Replay Attack?
7. GeeksforGeeks. Replay Attack. https://www.geeksforgeeks.org/computer-networks/replay-attack/ (n.d.). Accessed 8 Jan 2026
8. Wu, Z., Gao, S., Cling, E.S., Li, H.: A study on replay attack and anti-spoofing for text-dependent speaker verification. In: Proceedings of the Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA), pp. 1–5. IEEE, Siem Reap, Cambodia (2014). https://doi.org/10.1109/APSIPA.2014.7041636

9. Wikipedia, Tamper proofing, https://en.wikipedia.org/wiki/Tamperproofing (n.d.). Accessed 8 Jan 2026
10. Thomas, P.: The application of hash chains and hash structures to cryptography. Royal Holloway Research Online (2009, August 4)
11. Patil, R.S., & N, J. (2023). Enhanced machine learning based techniques for security in vehicular Ad-Hoc networks. In: In: Proceedings of the International Conference on Advances in Communication and Computing Technology (InCACCT 2023). Piscataway, NJ: IEEE. 386–393. doi:https://doi.org/10.1109/InCACCT57535.2023.10141791
12. Huo, Q., Ning, Y., Bian, C., Sun, D.: Research on anti-replay attack mechanism of intelligent connected vehicles based on hashing chain and V2X communication. In: Proceedings of the International Conference Optoelectronic Information and Optical Engineering (OIOE2024). SPIE, Bellingham, WA (2025). https://doi.org/10.1117/12.3054402
13. Sinha, S.K., Mukhopadhyay, D.: Time efficient hash key generation for blockchain enabled framework. IEEE Access. **12**, 155867–155884 (2024). https://doi.org/10.1109/ACCESS.2024.34788
14. Roy, A., Karforma, S.: A survey on digital signatures and its applications. J. Comput. Inf. Technol. **3**(1&2), 45–69 (2012)
15. Rakhra, M., Singh, A., Singh, D., Shruti: Digital signature verification in cloud computing. In: 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, pp. 1–6. IEEE, Piscataway, NJ (2024). https://doi.org/10.1109/ICRITO61523.2024.10522372
16. Iqbal, S., Sujatha, B.R.: Secure authentication and key management based on hierarchical enhanced identity based digital signature in heterogeneous wireless sensor network. Wirel. Netw. **31**, 127–147 (2025). https://doi.org/10.1007/s11276-024-03745-x
17. Muzakkir, F.B., Darwito, H.A., Yuliana, M.: Developing web-based application for QR code digital signatures using OpenSSL. In: International Electronics Symposium (IES), Denpasar, Indonesia, vol. 2024, pp. 386–392. IEEE, Piscataway, NJ (2024). https://doi.org/10.1109/IES63037.2024.10665883
18. Microsoft. STRIDE Threat Model. https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats (n.d.)
19. Wuyts, K., Joosen, W.: LINDDUN privacy threat modeling: A step-by-step guide. LINDDUN privacy threat modeling: A tutorial. KU Leuven – LINDDUN Project (2015)
20. Raya, M., Hubaux, J.P.: Securing vehicular ad hoc networks. J. Comput. Secur. **15**(1), 39–68 (2007)