JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 08 Issue 01
2024

Research Article
https://doi.org/10.56979/801/2024

Using Blockchain Technology to Enhance Security in VANET: A Comprehensive Analysis

Rania Naveed[1*], Irshad Ahmed Sumra[2], Syed Aleem Muzaffar[3], and Sumiya Sundas[3]

[1]Department of Information Technology, Lahore Garrison University, Lahore, 54000, Pakistan.
[2]Department of Computer Science, Lahore Garrison University, Lahore, 54000, Pakistan.
[3]Department of Computer Science, Numl University, Multan, Lahore, 54000, Pakistan.
Corresponding Author: Rania Naveed. Email: ranianaveed1509@gmail.com

Received: November 11, 2024 **Accepted:** December 01, 2024

Abstract: Vehicular Ad-hoc Networks (VANETs) are critical for enhancing road safety and traffic efficiency through real-time communication among vehicles and infrastructure. However, VANETs face numerous security challenges, including availability, confidentiality, integrity, and authenticity threats. This paper explores various types of attacks targeting VANETs and discusses how blockchain technology can be leveraged to enhance security. Blockchain offers decentralized, tamper-resistant data storage and consensus mechanisms that can mitigate these threats effectively. This study provides a comparative analysis of VANET attack types, their impact on security goals, and proposes blockchain-based solutions to strengthen VANET security.

Keywords: VANET (Vehicular Ad-hoc Networks); V2V (Vehicle-to-Vehicle) (V2V); V2I/I2V (Vehicle-to-Infrastructure); RSU (Road Side Unit); AU (Application Unit).

1. Introduction

A Vehicular Ad-Hoc Network (VANET) is a type of mobile ad-hoc network that connects cars to the roadway. With the number of vehicles increasing daily, the occurrence of accidents is also on the rise. VANETs are designed to prevent accidents by delivering safety signals to vehicles with minimal delay [1]. Due to the growing number of applications aimed at passenger safety, VANETs are attracting wireless network manufacturers and researchers through innovative communication systems known as Intelligent Transport Systems (ITS) [2]. The increasing rate of road incidents globally highlights the importance of road safety and improved transportation. VANETs offer an effective solution for drivers and passengers by enhancing road safety and providing additional applications. This specialized branch of ad-hoc networks involves vehicles as network nodes, roadside units (RSUs), and onboard units (OBUs) [3][4].

The VANET vehicles are self-organizing devices that operate without centralized management or infrastructure. Collaboration between vehicles ensures decentralization, allowing for autonomous decision-making based on communication data to supplement their partial environmental perception. To facilitate communication among these entities, it is crucial for different systems to interoperate seamlessly despite the lack of standardized communication protocols for both Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I/I2V) interactions. Each vehicle must maintain a local routing table managed by a routing protocol, defining the next hop to all destination [5].

While VANETs offer significant benefits, they also present numerous security challenges. Critical messages are exchanged between vehicles, and this information, which can save lives, must be received promptly and disseminated widely. Ensuring the security of these communications in vehicular environments is essential to meet these requirements.

One promising solution to enhance VANET security is blockchain technology. Blockchain has demonstrated tremendous potential across various fields, and it offers a robust method for securing essential knowledge distribution in VANETs. Blockchain technology (BCT) is an adaptive software

paradigm originally designed to support Bitcoin, providing protection and anonymity in Peer-to-Peer (P2P) networks [6]. In a VANET context, blockchain can secure data by creating a tamper-proof ledger of event messages. Each new block is constructed from these messages and linked sequentially through hashing, forming a secure and verifiable chain [6, 7]. This approach not only ensures the integrity and authenticity of the transmitted information but also enhances the overall security framework of VANETs.

This paper is organized as follows: In Section 2, discusses various types of attacks that VANETs are susceptible to, highlighting the security challenges in these networks. Section 3. explores how blockchain technology can be utilized to enhance the security of VANETs, detailing specific applications and benefits. In Section 4, we present a comparative analysis of traditional security approaches versus blockchain-based solutions, illustrating the advantages and potential drawbacks. Finally, Section 5 concludes the paper, summarizing the key findings and suggesting future research directions.

2. Attacks on VANET

The Materials and Methods should be described with sufficient details to allow others to replicate and build on the published results. Please note that the publication of your manuscript implicates that you must make all materials, data, computer code, and protocols associated with the publication available to readers. Please disclose at the submission stage any restrictions on the availability of materials or information. New methods and protocols should be described in detail while well-established methods can be briefly described and appropriately cited. In VANETs, security is paramount because the transmitted packets contain life-critical information. It is vital that these packets reach drivers without any alterations or unauthorized data insertions. The following attacks are divided into four categories:

A. Availability Attack

Availability of information is crucial for the reliability of VANETs. When there is a lack of accessible information, it can lead to a significant decrease in the system's reliability [9].

a. *Malware Attack*: Malware is designed to perform malicious actions. The goals of malware are limited only by the imagination of its creator. Common malware objectives include:

(i) *Information Exfiltration:* This type of cybercrime involves stealing records, passwords, payment information, etc. Such malware can be highly costly for individuals, enterprises, or governments affected by it.

(ii) *Payment Application:* Some malware is designed to extort money directly from the target. Scareware, for instance, uses hollow threats to frighten the victim into paying money [10].

b. *Jamming Attack:* Jamming is a significant challenge to IEEE 802.15.4-based Wireless Sensor Networks. In a jamming attack, attackers degrade network capacity by interfering with the transmission of packets [11].

c. *Denial-of-Service (DoS) Attacks:* A DoS attack aims to shut down a system or network, preventing its intended users from accessing it. This is done by overwhelming the target with traffic or sending information that causes it to crash [12].

d. *Blackhole Attack:* This attack targets the availability of ad hoc networks, including VANETs. In a blackhole attack, packets are dropped by a compromised router, leading to a denial-of-service situation. This can happen due to various factors affecting the router [13].

e. *Gray Hole Attack:* This is a variant of the black hole attack. It occurs when malicious vehicles selectively forward some data packets while discarding others, making it difficult to detect [14].

f. *Spamming Attack:* Spamming involves using messaging systems to send unsolicited communications (spam) to many recipients. This often includes commercial advertisements, non-commercial proselytization, or phishing attempts with fraudulent intentions [15].

g. *Greedy Behavior Attack:* This attack primarily impacts the MAC functionality. A malicious vehicle exploits the MAC protocol to maximize its bandwidth usage for multiple applications, leading to traffic congestion and collisions in the broadcast channel, which can delay legitimate services for registered users [16].

h. *Broadcast Tampering:* In this attack, attackers inject false safety messages into the network. These messages can include fake traffic alerts, such as false reports of accidents or traffic delays, creating critical situations [17].

B. Authentication Attacks in VANET

The Authentication is a vital feature of the VANET system, used to protect the network from attacks by malicious nodes. It safeguards VANETs from both external and internal threats [18].

a. Sybil Attack: This is one of the most severe attacks, where a node uses multiple fake identities to interfere with the normal functioning of VANET services by sending multiple messages [19].
b. Impersonation Node Attack: This attack occurs when an attacker successfully acquires and uses a valid user ID belonging to another registered VANET user [14].
c. Message Tampering: In this common attack, the attacker modifies messages shared in Vehicle-to-Vehicle (V2V) or Vehicle-to-Infrastructure (V2I) communications to create counterfeit responses.
d. Tunnelling Attack: The tunnelling attack, akin to the wormhole attack, involves establishing a private communication channel within the VANET network. By joining VANETs from two distant locations, the attacker creates the illusion that nodes far apart are neighbors [20].
e. Free-Riding Attack: The free-riding attack is viral in nature and involves false authentication attempts and cooperative message authentication by a malicious user. During this attack, the malicious actor exploits the security measures of other users without contributing their own efforts. This behavior is often referred to as free riding and poses a significant threat to the authentication of cooperative messages.
f. Masquerading Attack: This involves using messaging systems to send unwelcome communications (spam) to many recipients, often for commercial advertisements, non-commercial proselytization, or phishing. If the licensing mechanism is not fully secured, it can become highly vulnerable [21].
g. GPS Spoofing: In a GPS spoofing attack, a radio transmitter near the target interferes with legitimate GPS signals. The attacker can either block the data or send incorrect coordinates. Accurate and authentic node positioning is crucial in VANETs [22].

C. Data Integrity Attack in VANET

The Ensuring data integrity in VANETs involves maintaining the accuracy and trustworthiness of data exchanged between nodes, RSUs and AS areas through message exchanges. Integrating digital signatures with application access verifies the authenticity of messages [23]. Attacks on data integrity, such as tampering with vehicle sensors to manipulate data measurements or altering transmitted data, can compromise the reliability of message transmissions. It is crucial to implement effective mechanisms to safeguard the vehicle network from these types of attacks [24].

a. Replay Attack: A replay attack is a network exploit used to maliciously replicate or disrupt legitimate data transmissions [25]. Operating at a relatively low sophistication level, replay attacks are inherently passive in nature.
b. Message Tampering Attack: During a message tampering attack, an adversary alters the packet headers to redirect messages to another address or modifies data on the target system without altering the intended outcome. These passive attacks often serve as preliminary steps towards more aggressive actions [26].
c. Illusion Attack: In an illusion attack, malicious data obtained from antennas or sensors is used to fabricate misleading traffic alerts, presenting false traffic conditions to nearby vehicles [27].

D. Confidentiality Attacks

The Confidentiality in VANETs ensures that sensitive information remains undisclosed to unauthorized entities within the network [28]. It prevents unauthorized access to private details such as names, license plates, and locations. Pseudonyms are commonly employed in vehicle networks to preserve privacy, where each vehicle node is encoded with multiple unique pseudonyms. Messages are authenticated or signed with distinct keys associated with these pseudonyms, ensuring that they cannot be linked back to the vehicle's true identity without proper authorization [29].Attacks on confidentiality undermine this vital safety requirement in vehicle communications, aiming to intercept messages meant for authorized recipients only [30]. This security requirement is particularly crucial in group communications, where only designated group members should access sensitive information.

The Ensuring the confidentiality of messages exchanged among vehicle network nodes is challenging due to techniques like eavesdropping, where unauthorized parties intercept and collect information through broadcasted messages. Attackers exploit vulnerabilities in VANET setting, gathering information covertly from unsuspecting users [31].

The following are types of attacks that compromise confidentiality.

a. Eavesdropping Attack: Eavesdropping is a common threat in wireless networking technologies like MANETs and VANETs, where attackers aim to obtain confidential information, including user identities and vehicle locations, from secure transmissions [28].
b. Traffic Analysis: In this attack, attackers analyze the traffic flow within the vehicle network to gather comprehensive information about communication patterns, email addresses, and transactional details without modifying the data [29].
c. Man-in-the-Middle Attack: In V2V communication, a man-in-the-middle attack involves intercepting and potentially altering communications between vehicles. The attacker gains access to all V2V traffic, posing as a legitimate participant in private exchanges [32].
d. Social Attack: Social attacks target the distraction of drivers by disseminating unethical or immoral messages to passengers. These attacks aim to influence the behavior and efficiency of vehicle operations within the VANET system [33].

3. Blockchain Technology

The Blockchain operates as a decentralized ledger system designed to securely and transparently record transactions, eliminating reliance on centralized authorities for record-keeping. Instead, it relies on a network of participants known as "nodes," each of which maintains a complete copy of the ledger containing all transaction records. This distributed architecture prevents any single entity from controlling the information, thereby ensuring transparency and enhancing security. Transactions are stored in blocks within the blockchain, with each block linked to the previous one through a cryptographic hash value.

The integrity of blockchain data is maintained through a cryptographic hash function, such as SHA-256, which converts data into fixed-size, irreversible strings known as digests. This hash function is deterministic, meaning the same input always produces the same output, and any slight change in input generates a substantially different hash. These properties make altering blockchain data extremely challenging without detection. [35]

At the inception of a blockchain is its genesis block, serving as the foundational block containing essential data shared among all nodes, establishing a common starting point. The Merkle tree, another critical component, organizes data hierarchically by hashing child nodes to produce parent node hashes. This structure facilitates efficient verification of block contents using fixed-length hashes, thereby reducing the storage requirements for individual transactions [34-36]. The Merkle Hash, derived from the Merkle algorithm, ensures the cryptographic integrity of transactions within each block by collectively hashing them, with each block also including a hash of its predecessor's data.

A. Blockchain Consensus Mechanisms

In decentralized networks like Ethereum, achieving consensus among network nodes on current system states is crucial. This is facilitated through consensus mechanisms [37], which prevent economic attacks such as the "51% attack" where an intruder theoretically controls the majority of the network and compromises its integrity. Different consensus mechanisms address this security dilemma through various rules and contributions from participating blockchain nodes.

Proof of Work (PoW): PoW is a widely recognized consensus algorithm in public blockchains like Ethereum. It ensures agreement among nodes and defends against economic attacks on stored blockchain data [38, 39].

Proof of Stake (PoS): PoS provides decision-making authority to stakeholders who hold a stake in the blockchain network. It offers an alternative approach to achieving consensus [40].

B. Blockchain Application in VANET

In VANET, the adoption of blockchain introduces an immutable distributed ledger concept for secure message propagation. Inspired by the Bitcoin blockchain's capabilities, this approach has become feasible in recent years [6].

RSU (Road-Side Unit): RSU is a DSRC transceiver typically installed along roadways or pedestrian pathways. It can also be mobile, such as mounted on vehicles or handheld devices, with limitations on its operational scope [41]. The architecture of blockchain –based VANET is given in figure 1.

VANET Message: VANETs exhibit distinct characteristics including organized network structures, high-speed vehicle nodes, variable but constrained topologies, diverse mobility patterns, and wireless

signal interference from physical obstacles. These factors influence communication reliability and network partitioning [42].

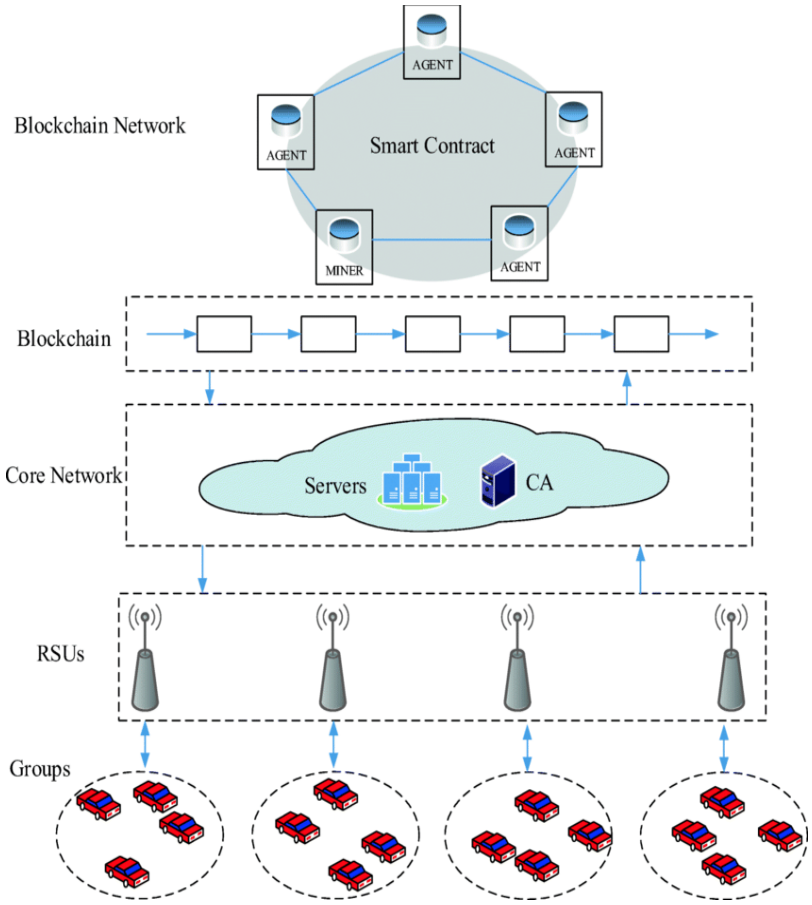

Figure 1. Blockchain based VANET Architecture [43]

C. Blockchain Solutions

The Blockchain technology offers several mechanisms that can help detect and mitigate various attacks in VANETs related to availability, confidentiality, integrity, and authenticity:

Availability Attacks Mitigation: Blockchain's decentralized nature and consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), ensure that no single point of failure exists. Nodes in the blockchain network validate transactions and maintain the integrity of the ledger. Even if some nodes are compromised or unavailable, the consensus mechanism ensures that valid transactions can still proceed, thus mitigating availability attacks [44].

a. Confidentiality Attacks Mitigation: Blockchain enhances confidentiality by using cryptographic techniques. Public and private keys are used to encrypt and decrypt transactions, ensuring that only authorized parties can access sensitive information. Pseudonymization techniques, where each node or participant in the network is represented by pseudonyms, add an additional layer of privacy protection. This prevents attackers from identifying specific users or intercepting confidential data [45].
b. Integrity Attacks Mitigation: Blockchain ensures data integrity by design. Each block in the blockchain contains a cryptographic hash of the previous block's data, creating a chain of blocks that are linked together. Any attempt to alter data in a block would require recalculating the hashes of all subsequent blocks, which is computationally impractical due to the decentralized nature and consensus mechanism of the blockchain. This makes it extremely difficult for attackers to tamper with data without detection [46].
c. Authenticity Attacks Mitigation: Blockchain employs digital signatures and cryptographic hash functions to verify the authenticity of transactions and messages. Each transaction is signed with the sender's private key, and the recipient can verify the sender's identity using the corresponding public key. This ensures that only authorized parties can initiate transactions or communicate within the

network. Any attempt to forge transactions or manipulate data would be immediately detected by other nodes in the network during the verification process [46].

4. Comparative Analysis

Table 1. Comparative Analysis of VANET Attack Types and Affected Layers

Attack Name	Attack Type	Affected Layer	Description
Denial-of-Service (DoS)	Availability	Network Layer	Overwhelms the network with traffic, disrupting communication services.
Eavesdropping	Confidentiality	Physical and Network Layers	Intercepts and monitors wireless communications to gather confidential information.
Message Tampering	Authentication, Integrity	Network Layer	Modifies data packets during transmission to disrupt or alter information integrity
Man-in-the-Middle (MitM)	Confidentiality	Application Layer	Intercepts and alters communications between nodes, impersonating legitimate participants.
Replay Attack	Integrity	Application Layer	Captures and re-transmits data packets to deceive recipients or disrupt communication sequences.
Illusion Attacks	Integrity	Application Layer	Sends false traffic information to mislead vehicles, potentially causing traffic congestion or accidents.
Information Exfiltration	Availability	Physical and Network Layer	Passively gathers information by intercepting wireless transmissions, compromising user privacy.
Traffic Anaylsis	Confidentiality	Network Layer	Analyzes communication patterns to deduce user behaviors and network activities, potentially breaching privacy.
Social Attack	Confidentiality	Application Layer	Delivers distracting or misleading messages to drivers, potentially compromising safety and attention.

5. Conclusion

In conclusion, securing VANETs against evolving cyber threats is paramount to ensuring safe and reliable communication among vehicles and infrastructure. Our comparative analysis has highlighted the diverse nature of attacks targeting VANETs, ranging from availability disruptions to confidentiality breaches and integrity compromises. Blockchain technology emerges as a promising solution, providing immutable data records, decentralized consensus, and enhanced cryptographic security. By integrating blockchain into VANET architectures, we can mitigate risks associated with malicious activities, enhance data integrity, ensure message authenticity, and safeguard user privacy. Future research should focus on

practical implementations and scalability of blockchain solutions tailored to VANET environments to achieve robust and resilient vehicular communication system.

Table 2. Comparative Analysis of VANET Attack Types, Security Goals Affected, and Blockchain Solutions

Attack Type	Attack	Detection Difficulty	Mitigation Strategy	Impact on Safety	Security Goal Affected	Blockchain Solution
Availability Attacks	Availability	Moderate	Redundant communication paths and load balancing	High	Availability	Consensus mechanisms, fault tolerance
Confidentiality Attacks	Confidentiality	High	Encryption, pseudonymization	Moderate	Confidentiality	Public/private key encryption
Integrity Attacks	Integrity	High	Blockchain consensus, digital signatures	High	Integrity	Hash functions, Merkle trees
Authenticity Attacks	Authenticity	High	Digital certificates, authentication protocols	High	Authenticity	Public key infrastructure (PKI)
Replay Attacks	Replay	Moderate	Timestamps, nonce values	Moderate	Authenticity, Integrity	Timestamps, smart contracts
Message Tampering Attacks	Message Tampering	High	Hash functions, checksums	High	Integrity	Hash functions
Illusion Attacks	Illusion	Moderate	Authentication of safety messages	High	Integrity, Confidentiality	Digital signatures
Eavesdropping Attacks	Eavesdropping	Moderate	Encryption, secure communication protocols	Moderate	Confidentiality	Encryption
Traffic Analysis Attacks	Traffic Analysis	High	Traffic encryption, anonymization	Moderate	Confidentiality	Traffic encryption
Man-in-the-Middle Attacks	Man-in-the-Middle	High	End-to-end encryption, secure key exchange	High	Authenticity, Integrity	End-to-end encryption
Social Attacks	Social	Low	Driver awareness programs, filtering algorithms	Low	Availability	Behavioral analysis, filtering algorithms

References

1. S. Boussoufa-Lahlah, F. Semchedine, and L. BoualloucheMedjkoune, "Geographic routing protocols for Vehicular Ad hoc NETworks (VANETs): A survey," Vehicular Communications, vol. 11, pp. 20-31, 2018.
2. C. T. Barba, M. A. Mateos, P. R. Soto, A. M. Mezher, and M. A. Igartua, "Smart city for VANETs using warning messages, traffic statistics and intelligent traffic lights," in 2012 IEEE intelligent vehicles symposium, 2012, pp. 902-907.
3. M. A. Shahid, A. Jaekel, C. Ezeife, Q. Al-Ajmi, and I. Saini, "Review of potential security attacks in VANET," in 2018 Majan International Conference (MIC), 2018, pp. 1-4.
4. I. A. Sumra, H. B. Hasbullah and J. -l. A. Manan, "Using TPM to ensure security, trust and privacy (STP) in VANET," 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW),Riyadh, Saudi Arabia, 2015, pp. 1-6, doi: 10.1109/NSITNSW.2015.7176402.
5. A. K. Ahmed, M. Q. Taha, and A. S. Mustafa, "On-road Automobile License Plate Recognition Using Co-Occurrence Matrix," Journal of Advanced Research in Dynamical & Control Systems, vol. 10, 2018.
6. Rakesh Shrestha, Rojeena Bajracharya, Anish P. Shrestha, Seung Yeob Nam, A new type of blockchain for secure message exchange in VANET, Digital Communications and Networks, Volume 6, Issue 2, ISSN 2352-8648, https://doi.org/10.1016/j.dcan.2019.04.003.
7. S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash SyNakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Consulted, 19. doi:10.1007/s10838-008-9062-0stem, J. Gen. Philos. Sci., vol. 39, no. 1, pp. 5367, 2008.
8. Appasani, B.; Mishra, S.K.; Jha, A.V.; Mishra, S.K.; Enescu, F.M.; Sorlei, I.S.; Bizon, N. Blockchain-enabled smart grid applications: Architecture, challenges, and solutions. Sustainability 2022, 14, 8801.
9. M. Kassim, R. Rahman, and R. Mustapha, "Mobile ad hoc network (MANET) routing protocols comparison for wireless sensor network," in Proceedings of the IEEE International Conference on System Engineering and Technology, ICSET, pp. 148–152, Shah Alam, Malaysia, January 2011.
10. I. A. Sumra, I. Ahmad, H. Hasbullah and J. -l. bin Ab Manan, "Classes of attacks in VANET," 2011 Saudi International Electronics, Communications and Photonics Conference (SIECPC),Riyadh, Saudi Arabia, 2011, pp. 1-5, doi: 10.1109/SIECPC.2011.5876939
11. Yan-qiang, Sun, and Wang Xiao-dong. "Jamming Attacks and Countermeasures in Wireless Sensor Networks." Handbook of Research on Developments and Trends in Wireless Sensor Networks, pp. 334–352., doi:10.4018/978-1-61520-701-5.ch015.
12. Sumra, I.A., Hasbullah, H.B., AbManan, Jl.B. (2015). Attacks on Security Goals (Confidentiality, Integrity, Availability) in VANET: A Survey. In: Laouiti, A., Qayyum, A., Mohamad Saad, M. (eds) Vehicular Ad-hoc Networks for Smart Cities.
    Advances in Intelligent Systems and Computing, vol 306. Springer, Singapore.
13. I. A. Sumra, H. Hasbullah and J. -l. A. Manan, "VANET security research and development ecosystem," 2011 National Postgraduate Conference, Perak, Malaysia, 2011, pp. 1-4, doi: 10.1109/NatPC.2011.6136344.
14. I. A. Sumra, I. Ahmad, H. Hasbullah and J. -l. bin Ab Manan, "Behavior of attacker and some new possible attacks in Vehicular Ad hoc Network (VANET)," 2011 3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Budapest, Hungary, 2011, pp. 1-8.
15. S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," Vehicular Communications, vol. 9, pp. 19-30, 2017, doi: 10.1016/j.vehcom.2017.02.001.
16. S. Benkerdagh and C. Duvallet, "Cluster- based emergency message dissemination strategy for VANET using V2V communication," International Journal of Communication Systems, vol. 32, no. 5, p. e3897, 2019, doi: 10.1002/dac.3897.
17. Daeinabi and A. G. Rahbar, "Detection of malicious vehicles (DMV) through monitoring in vehicular ad-hoc networks," Multimedia Tools and Applications, vol. 66, no. 2, pp. 325–338, 2013
18. J. R. Douceur, "+e sybil attack," in Peer-To-Peer Systems, pp. 251– 260, Springer, Berlin, Germany, 2002.
19. S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," Telecommunication Systems, vol. 50, no. 4, pp. 217-241, 2012, doi: 10.1007/s11235-010-9400-5.
20. "What Is a Masquerade Attack? - Definition from Techopedia." Techopedia.com,www.techopedia.com/definition/4020/masqueradeatt
    ack#:~:text=A%20masquerade%20attack%20is%20an,vulnerable%2 0to%20a%20masquerade%20attack.

21. Korolov, Maria. “What Is GPS Spoofing? And How You Can Defend against It.” CSO Online, CSO, 7 May 2019, www.csoonline.com/article/3393462/what-is-gps-spoofing-and-howyou-candefendagainstit.html html#:~:text=GPS%20spoofing%20is%20an%20attack,or%20could%20 transmit%20inaccurate%20coordinates.
22. T. Karimireddy and A. G. A. Bakshi, "A hybrid security framework for the vehicular communications in VANET," in 2016 international conference on wireless communications, signal processing and networking (WiSPNET), 2016, pp. 1929-1934, doi: 10.1109/WiSPNET.2016.7566479.
23. Festag, "Cooperative intelligent transport systems standards in Europe," in IEEE communications magazine, vol. 52, no. 12, pp. 166-172, December 2014, doi: 10.1109/MCOM.2014.6979970.
24. Replay Attack.” Wikipedia, Wikimedia Foundation, 27 Feb. 2021, en.wikipedia.org/wiki/Replay_attack#:~:text=A%20replay%20attack%20(also%20known,or%20fraudulently%20repeated%20or%20delayed
25. Shah, A. M., Aljubayri, M., Khan, M. F., Alqahtani, J., Sulaiman, A., & Shaikh, A. (2023). ILSM: Incorporated Lightweight Security Model for Improving QOS in WSN. Computer Systems Science & Engineering, 46(2).
26. “What Is Active Attack? - Definition from WhatIs.com.” WhatIs.com,TechTarget,21 Aug. 2014, whatis.techtarget.com/definition/active-attack.
27. N. W. Lo and H. C. Tsai, “Illusion attack on VANET applications—a message plausibility problem,” in Proceedings of the IEEE Globecom Workshops, Washington, DC, USA, Novenber 2007.
28. A. Sumra, I. Ahmad, and H. Hasbullah, "Classes of attacks in VANET," in 2011 Saudi International Electronics, Communications and Photonics Conference (SIECPC), 2011, pp. 1-5, doi: 10.1109/SIECPC.2011.5876939..
29. M. Abu Talib, S. Abbas, Q. Nasir, and M. F. Mowakeh, "Systematic literature review on Internet-of-Vehicles communication security," International Journal of Distributed Sensor Networks, vol. 14, no. 12, 2018, doi: 10.1177/1550147718815054
30. Sajjad, R., Khan, M. F., Nawaz, A., Ali, M. T., & Adil, M. (2022). Systematic analysis of ovarian cancer empowered with machine and deep learning: a taxonomy and future challenges. Journal of Computing & Biomedical Informatics, 3(02), 64-87.
31. R. Hussain, F. Hussain, and S. Zeadally, "Integration of VANET and 5G Security: A review of design and implementation issues," Future Generation Computer Systems, vol. 101, pp. 843-864, 2019, doi: 10.1016/j.future.2019.07.006.
32. Abbas, F., Iftikhar, A., Riaz, A., Humayon, M., & Khan, M. F. (2024). Use of Big Data in IoT-Enabled Robotics Manufacturing for Process Optimization. Journal of Computing & Biomedical Informatics, 7(01), 239-248.
33. J.-C. Xi, Q.-Q. Kong, and X.-G. Wang, "Spatial polarization of villages in tourist destinations: A case study from Yesanpo, China," Journal of Mountain Science, vol. 12, no. 4, pp. 1038-1050, 2015, doi: 10.1007/s11629-014-3358-9
34. M. L. Das, A. Saxena, V. P. Gulati, and D. B. Phatak, "A novel remote user authentication scheme using bilinear pairings," Computers & Security, vol. 25, no. 3, pp. 184-189, 2006, doi: 10.1016/j.cose.2005.09.002.
35. M. Raya and J.-P. Hubaux, "Security aspects of inter-vehicle communications," in 5th Swiss Transport Research Conference (STRC), 2005, no. CONF.
36. “Merkle Tree.” Brilliant Math & Science Wiki, brilliant.org/wiki/merkle-tree/.
37. “Merkle Tree in Blockchain Archives.” Blockchain, www.magicblockchainqa.com/category/merkle-tree-in-blockchain/.
38. R. C. Merkle, A digital signature based on a conventional encryption function, in proceedings of CRYPTO87, pp. 1620, 1987.
39. Siraj, M. A., Rehman, A., Aziz, O., & Khan, M. F. (2021). Systematic Literature Review: Smart Drone for Early Smoke Detection in Forest Using IOT. Journal of Computing & Biomedical Informatics, 2(01), 80-88.
40. Han, Meng, et al. “A Survey on Security and Privacy Issues of Blockchain Technology.” Mathematical Foundations of Computing, American Institute of Mathematical Sciences, 3 May 2018, www.aimsciences.org/article/doi/10.3934/mfc.2018007.
41. Haider, R. A., Zafar, K., Basharat, S., & Khan, M. F. (2024). Neural Network Based Skin Cancer Classification from Clinical Images: Accuracy and Robustness Analysis. Journal of Computing & Biomedical Informatics.
42. “Consensus Mechanisms.” Ethereum.org, ethereum.org/en/developers/docs/consensus-mechanisms/.
43. “Proof-of-Work (PoW).” Ethereum.org, ethereum.org/en/developers/docs/consensus-mechanisms/pow/.
44. S. King and S. Nadal, ” PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake,” Online, 2012. [Available: https://peercoin.net/assets/paper/peercoinpaper.pdf] (Accessed on Nov. 14, 2018)

45. Quittner, Josh. "The Future Begins with The Road Side Unit." Medium, Predict, 30 Jan. 2021, medium.com/predict/edge-computing-is-somuch-more funac2a8a23e696#:~:text=%E2%80%9CRoad%20Side%20Unit%20(RSU),hand%2Dcarried%20unit%20is%20stationary.
46. "A Survey and Comparative Study of Broadcast Warning Message Dissemination Schemes for VANETs." Mobile Information Systems, Hindawi, 28 Mar. 2016, www.hindawi.com/journals/misy/2016/8714142/.
47. Li, H., Pei, L., Liao, D., Sun, G., & Xu, D. (2019). Blockchain meets VANET: An architecture for identity and location privacy protection in VANET. Peer-to-Peer Networking and Applications, 12, 1178-1193.
48. Investopedia. (n.d.). *Consensus mechanism in cryptocurrency*. Investopedia. from https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp
49. UEEX. (n.d.). *Cryptography in blockchain technology: A beginner's guide*. UEEX Blog. from https://blog.ueex.com/cryptography-in-blockchain-technology-a-beginners-guide/
50. Rapid Innovation. (n.d.). *What is blockchain security?* Rapid Innovation Blog. from https://www.rapidinnovation.io/post/what-is-blockchain-security