A New Framework for Enhancing VANETs through Layer 2 DLT Architectures with Multi-Party Threshold Key Management and PETs

Haitham Y. Adarbah
haitham.adarbah@gulfcollege.edu.om
Gulf College
Mehmet Sabir Kiraz
De Montfort University
Suleyman Kardas
Batman University
Ali H. Al-Bayatti
De Montfort University
Hilal Mohammed Yousif Albayatti
Applied Science University

Research Article

Keywords:

Posted Date: March 18th, 2024

DOI: https://doi.org/10.21203/rs.3.rs-4093268/v1

Additional Declarations: No competing interests reported.

A New Framework for Enhancing VANETs through Layer 2 DLT Architectures with Multi-Party Threshold Key Management and PETs

Haitham Y. Adarbah[1], Mehmet Sabir Kiraz[2], Suleyman Kardas[3], Ali H. Al-Bayatti[2], and Hilal M. Y. Albayatti[5]

[1]Gulf College, Muscat, Sultanate of Oman
[2,4]De Montfort University, Leicester, UK
[3]Batman University, Batman, Turkiye.
[5]Applied Science University, Kingdom of Bahrain.
[1,2]The Corresponding Authors:haitham.adarbah@gulfcollege.edu.om and mehmet.kiraz@dmu.ac.uk

***Abstract*—This study provides an architectural framework and a comprehensive examination of how the combination of threshold key management, privacy-enhancing technologies (e.g., homomorphic encryption, secure multi-party Computation), and Decentralised Ledger Technologies (DLT) enhances the security and privacy of Vehicle Ad-Hoc Networks (VANETs). We also examine the challenges of existing VANET structures, with a particular focus on trust, privacy, and scalability concerns. Our proposed architecture shifts from centralised to decentralised systems, highlighting the advantages of a decentralized ledger framework, specifically in ensuring the robustness, strong availability, integrity, and resilience of data against various cyber security threats. The architecture uses Layer 2s instead of Layer 1s as Layer 2s is much cheaper and faster. Furthermore, we explore how the aforementioned advanced cryptographic mechanisms are utilized in VANETs for improving key management, the distribution of trust, and data privacy, together with privacy-preserving data analysis, aiming to achieve a resilient vehicle-to-everything (V2X) communication and privacy-preserving data analysis. We conclude by highlighting potential future directions for more secure, efficient, and resilient VANET systems in the era of 5G and beyond.**

I. Introduction

Intelligent transport systems depend on Vehicular Ad-hoc Networks (VANETs) for dynamic vehicle-roadside infrastructure communication. VANETs improve road safety and efficiency by providing wireless connectivity for traffic control and autonomous driving. The growing complexity and requirement for real-time data processing in these networks require comprehensive security and privacy procedures to ensure vehicular communication system stability and trustworthiness. However, this brings up a series of significant challenges, such as the concepts of trust, privacy, and scalability. To ensure the sustainability and reliability of these systems, it is crucial to address these challenges [39], [16], [6].

To ensure effective functionality and enhance safety, it is essential to provide better trust in VANETs. VANETs use Certificate Authorities (CAs) to authenticate automobiles and roadside equipment. Building trust in VANETs is very important because it is what makes safety-critical applications like avoiding collisions, managing traffic flow, and planning routes dynamically possible [74], [34], [8] work. However, relying on centralized CAs has significant concerns. For example, a CA may issue a certificate of trustworthiness that can be compromised in the event of a successful attack.

This has the potential to allow adversaries to impersonate authentic entities, leading to the dissemination of inaccurate information or even more concerning, providing attackers with the capability to alter traffic patterns. The existence of these vulnerabilities has the potential to significantly disrupt vehicle communications, leading to serious safety consequences such as crashes or extensive traffic congestion. Ensuring the mitigation of this risk is critical for the ongoing development of VANETs.

The CertLedger architecture [45] improves the existing weaknesses of PKI architecture by means of validity, storage, and revocation procedures of TLS certificates, simplifying the management of Trusted CA certificates within a unified and immutable decentralized network such as Ethereum. During the process of TLS handshakes, clients acquire verifications of certificate validity directly from the owners of the domain, hence improving the privacy of users. The issue of privacy in VANETs is of similar significance, as vehicles consistently transmit confidential data [83], [12], [15]. The existing privacy safeguards, such as pseudonymization, may not be sufficient in the continuously changing landscape of VANETs [64], [63]. Therefore, there is a need for more sophisticated privacy-preserving methods. Unfortunately, the use of conventional PKI systems makes the system more expensive because the use of the same certificates would break the unlinkability requirement. Furthermore, the authors in [16] proposed the utilisation of self-blindable certificates to enable anonymous communications, ensuring that the contact remains untraceable using a single valid certificate. Furthermore, the examination of data is of utmost significance. However, the attention should shift towards privacy issues. Hence, the incorporation of Privacy Enhancing Technologies (PETs), including homomorphic encryption [77], multi-Party computation [5], [48],

[23], [17], private set intersection [68], and trusted execution environments such as HSM and SGX [39], is crucial in VANETs. This connection allows for complete analysis that can assist manufacturers and road workers in building new roads or improving existing ones, based on informed data-driven choices.

The issue of scalability is also of greatest significance in the context of VANETs, especially considering the increasing connectivity and autonomy of vehicles in the ecosystem. As society enters a new era, the increasing quantity of vehicles on the road that have communication capabilities possesses the potential to surpass the current infrastructure's capacity to effectively handle and analyze the extensive volumes of data that are generated [46], [82], [7]. The task at hand encompasses not only the magnitude of data but also the speed and diversity of data that necessitates prompt processing and action-taking to guarantee uninterrupted functionality and safety within the realm of road transport [82], [9].

This paper aims to create a secure and efficient framework for VANETs by addressing trust, privacy, and scalability challenges. The study focuses on strategic aspects of VANETs, translating theoretical foundations into feasible solutions. The contributions of the paper can be summarised as follows:

- We propose a new framework that prevents single-point failures in VANETs by improving security, privacy, availability, integrity, and network resilience through the use of DLT with Multi-Party Threshold Key Management. The architecture features multiple layers, including the Application Layer for data security and authentication (e.g., Layer 2 solutions on Ethereum such as zkSync [85], Polygon zkEVM [43], Scroll [57]), a peer-to-peer network layer for data accessibility (e.g., Arweive [73], Siacoin [66], IPFS [70]), and the physical network layer for structural integrity and operational stability.
- We also aim to incorporate PETs such as threshold key management, homomorphic encryption, and secure multi-party computation into the new decentralized framework of VANET systems for further privacy-preserving data analysis. This keeps data confidential during transmission and processing. Multi-party threshold signatures use multiple signers to sign transactions, reducing fraud [49], [22]. The threshold homomorphic encryption system [28], [20], [29] requires a threshold number of participants for decryption, ensuring data privacy to analyze data without revealing the private data of participating parties.
- We finally identify some potential future directions for VANETs to integrate with emerging technologies like AI and IoT, developing quantum-resistant security solutions (i.e., post-quantum cryptographic algorithms), improving scalability and efficiency in high-density urban contexts, and conducting real-world implementation and testing to gain insights into the actual challenges and performance of the proposed architecture.

II. Security and Privacy Requirements of VANETs and Potential Enhancements

The existing solutions that offer essential requirements for VANETs, such as confidentiality, integrity, minimal trust assumptions, privacy preservation, and scalability, are notably scarce and present significant challenges. Following an extensive review, we identified several obstacles that are commonly encountered across all VANET architectures, which are detailed and presented in Table I. The table summarises the crucial security and privacy requirements that are necessary for the strong operation of VANETs. It also provides a thorough examination of the various security aspects, emphasizing important areas such as Authentication, which employs cryptographic methods like digital signatures and certificates to verify identities within VANETs; Integrity, which guarantees secure data transmission through cryptographic hashes and digital signatures; and Availability, which concentrates on network resilience against threats such as Denial of Service (DoS) attacks. It also emphasizes the utmost significance of Non-repudiation for ensuring legal responsibility, Privacy for protecting user identity credentials, and Access Control for regulating information flow and network resources. Table I discusses the security and privacy requirements of VANETs.

This research paper aims to emphasize trust management through decentralization using a public, transparent, and immutable ledger on a peer-to-peer network. This study also seeks to leverage the transparency and data immutability of VANETs to advance the field.

III. Related Work

Over the past decade, both researchers and industries have demonstrated a keen interest in deploying diverse Integrity, Trust, Privacy, and Scalability solutions for VANETs. Our analysis in this section reflects changing security, privacy, and trust management needs. Centralized architectures consistently face security and privacy vulnerabilities, potentially leading to irreversible scenarios of attacks and damages. Existing conventional PKI-based solutions have drawbacks such as centralized entities being eliminated, increasing memory usage for certificates and Certificate Revocation Lists (CRLs), and reducing single points of failure.

Trust management is a substantial obstacle in VANETs, wherein the process of authentication is employed to validate the legitimacy of vehicle-to-vehicle communication. However, it is unable to effectively mitigate the risk of permitted vehicles engaging in the deliberate transmission of fraudulent or modified communications. Many privacy-preserving authentication surveys for VANETs have been conducted in [15], [21], [50], [51], [55]. These studies cover VANET routing protocols, security, privacy, and hazards and threats. However, only a few of them provide detailed descriptions in algorithmic/protocol level and trust assumptions, privacy versus unlinkability, reliability of resources, and potential future challenges.

Radio communication interfaces will enable VANETs as vehicles become more intelligent. Vehicles serve as mobile nodes in these specialised mobile ad-hoc networks. VANETs have

TABLE I
SECURITY AND PRIVACY REQUIREMENTS OF VANETS

Requirement	Description
Authentication	Authentication in VANETs uses cryptographic techniques like digital signatures and certificates to verify the identity of communicating vehicles and infrastructure, preventing impersonation and false data dissemination.
Integrity	Integrity in VANETs ensures data transmission between vehicles and infrastructure is secure, using cryptographic hashes and digital signatures for safety-critical messages like collision warnings, and Message Authentication Codes (MACs) for verification.
Availability	VANETs' availability, including resilience against DoS attacks, is crucial for emergency and safety communication. Redundant system designs and efficient network management strategies enhance availability.
Non-repudiation	Non-repudiation in VANETs ensures message transmission, preventing entities from denying origin, crucial for legal scenarios like traffic violations and accident investigations, using digital signatures.
Privacy	VANETs protect user identities and locations, using pseudonyms and cryptographic techniques to prevent tracking and profiling while balancing anonymity with security needs for accountability.
Access Control	Access Control in VANETs manages sensitive information flow and efficient communication. It can be achieved through role-based systems or cryptographic techniques, preventing unauthorized use of network resources.
Efficiency	VANETs require efficient security mechanisms, cryptographic algorithms, and streamlined protocol designs to ensure rapid communication in high-speed vehicles while balancing security with fast data exchange.
Scalability	VANETs' scalability involves security mechanisms that can adapt dynamically to high mobility and large nodes, often involving decentralized approaches and efficient key management for security and performance.
Confidentiality	VANETs ensure confidentiality by restricting access to sensitive information, utilizing encryption for protection from eavesdroppers, while balancing encryption with rapid message processing and dissemination.
Revocation	Revocation in VANETs involves withdrawing authentication credentials from malicious or malfunctioning vehicles, maintaining network integrity and trust. Effective mechanisms must be timely and minimize false positives.
Traceability	Traceability in VANETs enable identification of malicious vehicles while maintaining user privacy, requiring secure logs accessed under controlled circumstances, while adhering to legal standards and ethical considerations.
Data Freshness	Data freshness in VANETs ensures recent, relevant information, especially for dynamic, time-sensitive data. Techniques like timestamping and sequence numbers prevent replay attacks and network disruption.

significant node mobility and short connection periods, making typical security methods ineffective. Vehicular communication has unique security and privacy challenges, prompting a surge in study. The survey in [53] covers VANET advances, their communication architecture, and the crucial privacy and security challenges that must be addressed for their safe and effective use. It categorizes VANET cryptographic security issues. It consolidates, compares, and analyses VANET-specific cryptographic techniques. The study also evaluates these methods and discusses future cryptographic protocol research for intelligent transportation systems. However, Petit et al. [62] examines the delicate balance between security and privacy in cooperative vehicular networks, especially for safety-critical applications. Node and message authentication, as well as vehicle and driver privacy, are stressed. The survey emphasizes the increased focus on vehicular network pseudonym solutions to fulfill these twin objectives. It describes the particular challenges and requirements of pseudonym systems and presents an abstract pseudonym lifecycle model. The study analyses and categorizes contemporary pseudonym systems based on public key and identity-based encryption, group signatures, and symmetric authentication. It compares various techniques, updates standardization initiatives, and identifies research needs and issues in this subject.

The survey in [67] examines VANETs, which have great potential to improve academic and industrial driving. VANETs' open-access environment makes security and privacy difficult, which may limit their adoption. The study begins by explaining VANETs and categorizing their security concerns. It then lists the basic requirements for VANET security and privacy solutions. The study surveys and analyses authentication algorithms for secure processes. It also studies VANET privacy approaches, emphasizing the delicate balance between security and privacy. The conclusion discusses more effective methods for detecting and revoking malicious nodes and highlights the unresolved issues in this evolving field.

Boualouache et al. [21] discusses a crucial stage in VANET deployment and highlights current research problems, with a focus on location privacy. Recognizing academic and business consensus, the research examines the pseudonym-changing strategy, extensively used to protect VANET users' geographical privacy. The report critiques simple pseudonym modifications' vulnerability to pseudonym-linking attacks and ineffective defense. This leads to an evaluation of pseudonym-changing tactics. A successful VANET pseudonym-changing strategy remains unsolved despite these efforts. A complete assessment and classification of pseudonym-altering tactics is provided in the paper, along with important criteria. Additionally, it illuminates current research activities, open difficulties, and future research objectives.

Ali et al. [16] discusses the complex issues of security and privacy in VANETs, especially in ITS. It shows how VANETs'

decentralised design can jeopardise location privacy and secrecy, especially when trusted third parties (TTPs) are unavailable or corrupted. Reusing digital signatures or certificates across communications makes VANETs vulnerable to linking attacks. They noted that many VANET systems fail to balance security, location privacy, and efficiency. The protocol lets vehicles conceal their private certificates for communication outside mix-zones and create an anonymous shared key using zero-knowledge proof of knowledge. The protocol functions without Roadside Units or Certificate Authorities, allowing secure operation outside mixed-zones. An ideal/real simulation paradigm verifies protocol security, ensuring authentication, forward unlinkability, and accountability. Their performance analysis showed that the suggested protocol outperformed previous systems in computational and communication efficiency.

Modern cars have sensors for collision avoidance, automatic lane tracking, and semi-autonomous driving, which improve the driving experience and offer a variety of services to drivers and passengers. Despite these advances, VANET acceptance depends on resolving privacy, authentication, and secure message dissemination. Research has focused on these difficulties because of their importance. The research work in [51] discusses these fundamental VANET difficulties and reviews solutions offered over the previous decade to address them. The poll also indicates outstanding concerns, suggesting VANET research areas. In [60], [65], [59], [25], the authors investigate the feasibility of electric vehicle (EV) self-sovereign decentralised identity system implementation in great detail. Essential terminologies such as EVCC, SECC, OEM, and EVSE were defined by them. Public Key Infrastructure (PKI) was highlighted as crucial to automotive cybersecurity, with digital certificates playing a key role in facilitating safe communication between various parts of a vehicle. It resolves issues with communication and charging for electric vehicles caused by incompatibilities between two ISO standards (i.e., 15118-2 and 15118-20) [71]. They also detailed the cryptographic methods and X.509v3 certificate specifications that are required by ISO 15118-20. They also highlighted the need for strong security measures by shedding light on possible dangers to smart car GPS systems and Electronic Control Units. An extensive section is devoted to outlining a privacy-preserving architecture for electric vehicle charging and communication using Self-Sovereign Decentralised Identity (DID) and Verifiable Credentials [43]. Among these were the charging process workflow, the responsibilities of different parties involved, and the use of blockchain technology to provide a safe, decentralized identification system for electric vehicles. Finally, they proposed both software and hardware ways to secure cryptographic keys utilized in EVs, stressing the fundamental need of doing so. With an emphasis on cyber security, standardization, and blockchain applications, they provided a thorough review of the problems and possible solutions associated with implementing decentralized identification systems in the electric vehicle industry.

IV. Blockchain Technologies: Layer 1 & Layer 2

Blockchain technologies aim to revolutionize digital asset interaction through peer-to-peer decentralized networks. Layer 1 is the term that is used to describe the underlying main blockchain architecture, which includes the creation of blocks, consensus mechanism, and database partitioning, while Layer 2 is an overlaying network that lies on top of the underlying blockchain. It aims to improve scalability and reduce transaction costs significantly by aggregating transactions, processing in parallel, and handling transactions off-chain. These two layers work together to create a more effective, adaptable, and user-friendly digital platform [33].

Bitcoin and Ethereum networks are the most dominant ones for their distinct features and significant contributions to the blockchain System. Bitcoin is the foundational Layer 1 network, primarily intended for enabling direct transactions between peers using its native coin BTC. It uses a Proof-of-Work (PoW) consensus algorithm, with miners verifying transactions and ensuring network security. However, its simplicity and limited functionality make it a strong platform for digital currency. Ethereum, on the other hand, utilizes the Ethereum Virtual Machine (EVM) to facilitate smart contracts, expanding the range of possible blockchain applications beyond simple financial transactions. Ethereum's Layer 1 initially employed a PoW method but has now transitioned to Proof-of-Stake (PoS) to address scalability concerns and reduce its ecological impact.

Decentralised networks offer potential benefits, but scalability remains a barrier for many blockchain projects. Increased network congestion can lead to higher transaction costs and reduced throughput, negatively impacting the user experience. In particular, both Bitcoin and EVM-based Layer 1 networks face challenges in terms of scalability and high transaction costs. Bitcoin faces limitations due to its restricted transaction capacity and slow block times, while Ethereum's adaptability and smart contract functionalities have led to increased demand, worsening its scalability concerns. Both networks are exploring Layer 2 alternatives, such as the Lightning Network for Bitcoin and optimistic and ZK rollups for Ethereum, to improve transaction processing capabilities while maintaining security and decentralization [87].

A. Optimistic Rollups

The academic world and industries have already been exploring scaling solutions like Optimistic Rollups (ORs) and Zero Knowledge Rollups (ZK Rollups) to address these issues (e.g., [79], [43], [42], [27]). See Figure 1 for some of Layer 2s on top of Ethereum. ZK proofs transfer computationally demanding operations to Layer 2, easing the congestion on the mainchain and stabilizing network fees and number of transactions per second [27], [81]. Optimistic Rollups and ZK Rollups have already been implemented in blockchain networks to enhance scalability. These approaches involve conducting transactions off-chain, hence minimizing the need for on-chain data verification. Optimistic Rollups operate on fraud proofs, improving the computational complexity. ZK

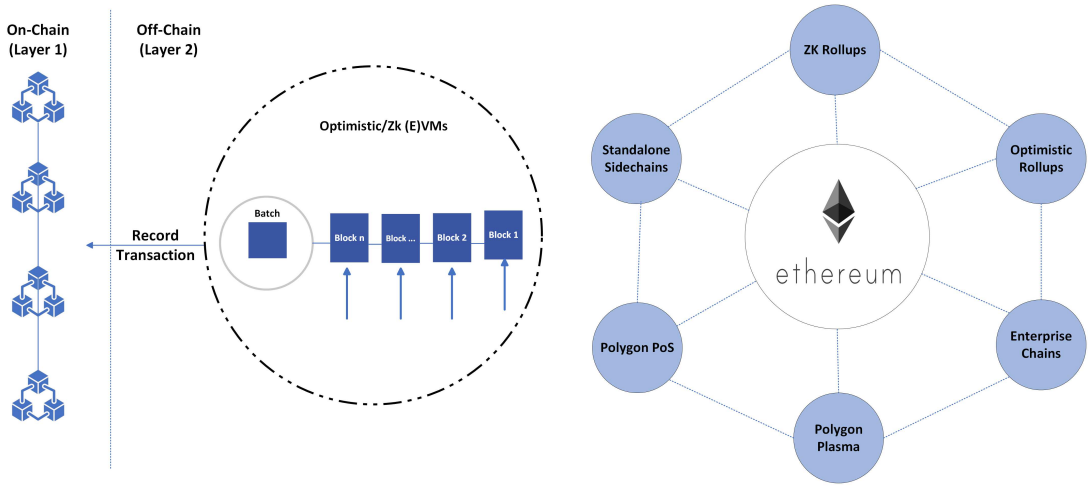

Fig. 1. The Layer 2 Ethereum-based Decentralized Ledger [4]

Rollups, on the other hand, employ cryptographic proofs to ensure the correctness of the given transactions, ensuring faster finalization while maintaining security measures. Both approaches have their benefits and compromises, with zkRollups providing a fully trustless architecture while optimistic rollups offer a more efficient solution (hence, cheaper tx costs) but rely on the assumption that transactions are correct until concerns are raised.

Optimism replicates the developer experience of the EVM, simplifying the process of constructing and implementing compatible rollup solutions. Furthermore, the protocol facilitates the utilisation of pre-existing Solidity smart contracts, integration with off-chain wallets, and user interfaces (UIs) [27].

Arbitrum fully supports the EVM, which ensures compatibility across all smart contract languages and the Ethereum mainchain. It includes a challenge period to guarantee the integrity of transactions. During this phase, network participants can challenge transactions if they suspect them to be fraudulent. Arbitrum does essential calculations to authenticate the legality of transactions, ensuring rapid processing while safeguarding the network against invalid or hostile operations. Arbitrum stands out due to its emphasis on enhancing the developer experience and ensuring compatibility with Ethereum's current tooling and smart contracts. Developers have the opportunity to implement their Ethereum applications on Arbitrum without making substantial changes, therefore taking advantage of enhanced scalability and efficiency, all while ensuring strong security assurances [27].

B. Zero Knowledge Rollups

ZK rollups aggregate multiple transactions off-chain and provide cryptographic proof of the validity of transactions without disclosing any specific transaction data. Subsequently, this verification, in conjunction with the transaction data, is made publicly available on the Layer 1 chain. zkRollups offers a significant benefit in that Layer 1 just needs to validate a single ZKP proof rather than each specific transaction. This procedure significantly reduces the computational workload required by Layer 1, enabling quicker transaction processing and higher throughput[79].

ZK proofs, such as zkSTARKs and zkSNARKs, are becoming increasingly popular in the blockchain world. These technologies facilitate the ability of one party to demonstrate to another party their knowledge of something without really disclosing the information itself. Both solutions are designed to enhance privacy and scalability by minimising the required information exchange between users. zkSNARKs stands for Zero Knowledge succinct non-interactive argument of knowledge. They lack interactivity, allowing the code to be deployed and operated alone. zkSNARKs rely on elliptic curves to ensure their security and necessitate a trustworthy setup. The dependence on a trusted set-up has raised concerns among critics, although developers only require its use in the beginning stages. Since there is no confidential data is used in the blockchain implementations, the community drops zk, and instead uses SNARKs and STARKs.

SNARKs have been embraced more rapidly than STARKs due to their early identification, extensive acceptance, and smaller size of proof [18], [44]. Conversely, STARKs offer certain benefits in terms of documentation and development assistance compared to STARKs. STARKs, in contrast to SNARKs, utilise hash functions, providing advantages such as resistance to quantum attacks and eliminating the need for a trusted setup. However, STARKs have bigger proof sizes, resulting in longer verification processes and requiring a greater amount of gas. Although the documentation for STARKs is not as detailed as that for SNARKs, the technical community has created a more comprehensive range of resources for individuals interested in implementing this state-of-the-art technology [18], [44].

StarkNet utilises STARKs to offer scalable and transparent anonymity on the blockchain. The decision to use STARKs instead of SNARKs is based on the former's superior scalability

and the absence of a trusted setup. This makes it an effective solution for building decentralised applications that demand robust security and privacy. Miden, Polygon ZkEVM, zkSync, and Scroll are projects that frequently employ SNARKs to improve the scalability and privacy of Ethereum such as zkSync [85], Polygon zkEVM [43], Scroll [57]. Taiko would select its ZK proof technology based on its particular objectives for scalability, privacy, and the necessity for a trusted setup. They usually choose between zkSTARKs and zkSNARKs based on their needs for privacy, scalability, and not needing a trusted setup [36], [32].

Several projects are leading the way in zkRollups to enhance scalability and efficiency in blockchain networks, particularly in Ethereum. Scroll enhances the overall efficiency and interoperability of the dApps with existing EVMs. By utilising ZK proofs, this system verifies transactions without revealing any details. This enhances efficiency and decreases expenses, all while upholding Ethereum's level of security. zkSync ensures cost-effective transactions and efficient processing, enabling Ethereum developers to smoothly transfer their existing dApps. Polygon is a zkRollup that is completely identical to the EVM, guaranteeing compatibility with all current Ethereum contracts and tools. StarkNet is a decentralised system based on zkRollup technology that focuses on facilitating scalable transactions while keeping costs at a minimum. Taiko aims to be user-friendly for developers while maintaining optimal performance and security [79].

V. Decentralisation of VANETs

A. Threshold Encryption

The utilization of threshold encryption has significantly altered the management of cryptographic keys. This is crucial in VANET. The idea behind this strategy is to divide a secret key into numerous pieces, each of which is in the possession of a different person. One important feature of this method is that, to reconstruct the original key, a threshold of shares must be met. For example, let's assume that each Participant i holds a public and private key share (pk, sk_i). Collectively, they yield a combined public and private key pair (pk, sk) that is generated from each of their separate keys in a threshold version (k, n) in which no single user is aware of the entire secret key sk. In this method, at least two of k users are required to decrypt the ciphertext. The confidentiality of participant information can be preserved by doing data analysis under encryption thanks to homomorphic encryption techniques like ElGamal or Paillier encryption [69], [54], [58], [72]. Hence, the security is increased by breaking the key into several pieces because the compromise of one piece does not compromise the system as a whole. In distributed network setups such as VANETs, where trust and security are critical, this approach greatly enhances these features. The following papers (refer to Table II) investigate several strategies and frameworks to improve security in VANETs through the utilisation of threshold encryption, and distributed trust management systems.

B. Threshold Signature Mechanism

A threshold signature mechanism allows transactions to appear on the Layer 1 or Layer 2 blockchain if a group of individuals collaboratively generates a signature without gaining any knowledge about the private key. In a (t, n)-threshold signature scheme, n participants own unique key shares, and any subset of t + 1 $< n$ distinct parties can provide a valid signature, whereas any subset of t or fewer parties cannot. The setup phase of the mechanism relies on the distributed key generation (DKG) protocol, in which the parties produce shares without revealing the key. Practically, the mechanism is frequently enhanced with a reshare protocol, also known as share rotation, to regularly update the shares while keeping the corresponding key unchanged. In a (t, n)-threshold mechanism, there are n parties, and the threshold $t < n$ represents the greatest number of parties that can be corrupted without compromising the security of the scheme. For more information about ECDSA performance and functionality, refer to [19]

In our threshold settings, we employ a trustless threshold ECDSA signature mechanism [35]. Throughout the Distributed Key Generation (DKG) process, all participants contribute to the randomness. However, to initiate a transaction on the Blockchain, a threshold of group members is expected to contribute to the approval of signature generation. Thus, the generation of a signed transaction is completed when a specific subset of participants collaborates in the signing process. This decreases transaction costs by only requiring a single collective signature compared to individual signatures from each member. It also offers a cost-effective, secure, and decentralised approach for validating transactions and reaching consensus among members.

C. Benefits and limitations

Threshold key management and homomorphic properties in VANETs have many obvious advantages, but their drawbacks need to be carefully considered. Enhanced network security is one of the main benefits. There is no such complete security breach because the system distributes cryptographic key sharing among several nodes. Even if one node is compromised, the entire key is secure. This strengthens the network's resistance to deliberate cyberattacks. Key management's decentralized structure has better fault tolerance. The system's overall integrity and functioning are preserved even if some nodes malfunction or are compromised. This is because the entire key may be rebuilt from the remaining shares. Furthermore, threshold cryptography works very well in VANET systems in terms of scalability and flexibility. The threshold values are adjusted to maintain a balance between security and performance as the network grows larger with the addition of more nodes. Additionally, the system is naturally resistant to some attacks, especially those that target a single crucial component, preventing the network as a whole from becoming inoperable due to a single point of failure.

Homomorphic encryption in VANETs enhances security and ensures data integrity and confidentiality during transmission.

TABLE II
A SUMMARY OF THRESHOLD HOMOMORPHIC ENCRYPTION SCHEMES FOR VANETS

Paper	Main Idea
WDC2023 [84]	Introduces a decentralised trust management framework for VANETs to mitigate the impact of malicious vehicles and compromised RSUs. The framework incorporates a process of beneficial oversight, encompassing trust assessment, decision-making, and a vehicle appeal system. The model's efficacy in detecting malicious vehicles is confirmed through comprehensive simulations, even in situations when RSUs are not reliable.
AHM2022 [11]	Presents a new approach that combines a blockchain-based incentive trust management model with a privacy-preserving threshold ring signature method for VANETs. The proposed solution aims to tackle several difficulties such as malicious assaults, privacy leakage, and lack of cooperation in traffic event validation. The system guarantees the authenticity of messages and the privacy of vehicles. It encourages participation by offering incentives. It also uses a consensus technique that can tolerate Byzantine faults, exhibiting both security and efficiency in VANET contexts.
ZSJ2021 [90]	Examines cryptographic primitives and presents two approaches for threshold key management, allowing stakeholders to collectively and safely retrieve secrets efficiently, especially in situations involving data sharing. This technique improves the security and functionality of blockchain in ITS.
TC2021 [14]	Introduces a security method that employs physical layer functions, such as encoders and decoders, along with shared keys, to build a model where communication between authorised parties is protected from unauthorised interception. The paper presents a method for creating threshold-secure codes using linear block codes, with a specific emphasis on Reed-Muller codes. It also showcases a very efficient implementation with quasi-linear time complexity, which can be adjusted to different key lengths.
HIC2019 [76]	Introduces a robust authentication and key management system for VANETs, employing edge computing and consortium blockchain to tackle challenges related to secure transmission and key management in diverse VANET contexts. The approach utilizes certificate-less authentication, employing individual session keys for cars and implementing efficient group key updating. Its security and efficiency have been demonstrated through rigorous security proofs and performance studies.
JSS2016 [40]	Addresses the task of determining the most effective threshold value for key reconstruction in threshold cryptography in cloud computing environments. The paper provides a framework for choosing this value, supported by experiments conducted with CloudSim to model the cloud environment and quantify the duration of key distribution and reconstruction procedures.

However, this requires complex computation that can increase latency in communication [80], [72]. There are also certain difficulties in putting VANET threshold key management into practice. Because of the continuous movement of cars, network architecture is dynamic, making it challenging to maintain consistent levels of privacy and trust. This makes managing trust and privacy more challenging, especially in light of the need for processing and decision-making in real-time. Additionally, the limited processing power in cars makes it difficult to implement sophisticated trust and privacy-preserving systems.

D. Decentralised Storage (DS)

Decentralized storage technologies like IPFS [3], Arweave [1], and Filecoin [2] are being used in VANETs to improve data availability, security, and scalability. IPFS is a peer-to-peer network that allows for the storage and sharing of data across multiple nodes, ensuring redundancy, high availability, and expedited access. Arweave, on the other hand, uses blockchain technology to store data in perpetuity with a single payment, making it an ideal solution for archival purposes. Filecoin aims to transform cloud storage into an algorithmic marketplace using a native token for storage space buying and selling [73].

They also provide more efficient and cost-effective data storage and access solutions compared to conventional centralized cloud storage services. For scenarios requiring prolonged data retention, systems like Arweave are essential, ensuring data accessibility for future analysis. This integration represents a step towards resolving VANETs' intrinsic challenges and redefining data management paradigms [70]. Moreover, decentralized systems like IPFS, Arweave, and Filecoin introduce robust security measures, including encryption and hash-based addressing. These measures are instrumental in safeguarding sensitive data transmitted across VANETs, thereby bolstering the privacy and integrity of V2V and V2I communications.

E. Enhancing Robustness and Privacy-Preserving Data Sharing with DLT

By redefining the dynamics of VANET connections, this method aims to provide a network infrastructure that is more transparent, efficient, and safe. [78], [41]. DLTs are considered a huge step forward regarding digital exchanges and data management [56], [86], [24], [43], [52]. Compared to standard centralized systems, systemic failures are less likely to happen in DTL networks. This makes data secure and provides a more stable way to handle it. In a blockchain system, transactions are recorded and managed in a more open and trustworthy way [10]. The blockchain system can be used in so many different ways, showing how its focus on security, openness, and decentralization could make big changes in many areas.

1) Role in enhancing VANET security: VANETs have vulnerabilities such as risks to data integrity, privacy violations, and vulnerability to different cyber-attacks. This is why security is considered of utmost importance in VANETs.

In several research works, the nature of DLT can improve the security of VANETs. The resilience and security of VANETs can be enhanced by the integration of blockchain technology because of certain features such as decentralised structure and cryptographic security measures [37], [26], [89]. Blockchain technology makes sure that the information sent

between vehicles is authentic and has integrity, and the blockchain provides a reliable way to check the accuracy of data, lowering the risks of data manipulation and cyberattacks [38].

2) Advantages over traditional methods: DLT removes single points of failure, makes data more accurate and reliable, and provides a safe and open space for exchanges. The advantages of DLT over traditional data management methods in VANETs are shown in Table III. These studies focus on the advantages of DLT, such as better security, more accurate data, decentralised management, and quick approval of data.

VI. Our New Model: A Robust Trustless and Privacy-Preserving Framework for VANETs

The suggested framework systematically addresses the intricate challenges of trust, privacy, and scalability inherent in VANETs. Building upon the foundational architecture depicted in Figures 2, our approach leverages the robust capabilities of DLT, with a particular focus on Ethereum and its Layer 2 scaling solutions such as Optimism [24], Arbitrum [42], zkSync [91], and Polygon ZKEVM [43]). These technologies have been carefully selected and integrated to forge a formidable framework that ensures secure, effective, and scalable communication within VANETs. The framework is divided into various layers (the physical layer, the P2P network layer, and the DLT layer).

For data security and authentication, the architecture has a decentralised ledger layer built on EVM. Multi-party Threshold Signatures are what make this layer stand out. They make sure that transactions are only approved and recorded when a certain number of parties agree. Adding threshold Homomorphic encryption also lets the system analyse encrypted data while keeping personal data safe. A P2P network layer makes the design even better by making the network much more reliable and making data easier to reach. This layer is very important because it lets multiple nodes share files, alarms, and error reports instantly and without any problems. The Base Layer, which is also called the Physical Network layer, is the most important part of this design. It is made up of servers and RSUs. These parts are the network's basis; they keep the structure strong and the operations stable.

A. The Physical Layer of the Architecture

Figure 2 illustrates our system model. RSUs enable V2I and V2V communication between vehicles. They can share messages with other vehicles and RSUs through the On-Board Unit (OBU). RSUs also link to the internet, allowing servers to handle and manage data. RSUs and central servers must communicate to coordinate and distribute traffic management data, safety warnings, and other crucial messages across the network. By providing hardware and communication infrastructure, the base layer supports the P2P network layer.

B. The P2P Network Layer of the Architecture

The P2P Network Layer's interconnected nodes demonstrate a mesh network topology. This arrangement allows direct contact between any two network nodes, improving resilience and data redundancy. Node failures and network topology changes require dynamic routing and reconfiguration, which the mesh-like structure provides.

Procedure 1 outlines the steps for setting up the P2P Network Layer in a VANET environment. This includes creating mesh connectivity.

Procedure 1: P2P Network Layer Operation

- **Step 1:** Initialize the VANET P2P Network Layer.
- **Step 2:** Connect OBUs and RSUs to the mesh.
- **Step 3:** Identify and establish connections with nearby OBUs.
- **Step 4:** Integrate network protocols.
- **Step 5:** Generate network-related data.
- **Step 6:** Ensure continuous data propagation.
- **Step 7:** End any process upon completion or condition.

C. The DLT Layer of the Architecture

Figure 2 illustrates an EVM-based Decentralised Ledger Layer in a VANET that ensures secure, transparent, and decentralized data transfers. In this architecture, we employ a multi-party computation (MPC) network where threshold signatures and threshold homomorphic encryption enable secure and private network data operations [90], [77], [86]. By integrating data collection from the physical layer to a DLT layer, this model establishes a network in which decentralized storage networks such as IPFS and Arweave, along with Layer 2 networks, connect each node to the others. Additionally, the mesh connects MPC nodes, which improves the resilience of the network and facilitates the dissemination of data.

Smart contracts that have been pre-established are implemented on the Layer 2 network during the establishment phase, thereby enabling the transparency of network operations. The information obtained from the mesh undergoes processing, including analysis, cleaning, and packaging, prior to being transmitted to DS (Decentralized Storage) system. For increased security, only the fingerprint of the published data (transaction identifier or content identifier) is transmitted to Layer 2; the original data remains within the DS system. By capitalizing on the benefits of decentralized storage and blockchain technology, this architecture guarantees the confidentiality and integrity of data, thus offering an all-encompassing resolution to the privacy and security obstacles encountered in VANETs. Multiple signers validate transactions through multi-party threshold signature schemes, and at least k out of n signatories must agree and sign the transactions to create valid transactions. This approach reduces potential fraud and minimizes the single point of failure by distributing transaction authorization power across multiple entities. Furthermore, the underlying threshold homomorphic encryption scheme uses key pairs to allow at least k people to decrypt a ciphertext in a (ℓ, m) threshold manner.

Before presenting the DLT protocols, a setup protocol needs to be executed to create necessary cryptographic keys for data sharing and analysis.

Procedure 2: Key generation

TABLE III
A COMPARISON OF DLT AND TRADITIONAL DATA MANAGEMENT IN VANETS

Paper	Main Idea
FDC2022 [31]	This study investigates the incorporation of blockchain technology into digital twins in VANETs to improve intelligent transport in smart cities. The aim is to utilise blockchain for the safe transmission and storage of data. The simulation findings demonstrate that the created model guarantees robust network security and achieves low latency performance. This provides a solid experimental foundation for the advancement of intelligent and secure transportation in smart cities.
PNC2022 [61]	Introduces a certificate management system for VANETs that utilizes blockchain technology. The goal of this method is to fix problems with renewing certificates and taking away vehicles. It makes privacy better by using pseudonym certificates and ring signatures for a voting-based annulment system. It aims to cut down on wait times in centralised management and improve the safety and efficiency of smart transport networks as a whole.
SRI2022 [75]	Using blockchain technology, it shows a way to encrypt messages and handle data for VANETs. This aims to lower cyber risks by ensuring privacy, being impossible to deny, and being strong against attacks like 51% attacks, eclipse attacks, and double-spending. The TB-SCDM system for authentication and authorization in VANETs is better than the current ways because it uses less storage space and computing power.
LPT2021 [47]	Shows how to use blockchain technology to control sharing of information in VANETs. A hybrid trust model is used to figure out how reliable shared material is, which is meant to ease security concerns. The system uses the PBFT consensus protocol, which checks to see how many times RSUs and cars are interacting to make sure they are exchanging information honestly and actively. There have been experiments done to show that these methods can be used in real life.
ZWP2020 [88]	Gives a way to make sure that sending and receiving data is safe in VANETs, focusing on responsibility, privacy protection, and transmission privacy. The plan sets up the Fengyi system and adds a Trusted Ledger Model (TLM). The study shows that the TLM is a good way to make sure that VANETs can share data securely.
DJW2020 [30]	The study used a hierarchical network that uses 5G and blockchain technologies to discuss how hard it is to keep data secure in VANETs. They used the PBFT algorithm to create a system for sharing data that emphasizes secure and quick data storage and transfer. To do this, they use the properties of data immutability and decentralisation.

- **Step 1:** Execute threshold multi-signature protocol between MPC nodes.
  - At the end of this protocol, each node will receive a private key share for later signing the transactions in a threshold manner.
  - The public key will be embedded into the smart contract.
- **Step 2:** Execute threshold encryption protocol between MPC nodes.
  - At the end of this protocol, each node will receive a private key share for later decrypting and analysing data in a threshold manner.
  - The public encryption key will be shared with the P2P layer, including RSUs and OBUs.

Procedure 3 outlines the steps for creating and controlling a DLT protocol in a VANET (see Figure 2). In our framework, we utilize Ethereum as an example to securely distribute keys, verify transactions, and allow for direct computation on encrypted data. This ensures the reliability and accessibility of the blockchain ledger.

Procedure 3: DLT Protocol

- **Step 1:** Deploy smart contracts to an Ethereum-based Layer 2 ledger for the VANET architecture (e.g., Arbitrum, Optimism, zkSync, Scroll).
- **Step 2:** Import public keys of MPC networks.
- **Step 3:** Generate and distribute encrypted data to OBUs. Note that the data generated by OBUs are already anonymized and the correctness can be proven through ZKSNARKs.
- **Step 4:** Sync and share encrypted data within OBUs, Roadside Units (RSUs), and Servers.
- **Step 5:** Synced data is sent to MPC network.
  - **Step 5.1:** The generated data will be analyzed. For example, some MPC applications allow to be analyzed before the decryption process.
  - **Step 5.2:** If required for further analysis, it may first be decrypted in a threshold manner.
  - **Step 5.3:** The final data will be cleaned and packed.
- **Step 6:** Once the packed data is ready, it will be published to a decentralized storage (DS) which will create a unique content identifier (CID) written in a transaction (possibly with transaction ID).
- **Step 7:** Steps 3 to 6 can be executed multiple times for different data. If the number of packed data is large enough (e.g., 4096 packed data), all CIDs are also published to DS and a Merkle root of the CID set is computed. Finally, the root CID will be published on the chain (through a transaction) along with the necessary information.
  - **Step 7.1:** In order to create a tx on the chain, the threshold number of MPC nodes is needed to validate the transaction and participate in the transaction signing ceremony.
  - **Step 7.2:** Once every participant has done their checks and partial contributions for the signing, the final signature along with the original transaction is submitted to the Blockchain.
  - **Step 7.3:** The contracts on the Blockchain do the final check on the message and store them in a transparent

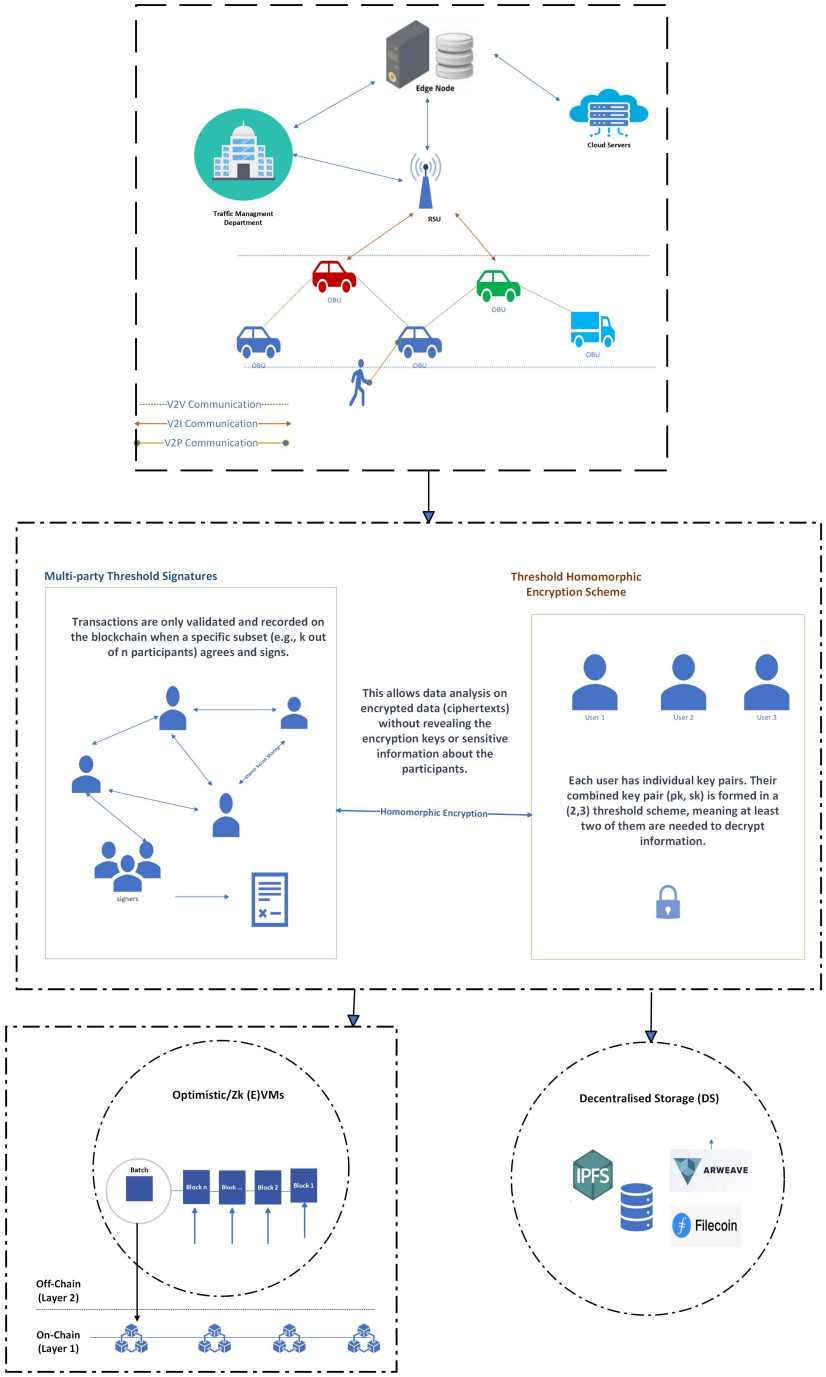

Fig. 2. Our Proposed Architecture: The System Model

way.

As said earlier, the framework employs Layer 2 DLT which is more cost-effective and faster than Layer 1 as the integration of Layer 1 using VANET would significantly lack the scalability and require significant costs.

VII. Further Security and Privacy Insights

A. Resilience Against Single-Point Failures

The proposed decentralised VANET framework is resilient to single-point failures compared to traditional centralised ones. This is crucial for vehicle networks, as uninterrupted functioning is essential for optimal efficiency and safety. A single server or node failure in a centralised system can result in a complete system shutdown. However, our decentralised

architecture guarantees that the network will remain operationally sound even if many nodes fail. This is accomplished via distributed ledger technology, enabling vehicles to communicate information seamlessly and autonomously without requiring a central coordinating node. This setup ensures a strong and reliable communication system for vehicles, greatly decreasing the chances of network failure and improving the overall dependability of vehicle communications.

The architecture is designed to adapt and reorganise itself based on network changes, such as adding or losing nodes. This self-repairing feature guarantees that data routing is consistently optimised, ensuring constant connection even in challenging circumstances. The system can rapidly compensate for lost nodes by utilising suitable algorithms for network routing and data redundancy, enhancing its resilience. This decentralised and self-adaptive method improves the system's resilience and scalability, making it suitable for the growing network of connected vehicles.

B. Enhanced Privacy through PETs

Our suggested framework allows data processing while maintaining privacy through the use of PETs. PETs enable computations to be carried out on encrypted data, producing an encrypted output that, upon decryption, corresponds to the results of operations conducted on the original plaintext. For example, threshold homomorphic encryption guarantees that only authorised entities can get decrypt the ciphertexts, preventing unauthorised access and data breaches.

Implementing and integrating advanced cryptographic techniques like zero-knowledge proofs and secure multi-party computing improves the privacy and security of VANETs by allowing verification of data integrity and authenticity without disclosing the actual data. This is crucial in situations where disclosing sensitive data (such as location or driver behaviour trends) could put user privacy or security at risk. The cryptographic primitives in our suggested framework meet current security needs and are designed to handle future threats and problems in the evolving field of vehicular communications. Our framework establishes a new benchmark for privacy and security in VANETs by implementing advanced security techniques to secure sensitive data from complex cyber threats.

VIII. Challenges and Future Directions

The following directions will help to create more sophisticated, safe, and effective vehicle communication systems by addressing the changing opportunities and problems in the field of VANETs:

- **Integration with AI:** The integration of the proposed VANET architecture with artificial intelligence could be investigated in subsequent studies. Incorporating artificial intelligence could improve decision-making processes and traffic management.
- **Quantum-resistant security solutions:** Recent developments in quantum computing have the potential to pose a threat to the conventional cryptographic algorithms and protocols which require computational assumptions such as discrete logarithm and factorization problems. To ensure the long-term security of VANETs, future efforts should concentrate on the development and integration of post-quantum cryptographic algorithms [13].
- **Scalability and efficiency improvements:** Especially in high-density urban contexts with a large number of vehicles and gadgets, it is important to investigate strategies to improve the scalability and efficiency of the suggested architecture. For this purpose, it may be necessary to optimize the procedures of key management and the decentralized ledger to execute activities more quickly and effectively.
- **Incentivization:** The proposed DLT-based framework could be significantly improved by incorporating an incentivization mechanism that encourages OBUs to share data. This approach is likely to result in a substantial increase in data volume, thereby ensuring the generation of accurate and reliable statistical information.
- **Real-World Implementation and Testing:** It is possible to gain useful insights into the actual challenges and performance of the proposed VANET architecture by conducting implementation studies and pilots in the real world. Taking into account data from the real world and comments from users, would help develop the model.

IX. Conclusion

This paper has presented a new architectural framework that combines threshold key management, PETs, and DLTs to greatly improve the security and privacy of VANETs. Our suggested architecture utilizes decentralized systems, which give robustness and resilience using DLTs. By using cryptographic methods like multi-party threshold key management and homomorphic encryption, this change protects data from a wide range of cybersecurity threats and makes sure that it is always available and correct. The suggested framework enhances both key management and trust distribution while also strengthening data privacy. The incorporation of these technologies into VANETs has exhibited a significant improvement in V2X communication, guaranteeing both effectiveness and confidentiality in data processing and transfer.

Declarations

Ethics approval and consent to participate

Not applicable

Consent for publication

Not applicable

Funding

Not applicable

Acknowledgements

Not applicable

REFERENCES

[1] "Arweave," https://www.arweave.org/, accessed: February 29, 2024.

[2] "Filecoin," https://filecoin.io/, accessed: February 29, 2024.

[3] "InterPlanetary File System (IPFS)," https://ipfs.tech/, accessed: February 29, 2024.

[4] "What is layer 2 scaling solutions & why it is required," 2024, accessed: February 29, 2024. [Online]. Available: https://medium.com/crypto-wisdom/what-is-layer-2-scaling-solutions-why-it-is-required-66b8dbf3bc9c

[5] M. Abspoel, R. Cramer, I. Damgård, D. Escudero, and C. Yuan, "Efficient information-theoretic secure multiparty computation over via galois rings," in *Theory of Cryptography Conference*. Springer, 2019, pp. 471–501.

[6] H. Y. Adarbah and S. Ahmad, "Channel-adaptive probabilistic broadcast in route discovery mechanism of manets," *Journal of Communications Software and Systems*, vol. 15, no. 1, pp. 34–43, 2019.

[7] H. Y. Adarbah, S. Ahmad, and A. Duffy, "Impact of noise and interference on probabilistic broadcast schemes in mobile ad-hoc networks," *Computer Networks*, vol. 88, pp. 178–186, 2015.

[8] H. Y. Adarbah, M. F. Moghadam, R. L. R. Maata, A. Mohajerzadeh, and A. H. Al-Badi, "Security challenges of selective forwarding attack and design a secure ecdh-based authentication protocol to improve rpl security," *IEEE Access*, vol. 11, pp. 11 268–11 280, 2022.

[9] H. Y. Adarbah, M. Sookhak, and M. Atiquzzaman, "A digital twin environment for 5g vehicle-to-everything: Architecture and open issues," in *Proceedings of the Int'l ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks*, 2023, pp. 115–122.

[10] S. Aggarwal and N. Kumar, "Basics of blockchain," in *Advances in computers*. Elsevier, 2021, vol. 121, pp. 129–146.

[11] W. Ahmed, W. Di, and D. Mukathe, "A blockchain-enabled incentive trust management with threshold ring signature scheme for traffic event validation in vanets," *Sensors*, vol. 22, no. 17, p. 6715, 2022.

[12] M. S. Al-Marshoud, A. H. Al-Bayatti, and M. S. Kiraz, "Improved Chaff-Based CMIX for Solving Location Privacy Issues in VANETs," *Electronics*, vol. 10, no. 11, p. 1302, 2021.

[13] G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, C. Miller, D. Moody, R. Peralta *et al.*, "Status report on the third round of the nist post-quantum cryptography standardization process," *US Department of Commerce, NIST*, 2022.

[14] N. Aldaghri and H. Mahdavifar, "Threshold-secure coding with shared key," *IEEE Journal on Selected Areas in Information Theory*, vol. 2, no. 1, pp. 95–105, 2021.

[15] I. Ali, A. Hassan, and F. Li, "Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey," *Vehicular Communications*, vol. 16, pp. 45–61, 2019.

[16] M. S. AlMarshoud, A. H. Al-Bayatti, and M. S. Kiraz, "Location privacy in VANETs: Provably secure anonymous key exchange protocol based on self-blindable signatures," *Vehicular Communications*, vol. 36, p. 100490, 2022.

[17] G. Asharov, A. Jain, A. López-Alt, E. Tromer, V. Vaikuntanathan, and D. Wichs, "Multiparty computation with low communication, computation and interaction via threshold fhe," in *Advances in Cryptology–EUROCRYPT 2012: 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings 31*. Springer, 2012, pp. 483–501.

[18] M. Asher, "Zero-knowledge proofs: Starks vs snarks," *ConsenSys Blog*, May 2021, accessed: February 29, 2024. [Online]. Available: https://consensys.io/blog/zero-knowledge-proofs-starks-vs-snarks

[19] J.-P. Aumasson, A. Hamelink, and O. Shlomovits, "A survey of ecdsa threshold signing," *Cryptology ePrint Archive*, 2020.

[20] D. Boneh, R. Gennaro, S. Goldfeder, A. Jain, S. Kim, P. M. Rasmussen, and A. Sahai, "Threshold cryptosystems from threshold fully homomorphic encryption," in *Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part I 38*. Springer, 2018, pp. 565–596.

[21] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A Survey on Pseudonym Changing Strategies for Vehicular Ad-Hoc Networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 770–790, 2017.

[22] R. Canetti, R. Gennaro, S. Goldfeder, N. Makriyannis, and U. Peled, "Uc non-interactive, proactive, threshold ecdsa with identifiable aborts," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 2020, pp. 1769–1787.

[23] D. Catalano, R. Cramer, G. Di Crescenzo, I. Darmgård, D. Pointcheval, T. Takagi, R. Cramer, and I. Damgård, "Multiparty computation, an introduction," *Contemporary cryptology*, pp. 41–87, 2005.

[24] B. K. Chaurasia and S. Verma, "Optimizing pseudonym updation for anonymity in VANETS," in *2008 IEEE Asia-Pacific Services Computing Conference*. IEEE, 2008, pp. 1633–1637.

[25] B. Chen, Z. Wang, T. Xiang, J. Yang, D. He, and K.-K. R. Choo, "Bcgs: Blockchain-assisted privacy-preserving cross-domain authentication for vanets," *Vehicular Communications*, vol. 41, p. 100602, 2023.

[26] X. Chen, Y. Chen, X. Wang, X. Zhu, and K. Fang, "Dsvn: A flexible and secure data-sharing model for vanet based on blockchain," *Applied Sciences*, vol. 13, no. 1, p. 217, 2022.

[27] Cryptopedia Staff, "Layer-2 scaling: zk-rollups and optimistic rollups," https://www.gemini.com/tr-TR/cryptopedia/layer-2-scaling-zk-rollup-optimistic-rollup-ethereum, 2023, accessed: February 29, 2024.

[28] I. Damgard, M. Geisler, and M. Kroigard, "Homomorphic encryption and secure comparison," *International Journal of Applied Cryptography*, vol. 1, no. 1, pp. 22–31, 2008.

[29] I. Damgård and J. B. Nielsen, "Universally composable efficient multiparty computation from threshold homomorphic encryption," in *Annual international cryptology conference*. Springer, 2003, pp. 247–264.

[30] X. Du, X. Jiang, H. Wu, J. Fang, G. Wang, and C. Du, "Data sharing strategy based on pbft algorithm in vanets," in *Proceedings of the 2020 International Conference on Aviation Safety and Information Technology*, 2020, pp. 583–586.

[31] H. Feng, D. Chen, and Z. Lv, "Blockchain in digital twins-based vehicle management in vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 10, pp. 19 613–19 623, 2022.

[32] G. Fuchsbauer, "Subversion-zero-knowledge snarks," in *Public-Key Cryptography–PKC 2018: 21st IACR International Conference on Practice and Theory of Public-Key Cryptography, Rio de Janeiro, Brazil, March 25-29, 2018, Proceedings, Part I 21*. Springer, 2018, pp. 315–347.

[33] A. Gangwal, H. R. Gangavalli, and A. Thirupathi, "A survey of layer-two blockchain protocols," *Journal of Network and Computer Applications*, vol. 209, p. 103539, 2023.

[34] T. Gazdar, O. Alboqomi, and A. Munshi, "A decentralized blockchain-based trust management framework for vehicular ad hoc networks," *Smart Cities*, vol. 5, no. 1, pp. 348–363, 2022.

[35] R. Gennaro and S. Goldfeder, "Fast multiparty threshold ecdsa with fast trustless setup," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018, pp. 1179–1194.

[36] Y. Gong, Y. Jin, Y. Li, Z. Liu, and Z. Zhu, "Analysis and comparison of the main zero-knowledge proof scheme," in *2022 International Conference on Big Data, Information and Computer Network (BDICN)*. IEEE, 2022, pp. 366–372.

[37] B. Hou, Y. Xin, H. Zhu, Y. Yang, and J. Yang, "Vanet secure reputation evaluation & management model based on double layer blockchain," *Applied Sciences*, vol. 13, no. 9, p. 5733, 2023.

[38] J. Hu, Y. Yang, J. Wu, and C. Long, "A blockchain-based cross-domain data sharing scheme for vanets," in *The 2022 4th International Conference on Blockchain Technology*, 2022, pp. 117–125.

[39] R. Hussain, J. Lee, and S. Zeadally, "Trust in vanet: A survey of current solutions and future research opportunities," *IEEE transactions on intelligent transportation systems*, vol. 22, no. 5, pp. 2553–2571, 2020.

[40] W. Janratchakool, S. Boonkrong, and S. Smanchat, "Finding the optimal value for threshold cryptography on cloud computing," *International Journal of Electrical and Computer Engineering*, vol. 6, no. 6, p. 2979, 2016.

[41] M. Jiang and X. Qin, "Distributed ledger technologies in vehicular mobile edge computing: a survey," *Complex & Intelligent Systems*, vol. 8, no. 5, pp. 4403–4419, 2022.

[42] H. Kalodner, S. Goldfeder, X. Chen, S. M. Weinberg, and E. W. Felten, "Arbitrum: Scalable, private smart contracts," in *27th USENIX Security Symposium (USENIX Security 18)*, 2018, pp. 1353–1370.

[43] J. Kanani, S. Nailwal, and A. Arjun, "Polygon whitepaper," https://whitepaper.io/document/646/polygon-whitepaper, 2021, accessed: February 29, 2024.

[44] K. Kim. (2023) Throne of zk: Snark vs. stark. Accessed: February 29, 2024. [Online]. Available: https://medium.com/nonce-classic/throne-of-zk-snark-vs-stark-e449984d5c36

[45] M. Y. Kubilay, M. S. Kiraz, and H. A. Mantar, "Certledger: A new pki model with certificate transparency based on blockchain," *Computers & Security*, vol. 85, pp. 333–352, 2019.

[46] K. Lim, K. M. Tuladhar, X. Wang, and W. Liu, "A scalable and secure key distribution scheme for group signature based authentication in VANET," in *2017 IEEE 8th annual ubiquitous computing, electronics and mobile communication conference (UEMCON)*. New York, NY, USA: IEEE, 2017, pp. 478–483.

[47] F. Lin, Y. Peng, T. Cui, X. Huang, and Q. Chen, "Blockchain based content sharing management in vanets," in *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*. IEEE, 2021, pp. 1–5.

[48] Y. Lindell, "Secure multiparty computation (mpc)," *Cryptology ePrint Archive*, 2020.

[49] R. Longo, A. Meneghetti, and M. Sala, "Threshold multi-signature with an offline recovery party," *Cryptology ePrint Archive*, 2020.

[50] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 2, pp. 760–776, 2018.

[51] D. Manivannan, S. S. Moni, and S. Zeadally, "Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs)," *Vehicular Communications*, vol. 25, p. 100247, 2020.

[52] Matter Labs, "Introduction to zksync for developers," https://docs.zksync.io/dev, 2022, accessed: February 29, 2024.

[53] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Vehicular Communications*, vol. 1, no. 2, pp. 53–66, 2014.

[54] S. J. Mohammed and D. B. Taha, "Performance evaluation of rsa, elgamal, and paillier partial homomorphic encryption algorithms," in *2022 International Conference on Computer Science and Software Engineering (CSASE)*. IEEE, 2022, pp. 89–94.

[55] P. Mundhe, S. Verma, and S. Venkatesan, "A comprehensive survey on authentication and privacy-preserving schemes in VANETs," *Computer Science Review*, vol. 41, p. 100411, 2021.

[56] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, vol. n/a, p. 21260, 2008.

[57] G. A. Oliva, A. E. Hassan, and Z. M. Jiang, "An exploratory study of smart contracts in the ethereum blockchain platform," *Empirical Software Engineering*, vol. 25, pp. 1864–1904, 2020.

[58] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *International conference on the theory and applications of cryptographic techniques*. Springer, 1999, pp. 223–238.

[59] R. P. Parameswarath, P. Gope, and B. Sikdar, "User-empowered privacy-preserving authentication protocol for electric vehicle charging based on decentralized identity and verifiable credential," *ACM Transactions on Management Information Systems (TMIS)*, vol. 13, no. 4, pp. 1–21, 2022.

[60] ——, "A privacy-preserving authenticated key exchange protocol for v2g communications using ssi," *IEEE Transactions on Vehicular Technology*, 2023.

[61] M. N. S. Perera, T. Nakamura, M. Hashimoto, H. Yokoyama, C.-M. Cheng, and K. Sakurai, "Certificate management scheme for vanets using blockchain structure," *Cryptography*, vol. 6, no. 2, p. 20, 2022.

[62] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym Schemes in Vehicular Networks: A survey," *IEEE communications Surveys & Tutorials*, vol. 17, no. 1, pp. 228–255, 2014.

[63] A. Pfitzmann and M. Hansen, "A Terminology for Talking about Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management," 2010.

[64] A. Pfitzmann and M. Köhntopp, "Anonymity, Unobservability, and Pseudonymity — A Proposal for Terminology," in *Designing privacy enhancing technologies*, H. Federrath, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 1–9.

[65] R. Poolat Parameswarath, P. Gope, and B. Sikdar, "Decentralized identifier-based privacy-preserving authenticated key exchange protocol for electric vehicle charging in smart grid," *arXiv e-prints*, pp. arXiv–2206, 2022.

[66] D. Praveena Anjelin and S. Ganesh Kumar, "Blockchain technology for data sharing in decentralized storage system," in *Intelligent Computing and Applications: Proceedings of ICICA 2019*. Springer, 2021, pp. 369–382.

[67] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985–2996, 2015.

[68] P. Rindal and M. Rosulek, "Malicious-secure private set intersection via dual execution," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 1229–1242.

[69] N. Ruan, T. Nishide, and Y. Hori, "Threshold elgamal-based key management scheme for distributed rsus in vanet," in *2011 International Conference on Selected Topics in Mobile and Wireless Networking (iCOST)*. IEEE, 2011, pp. 133–138.

[70] N. Sangeeta and S. Y. Nam, "Blockchain and interplanetary file system (ipfs)-based data storage system for vehicular networks with keyword search capability," *Electronics*, vol. 12, no. 7, p. 1545, 2023.

[71] J. Schmutzler, C. Wietfeld, and C. A. Andersen, "Distributed energy resource management for electric vehicles using iec 61850 and iso/iec 15118," in *2012 IEEE Vehicle Power and Propulsion Conference*. IEEE, 2012, pp. 1457–1462.

[72] B. Schoenmakers, "Threshold homomorphic cryptosystems," in *Encyclopedia of Cryptography and Security (2nd ed.)*. Springer, 2011, pp. 1293–1294.

[73] V. Shah, V. Thakkar, and A. Khang, "Electronic health records security and privacy enhancement using blockchain technology," in *Data-Centric AI Solutions and Emerging Technologies in the Healthcare Ecosystem*. CRC Press, 2023, pp. 1–13.

[74] M. A. Simplicio, E. L. Cominetti, H. K. Patil, J. E. Ricardini, L. T. Ferraz, and M. V. M. Silva, "Privacy-preserving certificate linkage/revocation in VANETs without linkage authorities," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3326–3336, 2020.

[75] J. Su, R. Ren, Y. Li, R. Y. Lau, and Y. Shi, "Trusted blockchain-based signcryption protocol and data management for authentication and authorization in vanets," *Wireless Communications and Mobile Computing*, vol. 2022, 2022.

[76] H. Tan and I. Chung, "Secure authentication and key management with blockchain in vanets," *IEEE access*, vol. 8, pp. 2482–2498, 2019.

[77] H. Tan, S. Xuan, and I. Chung, "HCDA: Efficient Pairing-Free Homographic Key Management for Dynamic Cross-Domain Authentication in VANETs," *Symmetry*, vol. 12, no. 6, p. 1003, 2020.

[78] A. Tesei, D. Lattuca, M. Luise, P. Pagano, J. Ferreira, and P. C. Bartolomeu, "A transparent distributed ledger-based certificate revocation scheme for vanets," *Journal of Network and Computer Applications*, vol. 212, p. 103569, 2023.

[79] L. T. Thibault, T. Sarry, and A. S. Hafid, "Blockchain scaling using rollups: A comprehensive survey," *IEEE Access*, 2022.

[80] R. Verma, "An efficient secure vanet communication using multi authenticate homomorphic signature algorithm," in *2023 International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*. IEEE, 2023, pp. 1–5.

[81] M. Vilá Brualla, "Blockchain layer 2 scalability solutions: a framework for comparison," Master's thesis, Universitat Politècnica de Catalunya, 2023.

[82] C. Wang, J. Shen, J.-F. Lai, and J. Liu, "B-TSCA: blockchain assisted trustworthiness scalable computation for V2I authentication in VANETs," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 3, pp. 1386–1396, 2021.

[83] J. Wang, Y. Sun, and C. Phillips, "Enhanced pseudonym changing in vanets: How privacy is impacted using factitious beacons," in *2023 Wireless Telecommunications Symposium (WTS)*. IEEE, 2023, pp. 1–6.

[84] Y. Wang, Y. Song, Y. Cao, L. Zhang, X. Ren *et al.*, "Appeal-based distributed trust management model in vanets concerning untrustworthy rsus," in *2023 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2023, pp. 1–6.

[85] M. Westerkamp and J. Eberhardt, "zkrelay: Facilitating sidechains using zksnark-based chain-relays," in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2020, pp. 378–386.

[86] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[87] Z. Xu and L. Chen, "L2chain: Towards high-performance, confidential and secure layer-2 blockchain solution for decentralized applications," *Proceedings of the VLDB Endowment*, vol. 16, no. 4, pp. 986–999, 2022.

[88] C. Zeng, Y. Wang, F. Liang, and X. Peng, "Fengyi: trusted data sharing in vanets with blockchain," in *2020 IEEE 25th Pacific Rim International Symposium on Dependable Computing (PRDC)*. IEEE, 2020, pp. 11–20.

[89] X. Zhang, J. Lai, and A. J. Moshayedi, "Traffic data security sharing scheme based on blockchain and traceable ring signature for vanets," *Peer-to-Peer Networking and Applications*, vol. 16, no. 5, pp. 2349–2366, 2023.
[90] T. Zhou, J. Shen, Y. Ren, and S. Ji, "Threshold key management scheme for blockchain-based intelligent transportation systems," *Security and Communication Networks*, vol. 2021, pp. 1–8, 2021.
[91] S. Zhu, Z. Cai, H. Hu, Y. Li, and W. Li, "zkcrowd: a hybrid blockchain-based crowdsourcing platform," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4196–4205, 2019.