2

Related Work

The advancement of IoV and VANETs has necessitated robust and efficient security mechanisms to ensure reliable communication and data integrity[1]. This chapter discusses state-of-the-art security solutions, focusing on two primary categories: TPD[111] and PUF[80]. The Figure 2.1 classifies the literature survey on security solutions in IoV based on these two categories. TPD-based solutions include various authentication schemes (public-key, identity-based, session key-based), batch verification schemes (static and dynamic), secure data handling, and vehicular cloud security. PUF-based solutions focus on PUF-based authentication (including DIoV), authenticated encryption, PUF-based key generation methods, and hardware-based cryptographic methods. This classification provides a structured overview of current research, highlighting key areas of focus and the specific security challenges addressed in IoV systems. The section 2.1 reviews public key-based, identity-based, and session key-based authentication schemes. Public key-based schemes offer robustness but are computationally intensive. Identity-based schemes simplify key management but depend on a single Private Key Generator (PKG). Session key-based schemes are more efficient but face challenges in secure key exchanges. The chapter also discusses batch verification methods essential for high message density in vehicular networks, categorized into static and dynamic batch verification methods. Static methods reduce computational overhead but struggle with high verification times. Dynamic methods adapt to varying network conditions but face scalability issues.

Additionally, the chapter explores secure data handling through edge computing[72] and vehicular cloud systems[74], addressing data latency and bottlenecks. It covers encryption techniques and secure indexing methods, including SSE and homomorphic encryption[73]. The section 2.2 examines PUF-based schemes, highlighting their use in generating unique, unclonable identifiers for secure authentication and key generation. PUF-based authentication schemes are designed to be lightweight and resistant to a wide range of attacks, making them suitable for resource-constrained IoV networks. The chapter also discusses authenticated encryption[112] and hardware-based cryptographic solutions, emphasizing the use of PUFs for secure key generation and storage. Combining these methods enhances security and performance against various attacks. By analyzing state-of-the-art methodologies and frameworks, this comprehensive survey offers an in-depth understanding of the current technological landscape. It systematically examines the strengths and limitations of existing approaches, providing critical insights into their functionality and efficacy. Moreover, this analysis highlights significant gaps and challenges within the field, leading to the introduction of the proposed security solutions designed to address these identified challenges. The proposed schemes in this thesis are tailored to bridge these gaps, thereby advancing the state of research in the field of IoV security.

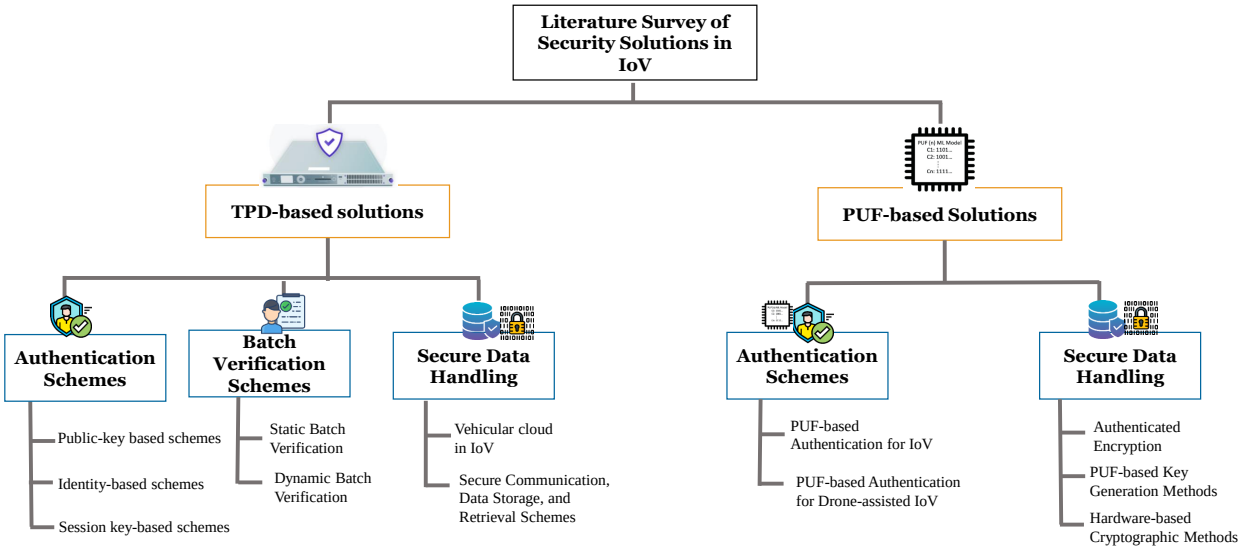

Figure 2.1: Structural organization of the literature survey

2.1 BASED ON TAMPER-PROOF DEVICE

The first part of this chapter reviews schemes that leverage TPDs for enhancing security in IoV and VANETs. These schemes are crucial for ensuring security against unauthorized access and tampering in vehicular communication. The following subsections explore various authentication, batch verification, and secure data handling methods, discussing their implementation, efficacy, and drawbacks.

2.1.1 Authentication Schemes

This chapter explores existing authentication schemes that are used within vehicular networks, including public key-based schemes, identity-based mechanisms, and session key-based approaches. These methodologies are crucial for establishing secure communication channels in the inherently dynamic and decentralized environment of VANETs and the broader IoV. Each scheme is analyzed to understand its computational demands, vulnerabilities to various attacks, and the practical challenges associated with its deployment in real-world vehicular scenarios. Public key-based authentication schemes[98, 99, 100, 101] are foundational to securing communications. These schemes leverage asymmetric cryptography. When a vehicle sends a message, it is signed with its private key, and the recipient can verify the authenticity of the message using the sender's public key[98]. This mechanism ensures that messages are not tampered with and that the sender's identity is authenticated. Despite their robustness, public key-based schemes often suffer from high computational overhead. The process of encrypting and decrypting messages, as well as generating and verifying digital signatures, can be computationally intensive[102], especially for resource-constrained vehicular systems. Moreover, these schemes can be vulnerable to certain types of attacks, such as man-in-the-middle attacks, where an attacker intercepts and potentially alters the communication between two parties. The detailed explanations of public key based authentication schemes and their limitations are discussed in the Table 2.1. Identity-based authentication schemes[102, 103, 46, 47, 48, 113] simplify the key management process by using the identities of vehicles (such as their license plate numbers) as public keys.

This approach eliminates the need for a Public Key Infrastructure (PKI) to distribute and manage public keys, which can be particularly beneficial in a highly dynamic vehicular network[46]. In identity-based schemes, a trusted third party, known as the PKI, is responsible for generating private keys based on the identity of each vehicle. While identity-based schemes reduce the overhead associated with key distribution, they introduce other challenges[32]. The reliance on a single PKI creates a single point of failure, making the entire system vulnerable if the PKI is compromised. Additionally, the computational cost of bilinear pairings, which are often used in these schemes, can be significant. Table 2.1 explains methodologies of the existing identity-based authentication schemes and their limitations. Furthermore, session key-based authentication schemes[50, 49, 114, 115, 116] use a temporary session key for secure communication between vehicles.

Table 2.1: State-of-the-art for TPD-based authentication schemes: Public key-based and Identity-based

Schemes	**Methodology and strengths**	**Limitations**
Wang et al. [98]	Public key based authentication, membership validity is used instead of a Certificate Revocation List (CRL), Diffie-Hellman hypothesis and bi-linear pairing are used.	High computation delay, data leakage issues.
Islam et al. [99]	Public key based authentication, it uses hash functions, and implemented without bi-linear pairing and ECC.	Does not provide key management, no solution for non-repudiation.
Azees et al. [100]	Public key based authentication, it uses bi-linear pairing and Provides solution for conditional traceability.	High Computational cost due to the pairing operations and vulnerable to DoS attack.
Zhang et al. [101]	Public key based authentication, it uses Chinese Remainder Theorem (CRT)-based domain key management technique and provide solution for data leakage.	Vulnerable to Man-in-the-Middle attack. It Does not provide a solution for key updates or password updates.
Li et al. [102]	Identity-based authentication, along with bi-linear pairing, is used. Performance analysis is done using IBS and IBOOS methods.	No security proof, high computation overhead, and vulnerable to side-channel attack.
Malhi et al. [103]	Identity-based authentication, it uses bi-linear map, along with Diffie-Hellman method. Bloom filters are used to design a security framework.	High computational cost, no security analysis, and vulnerable to data leakage issues.
Liu et al. [46]	Identity-based and proxy-based authentication, it uses bi-linear pairing and provides a solution to trace the malicious proxy node.	High computation overhead, no security proof, and vulnerable to leakage problems and impersonation attacks.
Bayat et al. [47]	Identity-based authentication, it uses ECC-based cryptography along with bi-linear pairing, and provides privacy preservation.	High computational overhead, vulnerable to various security attacks, and No security proof.
Jenefa et al. [48]	Identity-based authentication, it uses ECC, and considers non-repudiation, traceability, privacy-preservation, unlinkability.	Vulnerable to the data leakage problem that occurs due to the side channel attack.
Sutrala et al. [113]	Identity-based authentication, provide an efficient solution for batch message verification, detailed formal security proof and software-based security proof using AVISPA tool.	High Computation overhead, and vulnerable to collision attack.

These schemes typically involve the exchange of cryptographic keys at the beginning of a communication session, which are then used to encrypt and decrypt messages for the duration of the session[14]. Session keys are usually short-lived and regenerated for each new session, which enhances security by limiting the window of opportunity for attackers. Session key-based schemes are generally more efficient in terms of computational overhead compared to public key-based schemes, as symmetric key cryptography

used in session key mechanisms is less resource-intensive. However, these schemes still face practical deployment challenges. The initial key exchange process must be secure to prevent attackers from intercepting the session key[50]. Additionally, managing the frequent generation and distribution of session keys can be complex in a rapidly changing vehicular environment. The survey in Table 2.2 provides a comparative analysis of these session key-based authentication schemes, highlighting their respective strengths and weaknesses. Despite having many advantages, these schemes compromise user privacy and do not provide any solution to protect the privacy[42]. The deployment of these existing schemes in the IoV requires careful consideration of their computational overhead, susceptibility to attacks, and user's privacy challenges. The high mobility of vehicles and the need for real-time communication necessitate that authentication schemes should be very fast, resilient to various attacks and provide the balance between authentication and privacy preservation. Moreover, the diverse hardware capabilities of vehicles mean that authentication schemes must be adaptable to different levels of computational power and storage capacity[45]. The survey underlines the need for lightweight authentication mechanisms that can provide robust security without imposing significant computational or management burdens on IoV and without compromising user's privacy.

Table 2.2: State-of-the-art for TPD-based authentication schemes: Session key-based and MAC-based

Schemes	**Methodology and strengths**	**Limitations**
Chuang et al. [50]	Session key based authentication, uses the mechanism of transitive trust relationships.	No formal security proof, and vulnerable to data leakage problems or side-channel attacks.
Shao et al. [49]	Session key based authentication, it uses bi-linear pairing and the Diffie-Hellman technique, reduces the time to download and verify the CRL list.	High computational overhead, does not provide a solution for collision induction attack, no key management.
Wazid et al. [114]	Session key based authentication, it provides mutual authentication, and uses the concept of clusters and cluster-head.	Vulnerable to side-channel attacks and key lifetime self-extension attacks.
Bagga et al. [116]	Session key based authentication, it uses Secure Hash Algorithm (SHA)-1 hash function, and provides formal security proof using the AVISPA tool.	High computation overhead, and vulnerable side channel attack.
Lin et al. [117]	MAC-based authentication scheme , timed efficient protocol, communication and computation overhead minimized.	Does not provide any security proof, and vulnerable to data leakage problem.
Lyu et al. [118]	MAC-based authentication scheme, it provide solution for DoS attack, minimizes communication and computation overhead.	Vulnerable to side-channel attack, and impersonation attack.
Wang et al. [119]	MAC-based authentication scheme, uses Hash-Based Message Authentication Code (HMAC)-based scheme, and biometric technology.	Vulnerable to illegal bio-metric access.
Asl et al. [120]	MAC-based authentication scheme, provide solution for non-repudiation and integrity.	High computation overhead and vulnerable to DoS, side-channel, and impersonation attacks.
Li et al. [121]	HMAC based authentication, uses verifiable secret sharing concept along with the HMAC, and provides conditional privacy preservation.	High computation overhead, and does not provide password updation and key updation phases.

2.1.2 Batch Verification Methods

In vehicular networks, the high density of messages necessitates efficient verification mechanisms to maintain communication integrity without imposing excessive computational burdens on the network. Batch verification methods address this need by allowing multiple messages to be authenticated simultaneously, thereby enhancing the overall performance of IoV network by reducing the time and resources needed

for individual message verification[55]. In this thesis, these methods are broadly categorized into static and dynamic batch verification methods. This categorization stems from their differing abilities to handle the unique challenges posed by the dynamic nature of vehicular networks, ensuring that both efficiency and security are maintained across varying conditions. Static batch verification methods are typically pre-configured and suited for environments with stable traffic patterns, whereas dynamic batch verification methods are more adaptable, capable of adjusting to varying network conditions and traffic density. The followings are detailed literature surveys on both categories, highlighting their methodologies, advantages, and limitations in the context of IoV.

Static batch verification: Static batch verification is essential for maintaining efficiency in vehicular communications, particularly in environments where traffic patterns are predictable and stable. These methods are designed to verify multiple messages simultaneously, reducing the computational overhead and ensuring that vehicular networks can handle the high volume of data exchanged without significant delays. Static batch verification leverages pre-configured schemes that are well-suited to consistent network conditions, making them ideal for scenarios where the variability in message traffic is minimal. However, the effectiveness of the existing batch verification methods can be challenged by the need to mitigate the trade-off between security and efficiency, especially as vehicular networks grow more complex and interconnected. The detailed explanation of state-of-the-art static batch verification, highlighting the methodologies, strengths and limitations, is provided in the Table 2.3. Zhang et al. [122] proposed an innovative batch verification scheme using group testing for vehicular communications.

Table 2.3: State-of-the-art static batch verification schemes for IoV

Schemes	**Methodology and strengths**	**Limitations**
Zhang et al. [122]	Batch verification using group testing. Streamlines the verification process by reducing the number of individual verifications required.	High verification times due to the use of the Map to Point hash function, vulnerable to replay attacks, fails to ensure non-repudiation.
Lee et al. [123]	Secure batch verification using group testing. Applicable to both V2V and V2I communication environments, enhances security.	High verification times due to computationally intensive pairing operations, less suitable for real-time applications.
Tzeng et al. [124]	Identity-based batch verification. Improves security and privacy in VANETs, reduces verification time.	Vulnerable to man-in-the-middle attacks and impersonation.
Bayat et al. [47]	Batch verification using RSCN-based approach. Suitable for highly dynamic IoV networks where speed and efficiency are main concerns.	High verification times due to reliance on the Map-to-Point (M2P) hash function.
Limbasia et al. [125]	Energy-efficient and secure communication using Rivest-Shamir-Adleman (RSA) for batch verification. Ensures secure communication.	High computational demands of the RSA algorithm lead to increased execution times, less ideal for IoV where quick verification is necessary.

This method aims to streamline the verification process by reducing the number of individual verifications required. However, it suffers from high verification times due to the use of the Map to Point hash function. Additionally, this scheme is vulnerable to replay attacks and fails to ensure non-repudiation, posing significant security concerns within the vehicular network. Lee et al. [123] introduced a secure batch verification scheme that also employs group testing, applicable to both Vehicle-to-Roadside (V2R) and V2I communication environments. While this method enhances security, it incurs high verification times due to the computationally intensive pairing operations required. This high computational demand makes the scheme less suitable for real-time applications where rapid verification is critical. Tzeng et al. [124] presented an identity-based batch verification scheme aimed at improving security and privacy in VANETs.

Although this approach successfully reduces verification time, it is vulnerable to man-in-the-middle attacks and impersonation, highlighting the need for further improvements to strengthen its security measures. Bayat et al. [47] developed a batch verification and authentication scheme for VANETs using the RSCN-based approach. This scheme's reliance on the Map-to-Point (M2P) hash function results in high verification times, which is suitable for its practical deployment in highly dynamic IoV network where speed and efficiency are the main concerns. Limbasia et al. [125] proposed an energy-efficient and secure communication scheme, ESCBV that uses RSA for batch verification. While ESCBV ensures secure communication, the high computational demands of the RSA algorithm lead to increased execution times. This limitation makes the scheme less ideal for IoV where quick verification is necessary to maintain seamless data exchange. All the above-discussed methods offer a robust framework for efficient message verification in predictable vehicular environments. However, their effectiveness is often hampered by high computational demands and security vulnerabilities. Continued research and development are needed to address these challenges and enhance the practical deployment of these methods in IoV networks.

Dynamic batch verification: Dynamic batch verification methods offer a more adaptive approach, tailored to the highly variable and dynamic nature of vehicular environments. Unlike static methods, dynamic batch verification is designed to handle the rapid changes in vehicle density, mobility patterns, and communication demands of the IoV network. This adaptability is crucial for ensuring that IoV can provide reliable and secure communication in real-time, even as conditions change unpredictably. Many research has been conducted to achieve dynamic batch verification that are briefly illustrated in the Table 2.4 along with the strengths and limitations.

Table 2.4: State-of-the-art dynamic batch verification schemes for IoV

Scheme	Methodology and strengths	Limitations
Jing et al. [126]	Mini-batch strategy to enhance promptness by processing smaller message batches frequently.	Scalability issues, lacks comprehensive literature review.
Jiang et al. [127]	Group signature-based anonymous authentication for privacy-preserving distributed learning.	Challenges in large-scale key management.
Zhou et al. [128]	Certificateless, privacy-preserving batch verification reducing computational and communication burdens.	Requires empirical validation for practical effectiveness.
Wu et al. [129]	Batch-assisted scheme reducing verification delays, enhancing communication efficiency.	Dependency on verification terminals availability.
Ferng et al. [130]	Dynamic batch verification using ML for message classification, improving network performance.	Compromised effectiveness in skewed message authenticity distributions.
Zhang et al. [131]	Hierarchical authentication with short-term anonymous certificates for quick verification.	Complicates certificate management, potential security vulnerabilities.
Tao et al. [132]	Blockchain-based approach with elliptic curves for efficient privacy protection and message authentication.	Challenges in maintaining synchronized timestamps.
Liu et al. [133]	ECC-based multi-stage conditional privacy-preserving authentication protocol.	Complexity hinders practical deployment.
Maurya and Chaurasiya [34]	ECC-based conditional privacy preservation, robust security demonstrated by AVISPA.	High computational and communication overhead.

Jing et al. [126] proposed a mini-batch strategy aimed at enhancing the promptness of IoV communications. This method focuses on reducing the delay in message verification by processing smaller batches of messages more frequently. However, it faces limitations in scalability and lacks a comprehensive comparative literature review, which restricts its effectiveness in large-scale implementations where the volume of

messages can be significantly higher. Jiang et al. [127] introduced a group signature-based anonymous authentication scheme designed to support privacy-preserving distributed learning in vehicular networks. The scheme shows promising results in simulations, effectively balancing privacy and security. Nonetheless, managing secret keys at a large scale poses a significant challenge, potentially hindering its deployment in extensive IoV systems. Zhou et al. [128] developed a certificateless, privacy-preserving batch verification for VANETs. This approach aims to reduce computational and communication burdens while ensuring robust security against common attacks. Although the theoretical framework is sound, empirical validation is needed to confirm its practical effectiveness and resilience in real-world scenarios. Wu et al. [129] addressed verification delays in VANETs by introducing a batch-assisted scheme. Their theoretical analysis and simulations indicate significant reductions in verification delays, enhancing the efficiency of vehicular communication. However, the scheme's dependency on the availability of verification terminals presents a limitation, especially in scenarios where terminal access is restricted or inconsistent. Ferng et al. [130] proposed a dynamic batch verification scheme uses Machine Learning (ML) for message classification in VANETs. This approach improves network performance and communication efficiency by leveraging the predictive capabilities of ML. Nevertheless, its effectiveness may be compromised in networks with a skewed distribution of message authenticity, highlighting the need for further refinement. Zhang et al. [131] introduced a hierarchical authentication scheme for VANETs designed to improve message verification. The method relies on short-term anonymous certificates, which, while facilitating quick verification, complicate certificate management and introduce potential security vulnerabilities due to their transient nature. A blockchain-based approach [132] employed elliptic curves and batch verification to achieve efficient privacy protection and message authentication. Despite its theoretical strengths in providing secure and efficient communication, the approach faces challenges in maintaining synchronized timestamps across the network, which is critical for ensuring the integrity and reliability of authenticated messages. The conditional privacy-preserving Authentication Protocol [133] proposed an ECC-based multi-stage process for IoVs. This protocol promises strong security through its multi-layered approach, but the complexity of the multi-stage process poses significant hurdles for practical deployment, particularly in environments requiring rapid and straightforward implementation. Maurya and Chaurasiya [34] proposed an ECC-based conditional privacy preservation authentication scheme. Their security analysis using the ROM and Automated Validation of Internet Security Protocols and Applications (AVISPA) tool demonstrates robust security. However, the scheme is hindered by high computational and communication overhead, making it less suitable for lightweight applications where efficiency is paramount. In summary, existing dynamic batch verification methods present solutions to the challenges of securing and optimizing communication in highly dynamic IoV. While these methods offer significant advantages in terms of adaptability and efficiency, they also face challenges related to scalability, complexity, and practical implementation. Ongoing research and development are necessary to refine these approaches and ensure their effectiveness in real-world IoV applications.

2.1.3 Secure Data Handling

In IoV, the secure handling of data is essential due to the highly dynamic and distributed nature of vehicular networks. The convergence of edge computing and Vehicular cloud (V-cloud) systems offers a promising solution to the inherent challenges in IoV, such as data latency, bottlenecks in centralized systems, and the need for robust security and privacy measures. The literature on secure data handling within IoV includes various techniques to ensure the integrity, confidentiality, and availability of data transmitted across the network. This literature survey aims to provide a comprehensive overview of existing techniques designed to address these challenges, focusing on secure data collection, storage, and retrieval within IoV network.

The literature survey begins with an exploration of edge computing-based hybrid architectures. These architectures leverage the distributed nature of edge nodes to enhance data processing capabilities while maintaining secure communication channels. Further, the survey covers various secure communication schemes that have been proposed to protect data integrity and authenticity. This includes the utilization of PKI, identity-based cryptographic schemes, and advanced encryption techniques. In addition to secure communication, the literature survey explores secure storage mechanisms that ensure data confidentiality both at the edge and the V-cloud. These mechanisms include encryption techniques for data at rest and in transit, as well as secure indexing and retrieval methods that facilitate efficient and secure data access. The survey also highlights existing approaches to secure query searching, emphasizing on the balance of security and performance. Techniques such as SSE and homomorphic encryption are discussed in the context of their applicability to real-time vehicular data processing and retrieval.

Vehicular cloud in IoV: Many research schemes have been designed that describe how the concept of conventional cloud computing can be used in combination with traditional vehicular networks. These schemes are briefly explained in the Table 2.5 that highlights the strengths and weaknesses of the state-of-the-art schemes. Eltoweissy et al. [44] first introduced the concept of V-cloud in traditional vehicular networks. They suggested the term Autonomous Vehicular Clouds (AVC), in which the resources are dynamically allocated to the authorized user by autonomous vehicles. However, they do not provide any specific architecture for Vehicular Cloud Networking (VCN).

Table 2.5: State-of-the-art cloud computing schemes in IoV

Scheme	Methodology and strengths	Limitations
Eltoweissy et al. [44]	Introduced AVC, where resources are dynamically allocated by autonomous vehicles.	No specific architecture for VCN.
Bernstein et al. [74]	Proposed a PaaS model involving many humans in a highly dynamic network.	Centralized model prone to bottleneck issues.
Hussain et al. [75]	Proposed a possible architecture combining VANETs and the cloud, discussing VC, VuCs, and HC.	Does not address privacy concerns.
Yu et al. [76]	Designed a scheme combining cloud computing with smart vehicular networks, allowing nodes to handle different resources (computation, bandwidth, storage).	Challenging to implement in rural and urban areas.
Ahmad et al. [62]	Explained a three-tier architecture (V-cloud, infrastructure cloud, back-end cloud) incorporating cloud concepts.	Centralized approach is prone to bottleneck issue.
Mekki et al. [77]	Introduced a new idea about V-clouds, categorizing existing architectures based on the cloud state, deployment strategies, and centralization level.	Centralized approach not feasible in traffic scenarios.

Further, in 2010, Bernstein et al. [74] proposed involving many humans in a highly dynamic network. They discussed the Platform as a Service (PaaS) model for this purpose, but their model is centralized and prone to the bottleneck issue. Later, in 2012, Hussain et al. [75] proposed a possible architecture for combining VANETs and the cloud. In their research, Vehicular Cloud (VC), VANET using Clouds (VuCs), and Hybrid Clouds (HCs) are broadly discussed. This concept does not address privacy concerns. Yu et al. [76] designed a scheme to combine the concept of cloud computing with various purposes of the smart vehicular network. The proposed architecture allows the vehicular nodes to deal with different types of resources (i.e., computation, bandwidth, storage). However, the implementation of the given architecture in rural and urban areas is a challenging task. Ahmad et al. [62] explained a three-tier architecture (V-cloud,

infrastructure cloud, back-end cloud) incorporating the cloud concept and provided a brief description of each cloud. In 2017, Mekki et al. [77] introduced a new idea about V-clouds. They also categorized existing architectures based on the state of the cloud, the deployment strategies, and the level of centralization. Again, this centralized approach is not feasible in traffic scenarios.

Secure data storage and retrieval: Initially, the PKI was proposed to accomplish mutual authentication among the users. Later anonymous authentication methods have been recommended to preserve privacy by masking the real identities of users[134],[122]. An anonymous authentication scheme was proposed by Azees et al. [100] that provides privacy preservation and integrity along with the authentication. In [135], Gayathri et al. proposed a new pairing-less certificate-free authentication mechanism having low computational delay. This scheme does not provide secure data storage in the cloud. Hence it is vulnerable to the data leakage problem. Another identity-based authentication scheme was proposed by He et al. [136] that provides privacy preservation for the user in a VANET environment. The main drawback of this scheme is that it does not provide any solution for key disclosure. In 2019, Cui et al.[137] derived an algorithm for efficient authentication to monitor road conditions. The authors used the concept of fog computing and proposed a certificate-less aggregate signcryption mechanism. In 2021, Zhang et al.[101] discussed a security solution based on the CRT. The authors guaranteed that the proposed solution also meets the demand for privacy preservation. Still, the proposed batch verification solution depends on the size of the batches, which is not desirable. In [72], J. Cui et al. proposed a mechanism for authentication based on edge computing. The authors used the Cuckoo filter data structure to process a large amount of data. The main drawback of the Cuckoo filter is that it can not guarantee 100% true results, i.e., insertion may fail at any point in time. In 2021, Bagga et al.[116] proposed a security solution for IoV to authenticate vehicles. The authors used mutual authentication mechanism for this. They also used the AVISPA tool for formal security analysis. Further, a design for the SSE process is proposed by Curtmola et al. [138], which is used for data searching over the encrypted database. In [139], Kamara et al. suggested an SSE technique that satisfies the properties like the capability to effectively insert and remove files, sub-linear search time, security over the chosen-keyword threats, and compact indexes. Sub-linear search time for their technique is $O(\#f_w)$, where $\#f_w$ is the number of files having w keyword. In 2014, Cash et al. [140] gave an idea of a dynamic SSE method that can deal with a considerably large dataset. The time complexity of searching for [140] is $O((r+d_w)/p$, where r is the database $|DB(w)|$ having w query and p denotes number of processors. Sun et al. [141] proposed an improvised SSE method in which the online services are not dependent on the data owner, and the communication cost is also minimized. The existing schemes for secure searching are having the high search time complexity that is not desirable to get quick response for real-time incidents in IoV. Table 2.6 depicts the brief summary of the state-of-the-art secure communication and secure searching schemes including their methodologies, strengths and limitations.

Table 2.6: State-of-the-art authentication and secure searching schemes in IoV

Scheme	Methodology and strengths	Limitations
Zhang et al. [134], [122]	Proposed anonymous authentication methods to preserve privacy by masking real identities of users.	High computation overhead.
Azees et al. [100]	Proposed an anonymous authentication scheme providing privacy preservation and integrity along with authentication.	Vulnerable to man-in-middle-attack, high complexity.
Gayathri et al. [135]	Proposed a pairing-less certificate-free authentication mechanism with low computational delay.	Does not provide secure data storage in the cloud, vulnerable to data leakage.

Continued on next page

Scheme	Methodology and strengths	Limitations
He et al. [136]	Proposed an identity-based authentication scheme for privacy preservation in a VANET environment.	Does not provide a solution for key disclosure.
Cui et al. [137]	Derived an algorithm for efficient authentication using fog computing and a certificateless aggregate signcryption mechanism.	No solution for key disclosure, no solution for secure query searching.
Zhang et al. [101]	Proposed a security solution based on the CRT, ensuring privacy preservation.	High computation and communication overhead.
Cui et al. [72]	Proposed an edge computing-based authentication mechanism using the Cuckoo filter.	The Cuckoo filter cannot guarantee 100% true results, insertion may fail.
Bagga et al. [116]	Proposed a mutual authentication mechanism for IoV using the AVISPA tool for formal security analysis.	Vulnerable to data leakage issue, no secure query searching.
Curtmola et al. [138]	Proposed a design for the SSE process for data searching over encrypted databases.	High search time complexity.
Kamara et al. [139]	Suggested an SSE technique with effective file insertion/removal, sublinear search time, and security over chosen-keyword threats.	High search time complexity
Cash et al. [140]	Gave an idea of a dynamic SSE method dealing with large datasets.	High search time complexity
Sun et al. [141]	Proposed an improved SSE method minimizing the dependency on the data owner and communication cost.	High search time complexity, not desirable for real-time IoV.

2.2 BASED ON PHYSICAL UNCLONABLE FUNCTIONS

PUFs have emerged as a powerful technique for enhancing security in the IoV and VANETs. By leveraging the intrinsic physical characteristics of hardware components, PUFs provide a robust mechanism for generating unique and unclonable identifiers, which can be used for secure authentication and key generation. This section of the literature survey discusses various PUF-based schemes developed to address the security challenges in IoV, focusing on authentication schemes and secure data handling methods. The aim is to provide a comprehensive overview of the state-of-the-art PUF-based techniques, their methodologies, and their effectiveness in securing vehicular communications.

2.2.1 Authentication Schemes

PUF-based authentication schemes uses its unique, unclonable nature to establish secure identities and communication channels. The existing schemes are designed to be lightweight and resistant to a wide range of attacks, making them suitable for the resource-constrained and dynamic IoV networks.Several PUF-based authentication schemes are discussed, highlighting their methodologies and limitations. This thesis provides PUF-based security solution for IoV as well as Drone-assisted IoV (DIoV). Based on the proposed solutions, the survey for existing authentication schemes is further categorized into following subcategories:

Authentication schemes for IoV: Many researchers suggested PUF-based authentication schemes for IoV that are summarized in the Table 2.7 in terms of their strengths and limitations. In 2015, the authors in [105] discussed a provably secure protocol for ensuring privacy and mutual authentication between a server and a constrained device using PUFs. They claim that it is the first effort for the end-to-end design and evaluation

of a privacy-preserving PUF-based authentication protocol. However, the protocol does not have an internal synchronization, which makes it vulnerable to DoS attacks.

Table 2.7: State-of-the-art PUF-based authentication schemes in vehicular networks

Scheme	Methodology and strengths	Limitations
Aysu et al. [105]	Provably secure protocol for privacy and mutual authentication using PUFs. First end-to-end design and evaluation of a privacy-preserving PUF-based authentication protocol.	Lacks internal synchronization, vulnerable to DoS attacks.
Gope et al. [106]	Lightweight anonymous authentication protocol for RFID systems using PUFs. Focuses on security and privacy features.	Higher computation and communication overheads compared to other schemes.
Gope et al. [107]	Lightweight and physically secure mutual authentication protocol for IWSN.	Not suitable for highly dynamic IoV environment.
Chatterjee et al. [108]	PUF-based authentication and key exchange protocol for IoT without explicit CRPs in verifier database. Integrates IBE, PUFs, and keyed hash function.	Not resistant to side channel attacks, high computation and communication overhead, high resource complexity.
Aman et al. [51]	Privacy-preserving and scalable authentication protocol for IoV. Three-layer architecture with reduced number of authentication packets and MAC/PHY overhead.	Centralized system vulnerable to bottleneck problem at Trusted Authority (TA) failure.
Jiang et al. [142]	Three-factor authentication protocol using PUFs, combining password and biometrics with PUF. Uses AKE protocol for security.	Performance does not satisfy desired parameters for efficient IoV communication.

The authors in [106] designed an anonymous authentication protocol for Radio Frequency IDentification (RFID) systems using PUF which is lightweight and practical. The importance of RFID comes in the implementation of the IoT applications as it solves the identification issues of the things in a cost-effective manner. However, these systems are vulnerable to security and privacy issues. In order to solve these issues, PUFs are used. They claim that no other existing works has succeeded to address the problem of privacy preservation with the resistance of DoS attacks in a practical way. They mainly focused on the security and privacy features, hence the computation and communication overheads are comparatively higher than other schemes. The authors in [107] designed a mutual authentication protocol that is lightweight and physically secure for Industrial Wireless Sensor Networks (IWSNs). This protocol is not suitable for highly dynamic IoV environment. In 2019, Chatterjee et al. [108] came up with a PUF based authentication and key exchange protocol for IoT without explicit CRPs in verifier database. They integrated the concepts like Identity Based Encryption (IBE), PUFs, and key-ed hash function. Moreover, in the security analysis, it is proven that the scheme is resistant to session key attacks and the Universal Composability (UC) framework. However, the scheme is not resistant to the side channel attacks. Also, it has the high computation and communication overhead along with the high resource complexity. The authors in [51] proposed a privacy-preserving and scalable authentication protocol for IoV for reducing the overhead and improving throughput of application layer packets. They designed three layered architecture with road side units, road side unit gateways, and trusted authority as layers. The advantages are significantly reduced number of authentication packets and MAC/PHY (medium access control/physical medium) overhead. Due to the centralized system, the scheme is vulnerable to the bottleneck problem that occurs at the time of TA failure. Jiang et al. designed a three-factor authentication protocol [142] using PUFs, which eliminates the storage of any secret data in user devices or vehicle sensors. They have combined password and biometrics with PUF, so that the user device cannot be used by someone else to be successfully authenticated as the user. They claim that

using Authentication and Key Exchange (AKE) protocol, the system is secure even if the user devices are compromised. They focused to increase security and privacy features of the scheme and hence, the performance of the scheme does not satisfy the desired parameters required for efficient IoV communication.

Authentication schemes for DIoV: Further, drones, or Unmanned Aerial Vehicle (UAV)s, can play an important role in enhancing the capabilities of IoV by providing extended coverage, improved connectivity, and additional layers of security. The integration of drones in IoV, referred to as DIoV, introduces new dimensions in terms of mobility, scalability, and flexibility. Drones can act as mobile relays, data collectors, and surveillance units, significantly enhancing the performance and security of vehicular networks. The authentication protocols closely related to DIoV have been studied and briefly explained in the Table 2.8 including their methodologies, strengths and weaknesses.

Table 2.8: State-of-the-art authentication schemes in DIoV

Scheme	Methodology and Strengths	Limitations
Turkanovic et al. [143]	User authentication protocol for IoT, lightweight due to bit-wise XOR and hash functions.	Vulnerable to impersonation, stolen smart cards, man-in-the-middle attacks; lacks sensing node anonymity, user traceability, and session key security.
Farash et al. [144]	Improved user authentication method for IoT, using a session key for future secure communication.	Vulnerable to offline password guessing, impersonation, known session-specific temporary information, and stolen smart card attacks.
Challa et al. [145]	Signature-based user authentication and key agreement method for IoT, using fuzzy extractor and ECC.	Higher computation and communication costs.
Won et al. [146]	Suite of protocols for various scenarios: eCLSC-TKEM for one-to-one, CL-MRES for one-to-many, CLDA for many-to-one.	High computation overhead.
Wazid et al. [115]	Lightweight user authentication protocol for IoD, security analysis using AVISPA tool, practical implementation using NS-2.	Not resistant to stolen verifier and traceability attacks.
Khan et al. [147]	Privacy-preserving authentication scheme for UAV-enabled ITS, using digital signatures, hash function, and HECC techniques.	Not scalable.
Hussain et al. [148]	Lightweight user access protocol for drones, addressing flaws of [115], security analysis done both informally and formally.	Higher communication and computation costs.
Wu et al. [149]	Authentication scheme for edge computing enabled DIoV, providing anonymity and identity tracing.	Higher communication and computation costs.
Chaudhry et al. [150]	Lightweight authentication scheme for 6G-IoT enabled maritime transport system, validation using ROM.	Higher communication and computation costs.

In 2014, the authors in [143] designed a user authentication protocol for an IoT environment that can also be utilized in a DIoVs domain. They have used user nodes, sensor nodes, and gateways as components of the protocol. The scheme is lightweight due to bit-wise XOR and hash functions but is not resistant to impersonation, stolen smart cards, and man-in-the-middle attacks. In addition to that, the scheme fails to achieve sensing node anonymity, user traceability, and session key security. In 2016, Farash et al. [144] designed an improved user authentication method that overcomes the limitations of [143]. In this scheme also, a session key is used for future secure communication after a successful authentication process. This method also suffers from offline password guessing attacks, impersonation, known session-specific tempo-

rary information, and stolen smart card attacks. In 2017, the authors in [145] proposed a signature-based user authentication and key agreement method for an IoT environment that can also be integrated with an DIoVs environment. The method uses a fuzzy extractor technique ([151]) for the verification of the user's personal biometrics locally by the smart card. The scheme includes an ECC method for tracking the signature generation and verification mechanisms. However, it needs higher computation and communication costs compared with related schemes. In the same year, Won et al. [146] designed a suite of protocols to deal with three variety of scenarios, such as one-to-one, one-to-many, and many-to-one. For one-to-one, they proposed an efficient Certificateless Signcryption Tag Key Encapsulation Mechanism (eCLSC-TKEM) that supports authenticated key agreement, non-repudiation, and user revocation. The scheme reduces the time required to establish a shared key between a drone and a smart object by minimizing the computational overhead at the smart object. For one-to-many, they proposed a Certificateless Multi-Recipient Encryption Scheme (CL-MRES) by which a drone can efficiently send privacy-sensitive data to multiple smart objects. For many-to-one, they presented a Certificateless Data Aggregation (CLDA) protocol, which allows drones to efficiently collect data from hundreds of smart objects. In 2018, the authors in [115] proposed a lightweight user authentication protocol through which a user in the Internet of Drones (IoD) can access data directly from a drone, provided that the user is authorized to access the data from that drone. They have done the security analysis using AVISPA tool and practical implementation done using Network Simulator-2 (NS-2). However, the scheme is not resistant to stolen verifier and traceability attacks. A comparison with other competitive schemes needed to be carried out in order to examine the performance of the proposed methods in this thesis. For that, some closely related works have been considered and included here. In 2021, Khan et al. [147] discussed the security and privacy issues of UAV-enabled ITS, such as message alteration, vehicle locations, tracking of UAVs, and unauthorized access to data. In order to tackle with these issues, they have designed a privacy-preserving authentication scheme by combining digital signatures, hash function, and Hyper-Elliptic Curve Cryptography (HECC) techniques. The security analysis is done using ROM. However, the scheme is not scalable. In 2022, the authors in [148] designed a lightweight user access to drone for smart city surveillance. They identified the flaws of [115] and shows that the scheme in [115] cannot resist stolen verifier and traceability attacks. In addition to that, they claim that, an attacker with access to the verifier, can impersonate any user, drone or server of the system designed in [115]. To overcome these issues, the authors in [148] designed a lightweight system and the security analysis is done both informal and formal way. The scheme completes a cycle of authentication with a slight increase in computation time, but it offers all the required security features as compared with the scheme of Wazid et al. [115]. However, the scheme in [148] takes higher communication and computation cost. In the same year, Wu et al. [149] designed an authentication scheme for edge computing enabled DIoVs that provides anonymity and identity tracing. Here, the vehicles keep their identities anonymous during data transmission and roadside units act as mobile edge computing server which deals data from vehicles. However, the communication and computation cost of the scheme is higher. Recently, the authors in [150] proposed a lightweight authentication scheme for 6G-IoT enabled maritime transport system. The scheme validation is done using ROM. The communication and computation cost of the scheme is comparatively higher.

2.2.2 Secure Data Handling

In this subsection, the focus is on addressing the critical aspects of secure data handling by emphasizing two fundamental factors: Authenticated Encryption (AE) and hardware-based cryptographic solutions. AE ensures the confidentiality, integrity, and authenticity of data, making it suitable for securing communications in diverse applications, including IoV. Hardware-based cryptographic solutions, particularly those leveraging PUFs, offer robust and tamper-resistant mechanisms for secure key generation and storage.

The literature survey starts with a detailed examination of AE schemes. This includes various methods designed to provide secure encryption with integrated authentication, covering both symmetric and asymmetric approaches. The analysis focuses on their efficiency and suitability for resource-constrained environments such as IoV, where computational and energy resources are limited. Following this, the survey explores PUF-based cryptographic solutions, exploring how PUFs can be utilized in cryptographic applications, including key generation and secure storage. The final part of the survey discusses the integration of PUF technology with AE methods. By exploring these interlinked aspects, the survey aims to provide a comprehensive overview of the state-of-the-art techniques in secure data handling using PUFs.

Authenticated encryption methods: Usually, the AE methods are categorized based on different parameters such as AE categories, building blocks, modes and designs, and functional characteristics, etc. AE categories are defined as National Institute of Standards and Technology (NIST) competition, Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR) competition, beyond NIST or CAESAR competition). Building blocks for AE considers Block Ciphers (BC), Stream Ciphers (SC), General Permutations (PR), Sponge Construction (SP), Compression Functions (CF), so on. Modes and Designs for AE includes CTR, Synthetic Initialization Vector (SIV), Electronic Codebook (ECB), Offset Codebook (OCB), Even-Mansour Encryption (EME), Tiny AE (TAE), Addition-Rotation-XOR (ARX), Duplex construction, etc. In this literature survey, AE schemes have been categorized based on their building blocks. The detailed methodologies and limitations of these state-of-the-art AE schemes are briefly discussed in the Table 2.9. RFC 5084 [152] was Published in 2007, this document defines how to use AES in Counter with CBC-MAC (CCM) and Galois/Counter Mode (GCM) modes for AE within the Cryptographic Message Syntax (CMS). While AES-CCM and AES-GCM are widely used and considered secure, they do have some limitations like nonce reuse vulnerability, side-channel attacks, key management issues, and resource intensive. In 2014, Bogdanov et al. [153] proposed a new Authenticated Lightweight Encryption (ALE) that does not necessarily need associated data. Using the familiar AES operations, it boasts small hardware footprint (2.5x smaller than alternatives) and fast performance (2.5x faster, near AES-OCB). Further, in [154], authors proposed an AES-based AE method for 6G networks named as Rocca. They utilizes the Single Input-multiple Data (SIMD) instructions to design a comparable fast implementation platform for AES. Leveraging existing methods like AES, it surpasses them in speed by 4 times, reaching 138 Gbps. The authors of both the schemes does not provide the solution for nonce reuse issue. Recently, Lopez et al. [155] proposed an AE scheme using the combination of AES block cipher and Offset Two-Round (AES-OTR) to replace the GCM and OCB modes for fast implementation. The scheme does not handle the key management issue along with the nonce reuse attack. [156] introduces AES-LBBB, a new encryption scheme based on Beyond Birthday Bound (BBB), aiming for efficiency and security while being compatible with existing hardware designed for AES. This compatibility is achieved by limiting the internal state size and using the familiar AES operations. In [157], the authors uses ChaCha20 and Poly1305 cipher suits to mitigate side channel attack in standard AES block cipher and provided authenticated encryption. Although the scheme provides a good speed while implementing on Field-Programmable Gate Array (FPGA), the scheme is not suitable for resource constraints IoV devices. Ghouse et al. [158] proposed an improved version of AEGIS-128 encryption technique (i-AEGIS-128) that uses quarter round-based AES for the encryption and decryption process. The use of nonce increases the complexity and a chance for nonce reuse attack.

Table 2.9: State-of-the-art authenticated encryption schemes to achieve confidentiality and integrity

Scheme	Methodology and strengths	Limitations
Becker et al. [64]	Analyzed security of PUF-based key generation using index-based syndrome coding.	High execution time.
Delvaux et al. [159]	Proposed helper data algorithms for post-processing extracted bits from PUF chips to achieve reproducibility and high entropy.	High energy consumption.
Yanambaka et al. [160]	Lightweight authentication protocol for IoMT using PUF chips.	Takes 800 milliseconds to generate a 64-bit key, not suitable for resource-constrained IoV devices.
Satamraju and Malarkodi [161]	Mutual authentication scheme using PUFs for generating keys and identities of IoT devices; achieved 47.98% PUF randomness, 48.46% PUF uniqueness, and 2.38% PUF reliability.	Vulnerable to nonce reuse attack.
Noura et al. [162]	Efficient two-factor lightweight mutual authentication scheme for IoT devices, leveraging cryptographic protocol with configurable PUFs and a physical channel nonce.	Large power consumption and computation overhead for resource-constrained devices.
Zhang et al. [163]	Pairwise, continuous authentication protocol for IoT devices using PUFs with minimal computational overhead; uses CRP mechanism for periodic refreshment of authentication information.	High power consumption, not suitable for IoV devices with limited battery life.

PUF-based key generation methods: Various researchers, mentioned in the Table 2.10, used PUF chips to generate secure keys randomly to provide an extra layer of security. In 2015, Becker et al. [64] analyzed the security of PUF-based key generation that uses index-based syndrome coding. Further, Delvaux et al. [159] proposed helper data algorithms for post-processing the extracted bits from PUF chips to achieve reproducibility and high entropy. In [160], authors designed a lightweight authentication protocol for the Internet of Medical Things (IoMT) that uses PUF chips for the authentication process. However, the proposed method takes 800 milliseconds to generate a 64-bit key, which is not desirable for resource-constraint IoV devices. In 2020, Satamraju and Malarkodi [161] suggested a mutual authentication scheme that uses PUFs to generate the keys and the identities of the IoT devices. The authors achieved 47.98% PUF randomness, 48.46% PUF uniqueness, and 2.38% PUF reliability. Noura et al. [162] introduce an efficient two-factor lightweight mutual authentication scheme for IoT devices, leveraging a cryptographic protocol with configurable PUFs and a physical channel nonce, complemented by a unique entity-based fingerprint derived from communication protocol features. The scheme provides security against authentication attacks, but the power consumption and the computation overhead are large for the resource-constraint devices. In [163], authors introduce a pairwise, continuous authentication protocol for IoT devices using PUFs to ensure mutual authentication with minimal computational overhead. The protocol leverages a CRP mechanism for periodically refreshing authentication information, thereby enhancing security and performance through low-cost cryptographic operations like hashing and XOR. Compared to hardware cryptography, the power consumption of the proposed scheme is high and not desirable for IoV devices having limited battery life.

Table 2.10: State-of-the-art PUF-based schemes for secure key generation and authentication

Scheme	Methodology and strengths	Limitations
Becker et al. [64]	Analyzed security of PUF-based key generation using index-based syndrome coding.	Vulnerable to data leakage.

Continued on next page

Scheme	Methodology and strengths	Limitations
Delvaux et al. [159]	Proposed helper data algorithms for post-processing extracted bits from PUF chips to achieve reproducibility and high entropy.	High execution time to generate keys.
Yanambaka et al. [160]	Designed a lightweight authentication protocol for IoMT using PUF chips.	Takes 800 milliseconds to generate a 64-bit key, not desirable for resource-constrained IoV devices.
Satamraju and Malarkodi [161]	Suggested a mutual authentication scheme using PUFs for generating keys and identities of IoT devices; achieved 47.98% PUF randomness, 48.46% PUF uniqueness, and 2.38% PUF reliability.	Not suitable for resource-constraint devices due to high power consumption.
Noura et al. [162]	Introduced an efficient two-factor lightweight mutual authentication scheme for IoT devices, leveraging cryptographic protocol with configurable PUFs and a physical channel nonce.	High power consumption and computation overhead for resource-constrained devices.
Zhang et al. [163]	Proposed a pairwise, continuous authentication protocol for IoT devices using PUFs with minimal computational overhead; uses CRP mechanism for periodic refreshment of authentication information.	High power consumption, not suitable for IoV devices with limited battery life.

Hardware implementation of cryptography algorithm: In 2012, Gouvêa and López [164] implemented AE for the MSP430X microcontroller and compared different types of AE like CCM, GCM, SGCM, OCB3, Hummingbird-2 and Message Authenticated Streaming-encryption Heterogeneous Algorithm (MASHA). They concluded that the MASHA and Hummingbird-2 schemes are not suitable for hardware accelerators. The authors do not provide a solution for side-channel attacks, nonce-reuse, and key management issues. Nguyen et al. [165] proposed an Application-Specific Integrated Circuits (ASIC)-based hardware implementation of the AES-CCM AE technique to balance between throughput and resource constraints. The AES-CCM uses nonce as Initialization Vector (IV), and hence, the method is prone to nonce-reuse attacks. In [166], the authors implemented the AES block cipher using the pipeline method to improve the efficiency in speed and throughput. They introduced a masked S-box to mitigate the side channel attack but failed to provide a solution for the nonce-reuse issue. In [167], the author suggested a new hardware implementation of AES block cipher using the Finite State Machine with Datapath (FSMD). The implementation is done on the FPGA by providing two levels of modularity (AES operation over column/ bytes, key/ round expansion). However, the method is not suitable for resource-constrained devices due to high power consumption on FPGA. In 2021, Khan et al. [168] proposed generic implementation strategies like unrolled, round-based, and serialized to address throughput and security-related issues. The authors implemented Ascon-128 using these strategies. The power consumption using these techniques is higher in terms of resource-constrained devices. Further, for CAESAR competition, only ICE-POLE [169] and SCREAM[170] ciphers are implemented in their original document. Some of the CAESAR submissions like Ascon[171], CLOC[172], POET[173], Deoxys[174], PAEQ[175], etc. are considered for the competition for hardware implementation and the results are maintained by [176]. All these schemes are suitable for low area requirements but not suitable for resource-constrained devices in real-time applications. Further, the provided implementations are not nonce-reuse resistant.The proposed scheme aims to balance security and efficiency by making it nonce-reuse-resistant using PUF and suitable for resource-constrained devices in real-time applications. The brief explanations of the state-of-the-art hardware implementation schemes are provided in the Table 2.11, highlighting their strengths and weaknesses.

Table 2.11: State-of-the-art hardware implementation schemes for authenticated encryption

Scheme	Methodology and strengths	Limitations
Gouvêa and López [164]	Implemented AE for MSP430X microcontroller; compared CCM, GCM, SGCM, OCB3, Hummingbird-2, and MASHA.	MASHA and Hummingbird-2 not suitable for hardware accelerators; no solution for side-channel attacks, nonce-reuse, and key management issues.
Nguyen et al. [165]	ASIC-based hardware implementation of AES-CCM AE technique; balances throughput and resource constraints.	Prone to nonce-reuse attacks due to use of nonce as IV.
Oukili et al. [166]	Implemented AES block cipher using pipeline method; introduced masked S-box to mitigate side-channel attacks.	Does not address nonce-reuse issue.
Burciu [167]	Hardware implementation of AES block cipher using FSDM on FPGA; two levels of modularity.	High power consumption on FPGA; not suitable for resource-constrained devices.
Khan et al. [168]	Proposed unrolled, round-based, and serialized implementation strategies for Ascon-128; addresses throughput and security-related issues.	High power consumption for resource-constrained devices.
ICE-POLE [169]	Implemented for CAESAR competition.	Not suitable for resource-constrained devices in real-time applications; not nonce-reuse resistant.
SCREAM [170]	Implemented for CAESAR competition.	Not suitable for resource-constrained devices in real-time applications; not nonce-reuse resistant.
Ascon [171], CLOC [172], POET [173], Deoxys [174], PAEQ [175]	CAESAR competition submissions; considered for hardware implementation.	Suitable for low area requirements but not for resource-constrained devices in real-time applications; not nonce-reuse resistant.