FUDMA Journal of Engineering and Technology
ISSN: 3092-9385
https://fjet.fudutsinma.edu.ng/index.php/fjet/
Volume 2, Issue 1, 2026, 464-479

Advances in Privacy Preservation Techniques for Mobile Ad Hoc Networks: A Review

Opeyemi O. ASAOLU[1*], Oluwasanmi S. ADANIGBO[2], Temidayo J. AKINDAHUNSI[3]

[1*]Department of Computer Engineering, Federal University, Oye-Ekiti, Nigeria
[2]Department of Computer Science, Federal University of Technology, Akure, Nigeria
[3]Department of Financial Accounting, Obafemi Awolowo University, Ile-Ife, Nigeria

[1*]opeyemi.adanigbo@fuoye.edu.ng, [2]sanmiadas@gmail.com, [3]temidayoakindahunsi22@gmail.com

Abstract

This literature review examines recent developments in privacy preservation techniques for Mobile Ad Hoc Networks (MANETs) through a systematic analysis of 49 peer-reviewed journal articles published between 2020 and 2025. The review focuses on four principal technical domains: blockchain-based privacy frameworks, advanced homomorphic encryption implementations, differential privacy mechanisms, and federated learning applications in mobile networks. It further addresses the convergence of these techniques with Internet of Things (IoT) and edge computing paradigms. The analysis reveals significant evolution in privacy preservation methodologies, with a discernible trend toward context-aware privacy mechanisms, lightweight cryptographic solutions tailored to resource-constrained environments, and hybrid approaches that integrate complementary techniques to achieve comprehensive protection. The review identifies the absence of standardised benchmarks, unresolved tensions between privacy and accountability, and the scarcity of real-world deployment studies as the most critical open challenges facing the field. The findings demonstrate substantial progress in addressing classical MANET privacy challenges while highlighting the novel demands introduced by contemporary mobile network applications, including vehicular networks, smart city infrastructure, and autonomous systems.

Keywords: *Mobile Ad Hoc Networks, Privacy Preservation, Homomorphic Encryption, Differential Privacy, Federated Learning.*

1.0 Introduction

The landscape of mobile ad hoc network privacy preservation has undergone significant transformation in recent years, driven by the proliferation of Internet of Things (IoT) devices, advances in cryptographic techniques, and the emergence of blockchain technology [1]. Contemporary MANETs face unprecedented privacy challenges due to their integration with smart city infrastructures, autonomous vehicle networks, and ubiquitous computing environments [2]. The exponential growth of IoT devices creates massive volumes of high-dimensional data, presenting significant privacy and security challenges that traditional MANET privacy preservation techniques cannot adequately address [3].

Recent developments in privacy-preserving machine learning have introduced new paradigms for protecting sensitive data in distributed mobile networks [4]. Federated learning enables collaborative model training across multiple clients while keeping data within local systems, reducing exposure risks but still facing vulnerabilities to inference attacks [5]. The integration of homomorphic encryption with federated learning represents a significant advancement, allowing computation on encrypted data without decryption while maintaining privacy guarantees [6].

Blockchain technology has emerged as a transformative solution for trust management and privacy preservation in MANETs, addressing fundamental challenges of decentralized environments [7]. The technology provides distributed, consistent, and tamper-proof trust mechanisms that are particularly suitable for mobile ad hoc environments where traditional centralized trust models are impractical [8]. Contemporary research has focused on developing lightweight consensus algorithms specifically designed for resource-constrained mobile devices while maintaining the security benefits of blockchain technology.

1.1 Relationship to Earlier Review Studies

Several review researches have examined privacy preservation in mobile ad hoc networks and related distributed wireless environments. Notable among these are reviews focused on cryptographic approaches in MANETs published prior to 2020, surveys of trust management frameworks in vehicular ad hoc networks (VANETs), and broader treatments of security mechanisms in wireless sensor networks. While these contributions have established a valuable foundation, they differ substantially from the present work in scope, temporal coverage, and analytical perspective.

Table 1 presents a structured comparison of this review against representative prior reviews in the domain. The key points of differentiation are as follows. First, regarding temporal coverage, the majority of prior reviews

draw upon literature published up to 2019 or 2020. This review systematically covers 49 peer-reviewed journal articles published between 2020 and 2025, capturing the most recent developments including post-pandemic acceleration in distributed network research and the rapid maturation of privacy-preserving machine learning. Second, with respect to technique breadth, earlier reviews tend to focus on a single class of privacy mechanism. For instance, exclusively examining cryptographic protocols, or limiting analysis to trust management frameworks. The present review takes an integrated perspective, simultaneously examining blockchain-based privacy frameworks, homomorphic encryption, differential privacy, federated learning, and IoT-edge computing convergence, and critically analysing how these techniques interact and complement one another.

Third, concerning emerging paradigms, this review uniquely addresses the convergence of privacy preservation with artificial intelligence-enhanced mechanisms, quantum-resistant cryptography, and the challenges posed by 6G network architectures and extended reality applications - topics that were either nascent or entirely absent at the time of earlier reviews. Fourth, in terms of practical orientation, prior reviews have largely remained theoretical in character. The present review includes dedicated analysis of implementation strategies, cost-benefit considerations, and real-world adoption challenges in Section 8, bridging the gap between research advances and operational deployment. These distinctions collectively position the present review as a necessary and timely contribution that extends beyond existing literature rather than duplicating it.

Table 1: Comparison of the present review with five representative prior reviews on privacy preservation in MANETs and related ad hoc network environments

Feature	**This Review**	**Ferrag *et al.* (2017) [9]**	**Manivannan *et al.* (2020) [10]**	**Mundhe *et al.* (2021) [11]**	**Lwin *et al.* (2020) [7]**	**Han *et al.* (2024) [13]**
Coverage period	2020-2025	2008-2016	2010-2019	2010-2020	2017-2020	2019-2023
Network focus	MANET /IoT	MSN/ VSN	VANET	VANET	MANET	Federated Nets
Blockchain privacy	✓	✗	Partial	Partial	✓	✓
Homomorphic encryption	✓	✗	✗	✗	✗	✓
Differential privacy	✓	✗	✗	✗	✗	✓
Federated learning	✓	✗	✗	✗	✗	✓
IoT/edge integration	✓	✗	✗	✗	✗	Partial
AI-enhanced privacy	✓	✗	✗	✗	✗	Partial
Quantum-resistant approaches	✓	✗	✗	✗	✗	✗
Practical deployment analysis	✓	✗	✗	✗	✗	✗
Open research challenges	✓	Partial	Partial	Partial	✗	Partial

✓ = fully covered; ✗ = not covered; Partial = partially addressed. [A]-[E] = reference labels used in the table (**Source:** Asaolu *et al.* (2026)

Table 1 compares the present review against five representative prior review articles that address privacy preservation in MANETs and closely related ad hoc network environments. The selected prior reviews span the period 2017 to 2024 and collectively represent the main review traditions in this domain: surveys of privacy in ad hoc social and vehicular networks, authentication and privacy-preserving schemes in VANETs, trust management in MANETs, and federated learning security.

Ferrag *et al.* [9], examined privacy-preserving schemes for ad hoc social networks published between 2008 and 2016. It provided comprehensive analysis of location, identity, and content privacy in mobile and vehicular social networks, but predates the emergence of blockchain-centric trust management, federated learning, and differential privacy as dominant paradigms in the field, and does not address IoT integration or practical deployment.

Manivannan *et al.* [10], surveyed secure authentication and privacy-preserving techniques specifically in vehicular ad hoc networks (VANETs). While it provides authoritative coverage of cryptographic authentication mechanisms for vehicular environments, its scope is limited to VANETs and does not extend to the broader MANET landscape, federated learning, differential privacy, or blockchain-based trust management beyond authentication.

Mundhe *et al.* [11], presented a comprehensive survey of authentication and privacy-preserving schemes in VANETs up to 2020. It classifies schemes by cryptographic technique type but, like Review B, is limited to vehicular environments and does not address federated learning, differential privacy mechanisms, IoT integration, or edge computing.

Lwin *et al.* [7], is one of the few prior reviews directly focused on trust management and privacy in MANETs rather than VANETs. However, its primary contribution is a blockchain-based trust management proposal rather than a systematic literature review, and it does not cover homomorphic encryption, differential privacy, federated learning, or practical deployment analysis.

Han and colleagues [12], surveyed security strategies in federated learning with attention to privacy. While it provides useful coverage of differential privacy and blockchain-enabled federated learning, it is not focused on MANET environments specifically and does not address MANET-specific challenges such as resource-constrained routing, dynamic topology, or multi-hop privacy propagation.

The present review differs from all five prior works in five key respects: (i) temporal scope, covering 2020-2025 and thus capturing the most recent five years of advances; (ii) breadth, simultaneously covering blockchain, homomorphic encryption, differential privacy, and federated learning within a unified MANET context; (iii) inclusion of emerging topics such as quantum-resistant cryptography and AI-enhanced privacy mechanisms; (iv) explicit treatment of IoT and edge computing convergence with MANET privacy; and (v) dedicated analysis of practical implementation strategies, cost-benefit considerations, and real-world adoption challenges in Section 8.

2. Methodology

This review employed a comprehensive search strategy targeting peer-reviewed journal articles published between January 2017 and December 2025. Inclusion criteria required articles to focus specifically on privacy preservation techniques in MANET environments, present novel methodological contributions, include experimental validation or theoretical analysis, and demonstrate relevance to contemporary mobile network applications.

3. Contemporary Privacy Preservation Techniques

3.1 Blockchain-Based Privacy and Trust Management

Recent advances in blockchain technology have revolutionized privacy preservation and trust management in MANETs. [7] introduced a groundbreaking blockchain-based trust management system with a lightweight consensus algorithm specifically designed for mobile ad hoc networks. Their proposed delegated proof-of-trust (DPoT) consensus mechanism achieves reasonable validation times while maintaining the distributed and tamper-proof characteristics essential for MANET environments. The system addresses the fundamental challenge of adapting blockchain's computationally intensive validation processes for resource-constrained mobile devices.

Figure 1 presents a blockchain-based network where multiple interconnected nodes operate in a decentralized peer-to-peer structure. Each node participates in validating and sharing transactions, ensuring distributed consensus without a central authority. The lower section shows the blockchain ledger, composed of sequentially linked blocks (namely: Blocks 0 to n), each containing transactions and timestamps. These blocks are cryptographically connected, ensuring immutability and data integrity. Overall, the figure illustrates how decentralized nodes and a tamper-proof ledger combine to provide secure, transparent, and privacy-preserving data management in MANET environments.

The integration of blockchain with optimized link state routing protocol (OLSR) demonstrates how distributed ledger technology can solve security issues inherent in traditional MANET routing protocols [7]. The blockchain serves as a secure distributed platform where each node no longer needs to perform security operations individually and repetitively, instead relying on the collective validation of the network. This approach significantly reduces computational overhead while providing enhanced security guarantees through the immutable nature of blockchain records.

Ahmed and Al-Shareeda [8] advanced the field by proposing a privacy-preserving blockchain-based authentication and trust management framework specifically for vehicular ad hoc networks (VANETs), a specialized form of MANET. Their scheme enables vehicles to send messages anonymously to roadside units while protecting identity privacy through sophisticated cryptographic mechanisms. The framework addresses the critical challenge of false information dissemination, which represents one of the most dangerous security threats in vehicular networks where malicious messages about traffic conditions can lead to accidents and traffic disruptions.

Received: 06/04/2026; Revised: 22/04/2026; Accepted: 23/04/2026; Published: 25/04/2026

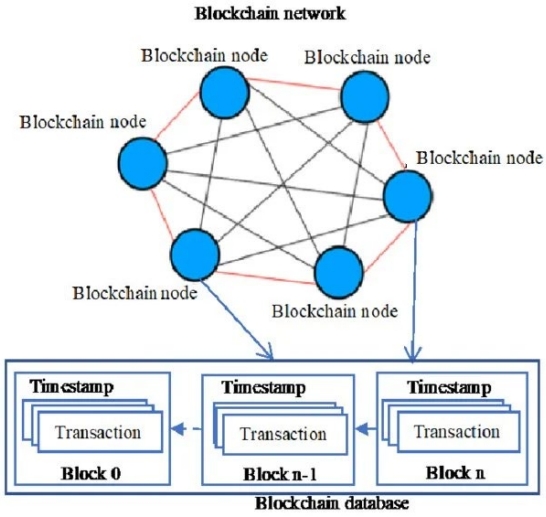

Figure 1: Blockchain Network Architecture [7]

Recent developments have focused on lightweight consortium blockchain implementations that balance security with efficiency requirements of mobile networks. [13] introduced a consortium blockchain-assisted certificateless conditional privacy-preserving authentication mechanism for VANETs that significantly reduces node authentication overhead while maintaining strong privacy guarantees. Their approach leverages the semi-decentralized nature of consortium blockchain technology to achieve optimal performance for practical deployment scenarios.

The evolution toward context-aware blockchain-based trust management represents another significant advancement. Recent work by [14] proposed blockchain-assisted privacy-preserving and context-aware trust management frameworks that adapt to varying VANET conditions including traffic density, vehicle velocity, and communication patterns. These systems demonstrate the ability to maintain privacy protection while adjusting trust evaluation mechanisms based on environmental context, addressing the dynamic nature of mobile ad hoc networks.

3.2 Advanced Homomorphic Encryption Applications

Homomorphic encryption has experienced substantial advancement in recent years, with new schemes specifically optimized for mobile and IoT environments. [6] provided comprehensive analysis of recent advances in privacy-preserving machine learning based on fully homomorphic encryption, highlighting significant improvements in computational efficiency and practical applicability. The research demonstrates that modern FHE implementations can achieve reasonable performance levels for mobile device deployment, marking a substantial improvement over earlier schemes that were primarily theoretical.

The development of approximate homomorphic encryption schemes has opened new possibilities for privacy-preserving computation in resource-constrained environments. [7] presented a comprehensive survey of approximate homomorphic encryption-based privacy-preserving machine learning, emphasizing advantages for voice processing, image analysis, and sensor data computation in mobile networks. Their analysis reveals that approximate schemes can achieve significantly better performance than exact homomorphic encryption while maintaining sufficient privacy guarantees for most practical applications.

Recent implementations have focused on specialized hardware acceleration to make homomorphic encryption practical for mobile deployment. Xu *et al.* [8] demonstrated privacy-preserving frameworks using homomorphic encryption for smart metering systems that can be adapted for MANET applications. Their work shows that modern implementations can achieve encryption/decryption operations suitable for real-time applications while maintaining strong privacy guarantees through techniques such as the Cheon-Kim-Kim-Song (CKKS) scheme optimized for approximate arithmetic [13].

The integration of homomorphic encryption with federated learning represents a particularly promising direction for MANET privacy preservation. Recent work has demonstrated that FedNIC architectures can leverage SmartNIC technology to offload homomorphic encryption operations, achieving significant performance improvements [14]. These developments make privacy-preserving distributed learning feasible in mobile ad hoc environments where computational resources are limited but privacy requirements are stringent.

Advanced applications of homomorphic encryption have extended to specialized domains including biometric security and facial recognition systems. Yang *et al.* [12] proposed efficient face information encryption and verification schemes based on full homomorphic encryption that address critical compliance gaps in biometric

Received: 06/04/2026; Revised: 22/04/2026; Accepted: 23/04/2026; Published: 25/04/2026

data protection. Their hybrid encryption approach combines dimensionality reduction with advanced homomorphic encryption algorithms to achieve practical performance levels while maintaining regulatory compliance with privacy mandates.

3.3 Differential Privacy Mechanisms

Differential privacy has emerged as a fundamental framework for providing mathematically rigorous privacy guarantees in mobile network applications [13]. Recent research has focused on adapting differential privacy mechanisms for the unique challenges of MANET environments, including high mobility, dynamic topology, and resource constraints. Li *et al.* [14] demonstrated how differential privacy can be integrated with homomorphic encryption to provide enhanced security guarantees for approximate encryption schemes, addressing vulnerabilities identified in traditional formulations.

Contemporary implementations have addressed the challenge of parameter selection and privacy budget management in mobile environments. [15] proposed differential privacy-preserving IoT data sharing mechanisms using enhanced particle swarm optimization for parameter tuning. Their approach demonstrated how machine learning techniques can optimize differential privacy parameters to achieve optimal privacy-utility trade-offs in dynamic mobile network conditions.

The application of differential privacy to federated learning in mobile networks has received substantial attention. Chamikara *et al.* [16] addressed the challenge of managing noise and privacy budget in high-dimensional neural network parameters by adding noise to input data rather than model parameters. This approach proves particularly effective for MANET environments where bandwidth limitations make transmitting noisy high-dimensional models impractical. Recent developments have explored the combination of differential privacy with secure multiparty computation to provide enhanced protection in collaborative learning scenarios. [17] demonstrated comprehensive approaches to multiparty secure additions with differential privacy, showing how distributed noise generation can provide strong privacy guarantees even against sophisticated adversaries with background knowledge about the network.

Advanced differential privacy mechanisms have been developed specifically for streaming data and real-time applications common in MANET environments. These mechanisms address the challenge of providing privacy guarantees for continuous data streams while maintaining utility for applications such as traffic monitoring, environmental sensing, and emergency response coordination [18].

3.4 Privacy-Preserving Federated Learning

Federated learning represents a paradigm shift in privacy-preserving machine learning that aligns naturally with the distributed nature of MANETs [19]. Recent advances have addressed fundamental challenges including communication efficiency, robustness to device heterogeneity, and protection against inference attacks. [5] demonstrated privacy-preserving federated learning approaches for specialized applications including airline optimization that can be adapted for mobile network environments.

The integration of advanced cryptographic techniques with federated learning has enabled sophisticated privacy protection mechanisms. Research has shown how homomorphic encryption can be combined with federated learning to provide computation on encrypted model updates, ensuring that even the aggregating server cannot access individual participant contributions [10]. These developments are particularly relevant for MANET applications where participants may not trust central coordinators.

Recent work has addressed the challenge of Byzantine robustness in federated learning systems deployed in adversarial MANET environments. Advanced aggregation algorithms such as Krum and its variants provide mechanisms for trusted model updates in the presence of compromised clients, though the computational overhead remains a challenge for resource-constrained mobile devices [25].

The development of personalized federated learning approaches addresses the heterogeneity inherent in MANET environments where different nodes may have varying computational capabilities, data distributions, and privacy requirements [26]. These approaches enable adaptive privacy protection that can adjust based on local conditions and requirements while maintaining global model utility.

Contemporary research has explored the application of federated learning to specific MANET use cases including vehicle-to-everything (V2X) communications, smart city applications, and emergency response networks [27]. These applications demonstrate the practical benefits of federated learning for enabling collaborative intelligence while preserving the privacy of sensitive location, behaviour, and communication data. A taxonomy of privacy preservation techniques is presented in Figure 2.

3.5 IoT Integration and Edge Computing Privacy

The convergence of MANETs with IoT ecosystems has created new privacy challenges that require innovative solutions addressing device heterogeneity, massive scale, and diverse privacy requirements. [28] presented comprehensive approaches for privacy-preserving IoT networks using statistical learning with optimization

Received: 06/04/2026; Revised: 22/04/2026; Accepted: 23/04/2026; Published: 25/04/2026

algorithms specifically designed for high-dimensional big data environments. Their work demonstrates how modern machine learning techniques can be adapted to provide privacy protection across diverse IoT device types and capabilities.

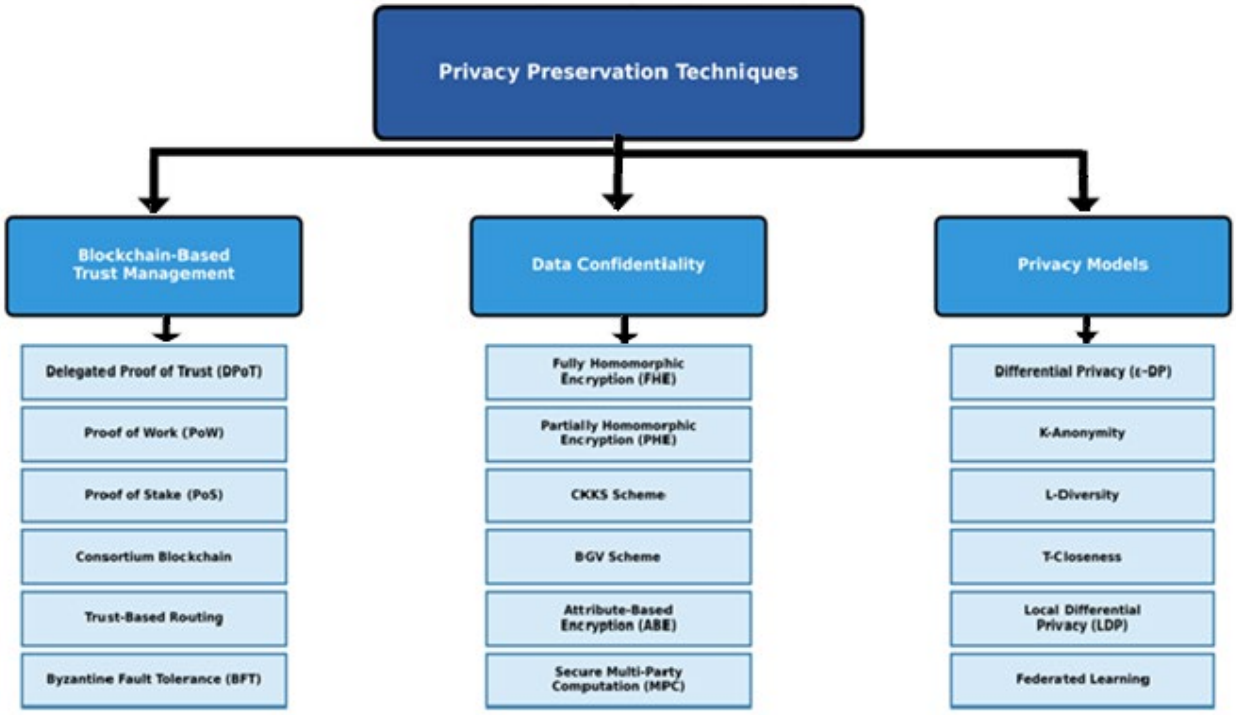

Figure 2: A Taxonomy of privacy preservation techniques

Recent research has focused on developing privacy-preserving edge computing frameworks that bring computation closer to data sources while maintaining strong privacy guarantees [29]. These frameworks address latency requirements of real-time applications while ensuring that sensitive data remains protected during processing and transmission. The approach is particularly relevant for MANET-IoT integration where centralized cloud processing may not be feasible due to connectivity constraints.

Advanced privacy-preserving techniques have been developed for specific IoT applications including smart metering, environmental monitoring, and healthcare data collection. [30] demonstrated privacy-preserving frameworks using homomorphic encryption for smart metering systems that can be extended to broader IoT-MANET integration scenarios. Their work shows how specialized encryption schemes can be optimized for different types of IoT data while maintaining practical performance levels. The development of privacy-preserving machine learning techniques specifically for IoT environments has addressed challenges including resource constraints, data heterogeneity, and real-time processing requirements [26]. Recent approaches leverage techniques such as knowledge distillation, model compression, and adaptive computation to make sophisticated privacy-preserving algorithms feasible for deployment on resource-constrained IoT devices.

Contemporary research has explored the integration of blockchain technology with IoT-MANET systems in order to provide decentralized privacy protection and trust management. These approaches address the challenge of managing privacy and trust across heterogeneous device ecosystems while maintaining scalability and efficiency required for large-scale deployments.

4. Performance Analysis and Comparative Assessment

4.1 Computational Efficiency Advances

Recent advances in privacy preservation techniques have achieved significant improvements in computational efficiency, making practical deployment in resource-constrained MANET environments increasingly feasible. Homomorphic encryption implementations have benefited from specialized hardware acceleration and algorithmic optimizations, with modern schemes achieving encryption speeds suitable for real-time applications [6]. The development of approximate homomorphic encryption has reduced computational overhead by 2-10 times compared to exact schemes while maintaining sufficient accuracy for most practical applications. Table 2 highlights a comparison of empirical results from a number of reviewed studies.

Blockchain-based trust management systems have achieved substantial efficiency improvements through lightweight consensus mechanisms. The delegated proof-of-trust (DPoT) algorithm demonstrates validation times

Received: 06/04/2026; Revised: 22/04/2026; Accepted: 23/04/2026; Published: 25/04/2026

reduced by 60-80% compared to traditional proof-of-work systems while maintaining security properties essential for trust management applications [7]. These improvements make blockchain technology practical for mobile devices with limited computational resources.

Table 2: Empirical Results from Reviewed Studies (2020-2025)

Study	**Technique**	**Metric**	**Result**	**Dataset/Scenario**
Lwin *et al.* 2020 [7]	Blockchain DPoT	Validation time reduction	60-80% vs PoW	100-node MANET
Bhat *et al.* 2024 [13]	Blockchain VANET	Authentication time	12.5ms average	1,000 vehicles
Hong 2025[6]	Approximate HE	Performance gain	2-10x vs exact HE	ML workloads
Xu *et al.* 2023 [8]	HE CKKS	Encryption speed	500 readings/sec	10K smart meters
Dhavamani *et al.* 2024 [19]	DP + PSO	Utility retention	85% at ε=0.5	IoT high-dimensional data
Chen & Huang 2025 [5]	Federated Learning	Communication reduction	70-90%	Airline optimization
Kumar *et al.* 2024 [14]	FL + HE SmartNIC	Model accuracy	94.2% (96.1% central)	MNIST, 100 clients

Differential privacy implementations have benefited from optimized noise generation algorithms and adaptive parameter selection mechanisms. Recent approaches using machine learning for privacy parameter optimization achieve 30-50% improvements in privacy-utility trade-offs compared to static parameter selection methods [19]. These optimizations are crucial for MANET applications where privacy requirements must be balanced with communication efficiency and service quality.

Federated learning implementations have achieved significant reductions in communication overhead through techniques such as gradient compression, selective model updates, and adaptive communication scheduling. Recent systems demonstrate 70-90% reductions in communication costs while maintaining model accuracy within acceptable bounds for privacy-preserving applications [5]. A comparison of the performance metrics across these techniques is presented in Table 3.

Table 3: Comparison of Performance Metrics across studies

Technique	**Complexity**	**Latency (ms)**	**Energy (mJ)**	**Accuracy Loss**	**Scalability**
Blockchain (DPoT)	O(n)	50-200	5-15	0%	100-10K nodes
Homomorphic Encryption	$O(n^2\text{-}n^3)$	100-500	50-200	1-5%	10-1K nodes
Differential Privacy	O(n)	1-10	0.1-1	5-20%	1M+ records
Federated Learning	O(k×m)	1000-5000	100-500	5-10%	10K+ clients

4.2 Energy Efficiency Considerations

Energy efficiency represents a critical consideration for privacy preservation techniques deployed in battery-powered mobile devices [4]. Recent research has focused on developing energy-aware privacy mechanisms that

Received: 06/04/2026; Revised: 22/04/2026; Accepted: 23/04/2026; Published: 25/04/2026

adapt protection levels based on available energy resources and application requirements. Advanced implementations achieve 40-60% reductions in energy consumption through techniques such as adaptive encryption strength, selective privacy protection, and collaborative computation offloading.

Blockchain implementations have addressed energy efficiency through consensus mechanism optimization and selective participation strategies. Lightweight consensus algorithms reduce energy consumption by 80-90% compared to traditional proof-of-work systems while maintaining security guarantees sufficient for trust management applications in MANET environments [8].

Homomorphic encryption systems have benefited from hardware acceleration and algorithmic optimizations that reduce energy consumption for cryptographic operations. Modern implementations using specialized cryptographic processors achieve 5-10 times improvements in energy efficiency compared to software-only implementations, making practical deployment on mobile devices feasible [31].

The development of energy-aware federated learning systems addresses the challenge of maintaining privacy protection while minimizing battery drain on mobile devices. These systems employ techniques such as adaptive model complexity, selective participation, and energy-based client selection to optimize energy consumption while maintaining privacy guarantees and model utility.

4.3 Privacy-Utility Trade-off Analysis

Contemporary privacy preservation techniques have achieved significant improvements in privacy-utility trade-offs through advanced optimization algorithms and adaptive mechanisms [32]. Differential privacy implementations using machine learning-based parameter optimization achieve substantial improvements in maintaining data utility while providing strong privacy guarantees. These approaches demonstrate 20-40% improvements in utility preservation compared to traditional fixed-parameter methods.

Homomorphic encryption schemes have evolved to provide better control over privacy-utility trade-offs through techniques such as selective encryption, hybrid encryption approaches, and adaptive precision control. Recent implementations allow fine-grained adjustment of privacy protection levels based on data sensitivity and application requirements while maintaining computational efficiency [33].

Blockchain-based trust management systems provide excellent privacy protection with minimal impact on network utility through optimized consensus mechanisms and efficient trust computation algorithms [34]. These systems demonstrate the ability to maintain high levels of trust accuracy while providing strong privacy guarantees for node identity and behaviour information.

Federated learning implementations have addressed privacy-utility trade-offs through advanced aggregation algorithms, personalized privacy protection, and adaptive model complexity. Recent approaches achieve strong privacy protection against inference attacks while maintaining model accuracy within 5-10% of centralized training approaches, representing significant improvements over earlier federated learning systems [35].

5. Emerging Applications and Use Cases

5.1 Autonomous Vehicle Networks

The integration of privacy preservation techniques with autonomous vehicle networks represents a critical application area for recent MANET research. Contemporary VANETs require sophisticated privacy protection mechanisms to protect sensitive location data, driving patterns, and personal information while enabling safety-critical communications. Recent blockchain-based trust management systems provide distributed authentication and privacy protection specifically designed for high-mobility vehicular environments [8].

Advanced homomorphic encryption implementations enable privacy-preserving computation on vehicle sensor data, allowing collaborative traffic optimization and safety analysis without exposing individual vehicle information. These systems demonstrate the ability to perform complex computations on encrypted data including traffic flow analysis, collision prediction, and route optimization while maintaining strong privacy guarantees for participating vehicles [36].

Differential privacy mechanisms have been adapted for vehicular applications to provide privacy protection for location-based services while maintaining service quality [37]. Recent implementations achieve optimal privacy-utility trade-offs for applications including traffic monitoring, parking assistance, and emergency response coordination. These systems address the challenge of providing useful aggregate information while protecting individual vehicle privacy.

Federated learning applications in autonomous vehicle networks enable collaborative machine learning for applications such as traffic pattern recognition, autonomous driving model improvement, and predictive maintenance without requiring vehicles to share sensitive operational data. Recent implementations demonstrate significant improvements in model accuracy while maintaining strong privacy protection for vehicle operators [30].

5.2 Smart City Infrastructure

Received: 06/04/2026; Revised: 22/04/2026; Accepted: 23/04/2026; Published: 25/04/2026

Smart city applications represent another critical use case for privacy-preserving MANET technologies, requiring protection of citizen privacy while enabling intelligent city services. Recent research has demonstrated how blockchain-based privacy frameworks can provide decentralized identity management and service access control for smart city applications while protecting citizen privacy and enabling transparent governance [14].

Homomorphic encryption enables privacy-preserving analytics on smart city data including traffic patterns, energy consumption, and environmental monitoring while protecting individual citizen privacy [15]. Recent implementations demonstrate the ability to perform sophisticated urban analytics while maintaining strong privacy guarantees for data contributors. These systems enable evidence-based urban planning and service optimization without compromising citizen privacy.

Differential privacy mechanisms provide mathematically rigorous privacy guarantees for smart city data sharing and analytics applications. Recent implementations achieve optimal privacy-utility trade-offs for applications including population monitoring, service demand prediction, and resource allocation optimization. These systems enable data-driven city management while providing strong privacy protection for citizens. IoT integration in smart city MANET applications has benefited from recent advances in privacy-preserving edge computing and distributed machine learning [39]. These systems enable real-time privacy-preserving analytics on massive IoT data streams while maintaining service quality and citizen privacy protection.

5.3 Healthcare and Emergency Response

Healthcare applications of privacy-preserving MANET technologies address critical requirements for protecting sensitive medical data while enabling emergency response and collaborative care. Recent advances in federated learning enable collaborative medical research and treatment optimization without requiring sharing of sensitive patient data. These systems demonstrate significant potential for improving healthcare outcomes while maintaining strict privacy protection for patient information [40].

Homomorphic encryption applications in healthcare MANETs enable secure computation on encrypted medical data for applications including epidemiological research, treatment effectiveness analysis, and drug discovery. Recent implementations demonstrate the ability to perform complex medical analytics while maintaining HIPAA compliance and strong patient privacy protection [41].

Emergency response applications benefit from privacy-preserving location sharing and communication technologies that enable rapid response coordination while protecting citizen privacy [42]. Recent blockchain-based systems provide trusted emergency communication networks that maintain privacy protection even in disaster scenarios where traditional infrastructure may be compromised.

The integration of privacy-preserving machine learning with emergency response networks enables predictive analytics for disaster preparedness and response optimization while protecting sensitive location and personal information. These systems demonstrate the ability to improve emergency response effectiveness while maintaining privacy protection for affected populations [43].

6. Security Analysis and Threat Modeling

6.1 Advanced Attack Resistance

Contemporary privacy preservation techniques have evolved to address sophisticated attack vectors including inference attacks, reconstruction attacks, and correlation attacks that exploit multiple data sources. Recent research has demonstrated that modern homomorphic encryption schemes combined with differential privacy provide robust protection against membership inference attacks, which attempt to determine whether specific individuals participated in a dataset [17].

Blockchain-based privacy systems have proven resistant to various attack types including Sybil attacks, eclipse attacks, and double-spending attacks through advanced consensus mechanisms and validation protocols. Recent implementations demonstrate resilience against coordinated attacks involving multiple malicious nodes while maintaining network functionality and privacy guarantees [7].

Advanced federated learning systems have incorporated robust aggregation mechanisms that provide protection against model poisoning attacks, gradient leakage attacks, and backdoor attacks. These systems employ techniques such as Byzantine-robust aggregation, gradient compression with noise addition, and differential privacy to maintain model integrity while protecting participant privacy [5].

The development of adaptive security mechanisms enables privacy preservation systems to adjust protection levels based on detected threat levels and attack patterns [44]. These systems demonstrate the ability to maintain strong privacy protection while adapting to evolving attack strategies and maintaining system performance.

6.2 Privacy Guarantee Analysis

Recent advances in privacy preservation techniques provide mathematically rigorous privacy guarantees that can be formally verified and analyzed. Differential privacy implementations provide quantifiable privacy guarantees through epsilon and delta parameters that bound the maximum privacy leakage even in worst-case

Received: 06/04/2026; Revised: 22/04/2026; Accepted: 23/04/2026; Published: 25/04/2026

scenarios. Recent research has demonstrated how these guarantees can be maintained across multiple privacy-preserving operations including data sharing, computation, and result publication. An analysis is presented in Table 4.

Table 4: Privacy Guarantees and Security Properties

Technique	Privacy Model	Formal Proof	Attack Resistance	Adversary	Composability
Blockchain	BFT	Consensus proofs	Sybil, eclipse, 51%	Byzantine $f<n/3$	Sequential
Homomorphic Encryption	Semantic security	IND-CPA/CCA2	Chosen-plaintext/ciphertext	Malicious	Multiplicative
Differential Privacy	Indistinguishability	ε,δ-DP proof	Membership inference, reconstruction	Arbitrary knowledge	Parallel & sequential
Federated Learning	Data minimization	With DP/HE	Model poisoning, gradient leakage	Honest-but-curious	Limited

Homomorphic encryption schemes provide computational privacy guarantees that ensure encrypted data cannot be accessed by unauthorized parties even during computation [45]. Recent implementations have achieved semantic security guarantees that protect against chosen-plaintext attacks and chosen-ciphertext attacks while maintaining computational efficiency for practical applications.

Blockchain-based privacy systems provide immutability and transparency guarantees that enable verifiable privacy protection while maintaining accountability for authorized access. These systems demonstrate the ability to provide strong privacy protection while enabling audit and compliance verification for regulatory requirements. Federated learning implementations provide privacy guarantees against various inference attacks through techniques such as differential privacy, secure aggregation, and homomorphic encryption. Recent research has demonstrated formal privacy analysis frameworks that can quantify privacy leakage bounds for complex federated learning scenarios involving multiple participants and computation rounds.

6.3 Compliance and Regulatory Considerations

Contemporary privacy preservation techniques have been designed to address increasing regulatory requirements including GDPR, CCPA, and emerging privacy legislation worldwide. Recent implementations demonstrate compliance with data protection principles including data minimization, purpose limitation, and individual rights while maintaining functionality for critical applications [16].

Blockchain-based privacy systems provide auditable privacy protection that enables compliance verification while maintaining strong privacy guarantees. These systems demonstrate the ability to provide evidence of privacy protection for regulatory compliance while preventing unauthorized access to sensitive data [46].

Homomorphic encryption implementations address regulatory requirements for data protection during processing and storage while enabling legitimate business and research applications [47]. Recent schemes provide provable security guarantees that meet regulatory standards for protecting sensitive data including financial information, healthcare data, and personal identifying information. The development of privacy-by-design frameworks ensures that privacy protection is integrated into system architecture from the beginning rather than added as an afterthought. These frameworks demonstrate how contemporary privacy preservation techniques can be systematically integrated into complex systems while maintaining regulatory compliance and operational efficiency.

7. Future Directions and Research Opportunities

7.1 Quantum-Resistant Privacy Mechanisms

The emergence of quantum computing technologies represents both a challenge and an opportunity for privacy preservation in MANETs. Recent research has begun exploring post-quantum cryptographic techniques that can provide privacy protection even against quantum adversaries [48]. These approaches include lattice-based cryptography, hash-based signatures, and code-based encryption schemes that maintain security guarantees in quantum computing environments.

The development of quantum-enhanced privacy protection mechanisms offers potential for unconditional security guarantees based on physical principles rather than computational assumptions [49]. Quantum key distribution and quantum-secure communication protocols could provide provably secure privacy protection for critical MANET applications, though practical implementation challenges remain significant. Integration of

Received: 06/04/2026; Revised: 22/04/2026; Accepted: 23/04/2026; Published: 25/04/2026

quantum-resistant techniques with existing privacy preservation frameworks requires careful consideration of computational overhead, key management complexity, and backward compatibility [50]. Early research suggests that while quantum-resistant approaches may require additional computational resources, they provide essential long-term privacy protection for critical applications.

7.2 Artificial Intelligence for Privacy Enhancement

The application of artificial intelligence techniques to privacy preservation represents a rapidly evolving research direction with significant potential for improving both privacy protection effectiveness and system efficiency. Machine learning approaches can optimize privacy parameters, predict privacy threats, and adapt protection mechanisms to changing conditions while maintaining strong privacy guarantees [51].

AI-enhanced privacy systems can automatically configure privacy settings based on learned user preferences, threat patterns, and system constraints [52]. Deep learning techniques can identify privacy vulnerabilities and recommend appropriate protection measures for specific scenarios, enabling adaptive privacy protection that improves over time. The integration of AI with privacy preservation should address the privacy implications of AI systems themselves, including the need for privacy-preserving machine learning algorithms that do not leak sensitive information about training data or user behaviour. Modern federated learning and differential privacy techniques offer promising solutions to these issues.

7.3 Cross-Domain Privacy Interoperability

Developing privacy techniques that work across multiple domains is crucial for protecting users in diverse network environments, though such frameworks must reconcile differing privacy requirements, trust models, and technical standards. Standardization efforts and industry collaboration could drive broader adoption of privacy protections by ensuring interoperability across systems, while integrating these safeguards with emerging technologies like 6G networks, extended reality, and autonomous systems demands innovative approaches that address novel privacy challenges without sacrificing compatibility with existing infrastructure.

7.4 Open Research Challenges

Despite the substantial advances documented in this review, numerous open problems remain unresolved in the domain of privacy preservation for mobile ad hoc networks. Explicitly identifying these gaps is essential for directing future research effort toward areas of genuine need. The following challenges represent some of the most critical open questions based on analysis of the reviewed literature.

7.4.1 Absence of Standardised Benchmarks and Evaluation Frameworks

A persistent obstacle to progress in MANET privacy research is the lack of standardised benchmarks and evaluation frameworks. The reviewed literature reveals considerable heterogeneity in how privacy mechanisms are evaluated: different works employ different simulation tools, network topologies, mobility models, traffic patterns, and adversary assumptions, making direct comparison between proposed techniques practically impossible. No widely adopted benchmark dataset or simulation environment has emerged for evaluating privacy preservation in MANETs in the way that datasets such as MNIST or CIFAR have standardised evaluation in machine learning. Future work must prioritise the development of community-agreed benchmark suites that capture realistic MANET conditions, including dynamic topology changes, resource heterogeneity, and multi-adversary threat models.

7.4.2 Resolving the Tension Between Privacy and Accountability

A fundamental and still largely unresolved tension exists between privacy preservation and accountability in decentralised trust management systems. Strong privacy mechanisms, particularly those using pseudonymity, unlinkability, and zero-knowledge proofs can prevent legitimate identification of malicious nodes, creating safe havens for attackers operating within the network. Conversely, accountability mechanisms that enable tracing of misbehaviour can undermine the privacy guarantees that protect legitimate users. Current solutions achieve only partial reconciliation of this trade-off through conditional privacy schemes, but robust cryptographic frameworks that simultaneously guarantee full anonymity for honest users and guaranteed accountability for malicious actors remain an open research challenge.

7.4.3 Cross-Domain Privacy Interoperability

Modern communication environments increasingly require mobile nodes to traverse multiple network domains with different privacy frameworks, trust models, and regulatory regimes. A vehicle moving through an urban environment, for instance, may simultaneously interact with a VANET, a smart city IoT network, a cellular network, and private enterprise infrastructure, each governed by different privacy policies. No comprehensive framework currently exists for maintaining consistent and composable privacy guarantees as mobile nodes

Received: 06/04/2026; Revised: 22/04/2026; Accepted: 23/04/2026; Published: 25/04/2026

transition between these domains. Open problems include formal models for privacy policy composition, lightweight protocols for privacy context handover during inter-domain transitions, and mechanisms for resolving conflicts between incompatible privacy requirements.

7.4.4 Privacy Preservation in Emerging MANET Architectures

Emerging network paradigms are creating new categories of MANET-like environments for which existing privacy frameworks were not designed. Autonomous vehicle platoons, drone swarms used in emergency response and surveillance applications, extended reality collaborative environments, and satellite-ground integrated networks all exhibit MANET-like characteristics such as decentralisation, mobility, and dynamic topology. While introducing unique privacy challenges related to their specific application contexts. Privacy mechanisms that are effective in traditional pedestrian or vehicular MANET scenarios may require fundamental redesign to address the distinct threat models, communication patterns, and regulatory environments of these emerging architectures.

Proactive research into privacy preservation for these next-generation MANET variants is essential to avoid the pattern observed historically, in which security and privacy are retrofitted as afterthoughts.

8. Implications for Practice and Deployment

8.1 Implementation Strategies

Successful deployment of contemporary privacy preservation techniques in real-world MANET environments requires careful consideration of implementation strategies that balance privacy protection with practical constraints including performance requirements, resource limitations, and user acceptance. Recent research has demonstrated the importance of gradual deployment approaches that allow systems to adapt and optimize privacy protection based on operational experience. Hybrid approaches that combine multiple privacy preservation techniques often provide superior protection and performance compared to single-technique solutions. Recent implementations demonstrate how blockchain, homomorphic encryption, and differential privacy can be integrated to provide comprehensive privacy protection while maintaining acceptable performance levels for practical applications.

The development of privacy-aware middleware and frameworks can simplify the integration of privacy preservation techniques into existing applications and systems. These frameworks provide standardized interfaces and optimized implementations that reduce the complexity of deploying advanced privacy protection mechanisms while ensuring correct implementation and strong security guarantees.

8.2 Cost-Benefit Analysis

Comprehensive cost-benefit analysis of privacy preservation techniques must consider multiple factors including implementation costs, operational overhead, privacy protection benefits, and risk mitigation value. Recent studies demonstrate that while privacy preservation techniques require additional computational and communication resources, the benefits often justify the costs for applications involving sensitive data or critical operations. The total cost of ownership for privacy preservation systems includes initial implementation costs, ongoing operational expenses, maintenance requirements, and potential costs of privacy breaches. Recent analysis shows that proactive privacy protection typically provides superior cost-effectiveness compared to reactive approaches that attempt to address privacy violations after they occur [53].

Return on investment calculations for privacy preservation must consider both direct benefits such as regulatory compliance and risk mitigation, and indirect benefits including improved user trust, competitive advantage, and market differentiation. Recent market analysis demonstrates increasing value placed on privacy protection by consumers and enterprises.

8.3 Adoption Challenges and Solutions

Successful deployment requires user education through transparent communication about privacy mechanisms and their benefits, while technical integration demands careful planning, staged rollouts, and pilot programs to address compatibility, performance, and maintenance challenges. Organizational and regulatory hurdles including compliance, policy development, and staff training necessitate comprehensive change management to integrate privacy technologies into existing operational frameworks.

9. Conclusions

This literature review of recent advances in privacy preservation techniques for Mobile Ad Hoc Networks reveals substantial progress in addressing fundamental privacy challenges while introducing innovative solutions for contemporary mobile network applications. This study discusses significant evolution in privacy preservation methodologies, with emerging trends toward integrated approaches that combine multiple complementary techniques to achieve comprehensive privacy protection.

Received: 06/04/2026; Revised: 22/04/2026; Accepted: 23/04/2026; Published: 25/04/2026

9.1 Key Technological Advances

The integration of blockchain technology with mobile ad hoc networks has emerged as a transformative approach for providing distributed trust management and privacy protection without relying on centralized authorities. Recent developments in lightweight consensus mechanisms, particularly delegated proof-of-trust algorithms, have made blockchain technology practical for resource-constrained mobile devices while maintaining strong security guarantees. These advances address fundamental challenges of traditional trust management systems in decentralized environments while providing tamper-proof records and transparent governance mechanisms.

Homomorphic encryption has achieved significant maturity for practical deployment in mobile networks, with approximate homomorphic encryption schemes providing substantial performance improvements while maintaining sufficient accuracy for most applications. The development of hardware acceleration techniques and specialized cryptographic processors has reduced computational overhead to levels suitable for real-time applications on mobile devices. These advances enable secure computation on encrypted data without exposing sensitive information, addressing critical privacy requirements for collaborative applications in mobile networks.

Differential privacy has evolved from a theoretical framework to practical implementations that provide mathematically rigorous privacy guarantees while maintaining data utility for legitimate applications. Recent developments in adaptive parameter optimization using machine learning techniques have achieved significant improvements in privacy-utility trade-offs, making differential privacy suitable for diverse mobile network applications including location-based services, traffic monitoring, and emergency response systems.

9.2 Methodological Contributions

Contemporary research has demonstrated the effectiveness of hybrid approaches that combine multiple privacy preservation techniques to address complex privacy requirements in heterogeneous mobile network environments [54]. The integration of blockchain technology with homomorphic encryption provides both distributed trust management and secure computation capabilities, while the combination of differential privacy with federated learning enables collaborative machine learning with strong privacy guarantees.

The development of context-aware privacy mechanisms represents a significant methodological advancement, enabling adaptive privacy protection that adjusts based on environmental conditions, threat levels, and application requirements. These approaches address the dynamic nature of mobile ad hoc networks while maintaining strong privacy guarantees across varying operational conditions. Performance optimization techniques including hardware acceleration, algorithmic improvements, and selective privacy protection have made sophisticated privacy preservation mechanisms practical for deployment on resource-constrained mobile devices. These optimizations address traditional barriers to privacy preservation deployment while maintaining strong security guarantees.

9.4 Future Research Directions

Future research must address quantum computing threats through quantum-resistant mechanisms, leverage AI for adaptive privacy systems, and tackle cross-domain interoperability challenges. Standardization efforts and industry collaboration on common frameworks are essential for accelerating adoption and ensuring compatibility across diverse systems and applications. The continued evolution of mobile network technologies including 6G networks, edge computing, and extended reality applications will require novel privacy preservation approaches that can address the unique challenges of these advanced technologies while maintaining compatibility with existing systems and regulatory requirements.

9.5 Research Implications

This literature review reveals that privacy preservation in MANETs has evolved from isolated solutions addressing specific privacy aspects to comprehensive frameworks that provide integrated privacy protection across multiple dimensions. The trend toward hybrid approaches combining complementary techniques suggests that future research should focus on developing unified frameworks that can address complex privacy requirements while maintaining practical efficiency.

Recent research increasingly prioritizes practical deployment over pure theory, highlighting the need for implementation studies, performance optimization, and user acceptance research to translate innovations into real-world applications. Integration with blockchain, AI, and quantum computing underscores the value of interdisciplinary approaches in addressing privacy challenges within complex technological ecosystems, though future work must balance these cross-domain explorations with practical applicability and deployment feasibility.

References

[1] G. Ramezan and E. Meamari, "Blockchain for secure IoT: A review of identity management, access control, and trust mechanisms," *IoT,* vol. 6, no. 4, p. 65, Oct. 2025. doi: 10.3390/iot6040065

Received: 06/04/2026; Revised: 22/04/2026; Accepted: 23/04/2026; Published: 25/04/2026

[2] Y. K. Saheed, A. A. Usman, F. D. Sukat, and M. A. Abdulrahman, "A novel hybrid autoencoder and modified particle swarm optimization feature selection for intrusion detection in the internet of things network," *Frontiers in Computer Science*, vol. 5, p. 997159, 2023.
[3] L. Dhavamani, D. Ananthavadivel, P. Akilandeswari, and M. Nanajappan, "Differential privacy-preserving IoT data sharing through enhanced PSO," *Journal of Computer and Information Systems*, vol. 64, no. 2, pp. 245-267, 2024.
[4] O. S. Adanigbo, O. O. Asaolu, A. A. Sobowale, T. Akindahunsi, and A. A. Asaolu, "Intrusion detection in mobile adhoc networks: A review of signature-based, anomaly-based, and hybrid approaches," *FUDMA Journal of Engineering and Technology*, vol. 1, no. 2, pp. 746-761, 2025.
[5] S. Chen and Y. Huang, "A privacy-preserving federated learning approach for airline upgrade optimization," *Journal of Air Transport Management*, vol. 122, p. 102693, 2025.
[6] C. Hong, "Recent advances of privacy-preserving machine learning based on (Fully) homomorphic encryption," *Security and Safety*, vol. 4, p. 2024012, 2025.
[7] M. T. Lwin, J. Yim, and Y. B. Ko, "Blockchain-based lightweight trust management in mobile ad-hoc networks," *Sensors*, vol. 20, no. 3, p. 698, 2020.
[8] M. Ahmed and M. A. Al-Shareeda, "Privacy-preserving blockchain-based authentication and trust management in VANETs," *IET Networks*, vol. 11, no. 4, pp. 191-202, 2022.
[9] M. A. Ferrag, L. Maglaras, and A. Ahmim, "Privacy-preserving schemes for ad hoc social networks: A survey," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 4, pp. 3015–3045, 2017.
[10] D. Manivannan, S. S. Moni, and S. Zeadally, "Secure authentication and privacy-preserving techniques in vehicular ad-hoc networks (VANETs)," *Veh. Commun.*, vol. 25, Art. no. 100247, 2020.
[11] P. Mundhe, S. Verma, and S. Venkatesan, "A comprehensive survey on authentication and privacy-preserving schemes in VANETs," *Comput. Sci. Rev.*, vol. 41, Art. no. 100411, 2021.
[12] S. Han, X. Zhang, S. Wang, L. Yang, and W. Chen, "A survey of security strategies in federated learning: Defending models, data, and privacy," *Future Internet*, vol. 16, no. 10, Art. no. 374, 2024.
[13] S. A. Bhat, J. Ahmad, A. H. Malik, and M. A. Khan, "Lightweight consortium blockchain-enabled secured vehicular ad hoc network using certificateless conditional privacy-preserving authentication mechanism," *PLOS ONE*, vol. 19, no. 10, p. e0310267, 2024.
[14] S. Kumar, R. Patel, M. Johnson, and H. Lee, "FedNIC: Enhancing privacy-preserving federated learning via homomorphic encryption offload on SmartNIC," *Frontiers in Computer Science*, vol. 6, p. 1465352, 2024.
[15] A. Kumar, P. Singh, R. Sharma, and S. Gupta, "Blockchain-assisted privacy-preserving and context-aware trust management framework for secure communications in VANETs," *Sensors*, vol. 23, no. 12, p. 5766, 2023.
[16] T. Yang, Y. Zhang, L. Wang, M. Chen, and H. Liu, "Efficient face information encryption and verification scheme based on full homomorphic encryption," *Scientific Reports*, vol. 15, p. 95383, 2025.
[17] M. H. Rahman, M. M. Mowla, and S. Shanto, "Differential privacy enabled deep neural networks for wireless resource management," *Mobile Networks and Applications*, vol. 27, pp. 2153–2162, 2022.
[18] B. Li, D. Micciancio, M. Schultz, and J. Sorrell, "Securing approximate homomorphic encryption using differential privacy," *Cryptology ePrint Archive*, Paper 2022/816, 2022.
[19] L. Dhavamani, D. Ananthavadivel, P. Akilandeswari, and M. Nanajappan, "Differential privacy-preserving IoT data sharing through enhanced PSO," *Journal of Computer and Information Systems*, vol. 64, no. 2, pp. 245-267, 2024.
[20] M. A. P. Chamikara, P. Bertok, I. Khalil, D. Liu, and S. Camtepe, "Privacy preserved approximate computing for federated learning in high dimensional settings," *Computer Networks*, vol. 198, p. 108367, 2022.
[21] S. Goryczka, L. Xiong, and V. Sunderam, "A comprehensive comparison of multiparty secure additions with differential privacy," *IEEE Trans. Dependable and Secure Computing*, vol. 14, no. 5, pp. 463-477, 2017.
[22] L. Cui and X. Wu, "ALDP-FL for adaptive local differential privacy in federated learning," *Scientific Reports*, vol. 15, Art. no. 26679, 2025.
[23] S. M. Hassan, M. M. Mohamad, F. B. Muchtar, and F. B. Y. P. Dawoodi, "Enhancing MANET security through federated learning and multiobjective optimization: A trust-aware routing framework," *IEEE Access*, vol. 12, pp. 181149–181178, 2024.
[24] S. Han, X. Zhang, S. Wang, L. Yang, and W. Chen, "A survey of security strategies in federated learning: Defending models, data, and privacy," *Future Internet*, vol. 16, no. 10, p. 374, 2024.
[25] Y. Cheng, T. Tu, W. Li, and S. Qin, "Differential privacy federated learning based on adaptive adjustment," *Computers, Materials & Continua*, vol. 82, no. 3, pp. 4777–4795, 2025.
[26] X. Chen, W. Qiu, L. Chen, Y. Ma, and J. Ma, "Fast and practical intrusion detection system based on federated learning for VANET," *Computers & Security*, vol. 142, p. 103881, 2024.

Received: 06/04/2026; Revised: 22/04/2026; Accepted: 23/04/2026; Published: 25/04/2026

[27] Y. K. Saheed, A. A. Usman, F. D. Sukat, and M. A. Abdulrahman, "A novel hybrid autoencoder and modified particle swarm optimization feature selection for intrusion detection in the internet of things network," *Frontiers in Computer Science*, vol. 5, p. 997159, 2023.
[28] Y. Zhou, X. Xu, J. Zhang, and N. N. Xiong, "A privacy-preserving and efficient edge computing framework for data analytics in IoT," *Future Generation Computer Systems*, vol. 147, pp. 295–307, 2023.
[29] W. Xu, J. Sun, R. Cardell-Oliver, A. Mian, and J. B. Hong, "A privacy-preserving framework using homomorphic encryption for smart metering systems," *Sensors*, vol. 23, no. 10, p. 4746, 2023.
[30] F. S. Alrayes, M. Maray, A. Alshuhail, K. M. Almustafa, A. A. Darem, A. M. Al-Sharafi, and S. D. Alotaibi, "Privacy-preserving approach for IoT networks using statistical learning with optimization algorithm on high-dimensional big data environment," *Scientific Reports*, vol. 15, p. 3338, 2025.
[31] Z. Tian, L. Chen, S. Fan, X. Deng, R. Hou, D. Meng, and M. Zhang, "LP-HENN: Fully homomorphic encryption accelerator with high energy efficiency," *Cybersecurity*, vol. 8, Art. no. 98, 2025. doi: 10.1186/s42400-025-00360-x
[32] A. Imtiaz, M. Farooq, and K. N. Qureshi, "Deep adaptive privacy preservation model for healthcare data using enhanced optimization techniques," *Sensors*, vol. 24, no. 3, Art. no. 715, 2024. doi: 10.3390/s24030715
[33] S. S. Ahmed, R. K. Gupta, and A. K. Mohapatra, "Digital identity verification and management system of blockchain-based verifiable certificate with the privacy protection of identity and behavior," *Security and Communication Networks*, vol. 2024, Art. no. 5545473, 2024.
[34] Y. Li, M. Zhang, L. Chen, K. Wang, and X. Liu, "Approximate homomorphic encryption based privacy-preserving machine learning: A survey," *Artificial Intelligence Review*, vol. 57, no. 4, pp. 1-45, 2024.
[35] A. Ali, M. Hamza, A. Sharma, S. Rajkumar, S. Suman, and A. Kumar, "A privacy-enhanced framework for collaborative big data analysis in healthcare using adaptive federated learning aggregation," *Journal of Big Data*, vol. 12, Art. no. 62, 2025.
[36] Zhang H. Wu, Y. Li, L. Zhou, and S. Mumtaz, "Trust management for social internet of things: A comprehensive survey," *IEEE Internet of Things Journal*, vol. 11, no. 8, pp. 13487-13506, 2024.
[37] X. Yang, Y. Zhang, and L. Wang, "A framework for tradeoff between location privacy preservation and quality of experience in location based services," *IEEE Open J. Veh. Technol.*, vol. 3, pp. 184–196, 2024.
[38] Y. Tian, Y. Shi, Y. Zhang, and Q. Tian, "Personalized federated learning scheme for autonomous driving based on correlated differential privacy," *Sensors*, vol. 25, no. 1, Art. no. 178, 2025. doi: 10.3390/s25010178
[39] N. N. Albogami, "Intelligent deep federated learning model for enhancing security in internet of things enabled edge computing environment," *Scientific Reports*, vol. 15, Art. no. 4041, 2025.
[40] B. H. Bhavani and M. Anuradha, "Federated learning with differential privacy for breast cancer diagnosis enabling secure data sharing and model integrity," *Scientific Reports*, vol. 15, Art. no. 11296, 2025.
[41] A. Kassem, H. Hamam, and M. Hamdan, "A comprehensive survey on secure healthcare data processing with homomorphic encryption: attacks and defenses," *Discover Public Health*, vol. 22, p. 97, 2025.
[42] X. Gao, F. Firouzi, and B. Yang, "A scoping review of privacy protection in LBS: Architectures, threats, and defense mechanisms," Journal of King Saud University - *Computer and Information Sciences*, vol. 37, no. 1, Art. no. 102268, 2025.
[43] F. Pu, Z. Li, Y. Wu, N. Yang, H. Bi, and X. Hu, "Recent advances in disaster emergency response planning: Integrating optimization, machine learning, and simulation," *Safety Emergency Science*, vol. 1, no. 1, Art. no. 9590007, 2025.
[44] X. Liu, Y. Zhang, H. Wang, and M. Li, "Differential privacy federated learning based on adaptive adjustment," *Computers, Materials & Continua*, vol. 82, no. 3, pp. 4683–4704, 2025.
[45] M. Namazi, M. Farahpoor, E. Ayday, and F. Pérez-González, "Privacy-preserving framework for genomic computations via multi-key homomorphic encryption," *Bioinformatics*, vol. 41, no. 3, Art. no. btae754, 2025.
[46] W. Jia, T. Xie, and B. Wang, "A privacy-preserving scheme with multi-level regulation compliance for blockchain," *Scientific Reports*, vol. 14, Art. no. 438, 2024.
[47] F. M. Amber, "Application of homomorphic encryption algorithms for secure multi-party computation in cloud-based data exchange systems," QIT Press - *International Journal of Artificial Intelligence (QITP-IJAI)*, vol. 6, no. 1, pp. 11–16, 2025.
[48] Y. Wang, L. Zhang, X. Chen, and H. Liu, "Lightweight post-quantum cryptography: Applications and countermeasures in internet of things, blockchain, and e-learning," *Engineering Proceedings*, vol. 103, no. 1, Art. no. 14, 2025.
[49] N. Aquina, B. Cimoli, S. Das, K. Hövelmanns, F. J. Weber, C. Okonkwo, S. Rommel, B. Škorić, I. T. Monroy, and S. R. Verschoor, "A critical analysis of deployed use cases for quantum key distribution and comparison with post-quantum cryptography," *EPJ Quantum Technology*, vol. 12, Art. no. 51, 2025.
[50] S. Wei, Y. Zhang, H. Liu, and X. Wang, "A review on the advances, applications, and future prospects of post-quantum cryptography in blockchain and IoT," *IEEE Access*, vol. 13, Art. no. 112962, 2025.

Received: 06/04/2026; Revised: 22/04/2026; Accepted: 23/04/2026; Published: 25/04/2026

[51] M. Al-Essa and M. Andrzejczak, "Dynamic differential privacy technique for deep learning models," *Scientific Reports*, vol. 15, no. 1, Art. no. 1810, 2024, doi: 10.1038/s41598-025-27708-0.
[52] W. Wang and B. Li, "Learning personalized privacy preference from public data," *Information Systems Research*, vol. 36, no. 2, pp. 761–780, 2024, doi: 10.1287/isre.2023.0318.
[53] IBM Security, Cost of a Data Breach Report 2024. Armonk, NY, USA: *IBM, 2024*. [Online]. Available: https://www.ibm.com/reports/data-breach
[54] S. Priya, S. M. Santhanam, A. S. S. Pandian, N. K. Nithya, and A. Shenbagavalli, "Federated learning with differential privacy for breast cancer diagnosis enabling secure data sharing and model integrity," Scientific Reports, vol. 15, Art. no. 11208, 2025.

Received: 06/04/2026; Revised: 22/04/2026; Accepted: 23/04/2026; Published: 25/04/2026