IEEE Open Journal of
Intelligent Transportation
Systems

Received 7 February 2025; revised 1 July 2025; accepted 28 December 2025. Date of publication 6 January 2026; date of current version 15 January 2026.

Digital Object Identifier 10.1109/OJITS.2026.3651438

Advancing IoT-Driven Transportation Security: A Comprehensive Review of Privacy-Preserving Identity-Based Encryption With Quantum Enhancements

HAFIZ MUHAMMAD WASEEM[1], NOOR MUNIR[2], AND SEONG OUN HWANG[3] (Senior Member, IEEE)

[1]Warwick Manufacturing Group, University of Warwick, CV4 7AL Coventry, U.K.
[2]Department of Engineering Sciences, University of Oxford, OX1 2JD Oxford, U.K.
[3]Department of Computer Engineering, Gachon University, Seongnam 13120, South Korea

CORRESPONDING AUTHOR: S. O. HWANG (e-mail: sohwang@gachon.ac.kr)

This work was supported by the National Research Foundation of Korea (NRF) funded by the Korean Government (Ministry of Science and ICT) under Grant RS-2024-00340882.

ABSTRACT Intelligent transportation initiatives increasingly employ extensive networks of Internet-of-Things (IoT) sensors in combination with fog-computing platforms that locate computational resources near data sources in both maritime and urban environments. Although such connectivity enhances traffic monitoring and control, it simultaneously broadens the attack surface, placing sensitive operational data at heightened risk. Identity-Based Encryption (IBE) simplifies cryptographic key management in these contexts; however, it remains constrained by key-escrow exposure and the practical complexity of securely distributing private keys. This study analyzes these limitations and evaluates the extent to which two quantum techniques, Blind Quantum Computation (BQC) and Quantum Annealing (QA), can provide effective solutions. In particular, BQC enables encrypted computation without disclosing the user's identity to the processing server, thereby substantially mitigating the key-escrow vulnerability inherent in conventional IBE deployments. Meanwhile, QA is recommended for its ability to dynamically optimize network performance and security configurations. By synthesizing recent developments, discussing challenges, and recommending quantum-enhanced solutions, this study marks a significant step towards securing and optimizing smart transportation systems through advanced cryptographic techniques and quantum computing.

INDEX TERMS Blind quantum computation, blockchain, escrow-less cryptography, identity-based encryption, IoT security, quantum annealing, smart transportation.

I. INTRODUCTION

THE SMART ocean and fog computing have aroused the interest of government, business, academia, and individuals due to the wealth of marine resources and the nodes infrastructure for communication and computation. Fog computing allows IoT devices at the edge of the network to be connected to high-end cloud servers [1], [2], [3]. These devices collect a variety of information from the sensor nodes in smart seas that can assist with underwater green transportation systems (UwGTs) [4], military intelligence gathering [5], and several human activities, such as monitoring, protection, and aquaculture [6], [7], [8]. These devices may process data, reducing application delays by storing and forwarding processed data to cloud platforms. The data needs to be shared across network users with personal identities, and blockchain technology enables the secure methods of protecting information from unauthorized modifications [9]. Each block has a distinct structure, and the chain of entire blocks maintains the system intact. The information recorded in each block cannot be modified without the majority consensus of the network's participants, and the validation process relies on algorithms and parameters included in the blocks. Blockchain infrastructure is currently

The review of this article was arranged by Associate Editor Peter Han Joo Chong.

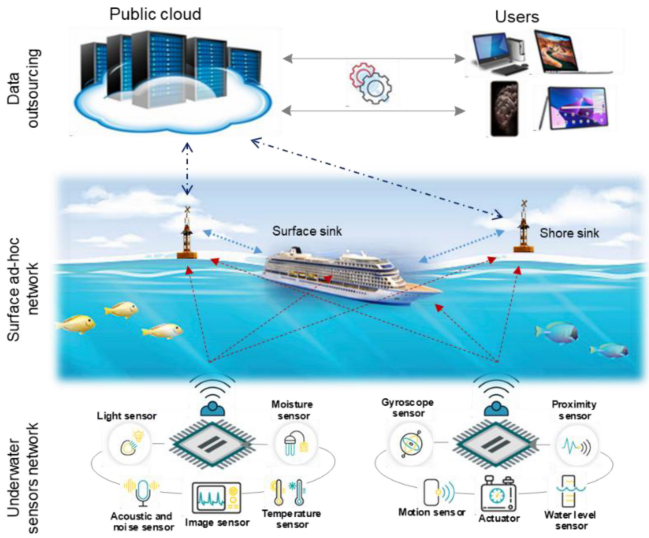

FIGURE 1. An overview of intelligent transportation systems.

being rolled out for various applications in transportation networks, such as vehicular networks [10], [11], smart oceans [12], smart cities [13], and health sectors [14], [15] by building blocks to actualize intelligent transportation systems.

The smart transportation network is composed of numerous components, as shown in **Fig. 1**. The central components of the UwGTs network are the low-cost nodes with acoustic modem accuracy, i.e., submarine sensors. These sensors can detect, process, and send data on diverse environmental parameters like aquatic habitats, temperature, pressure, and organic materials. The information needs to be transmitted to the sink [16], which is implanted at the water's surface, and then transferred to a remote monitoring center after it is received at the sink. The monitoring center, located near the coastline, is responsible for analyzing the data collected by the sensors. Sink devices capture data from sensors and transfer it to privately owned networks and cloud platforms for storage and analysis. End users can utilize the data collected by UwGTs nodes.

However, the use of these IoT devices in intelligent transportation systems poses challenges due to their limited power and memory resources. Traditional cryptographic methods based on ciphers and hash functions are not feasible for these devices in the smart network. Therefore, the primary focus should be on ensuring data security rather than the overall system's efficiency. According to recent studies conducted by Abera et al. [17] and Chen et al. [18], the physical system is highly vulnerable to malicious code injection [19], code-reuse [20], and fake data injection attacks [21]. These attacks can result into a total blackout targeting IoT devices, leading to eavesdropping, SQL injection [22], watering-hole [23], password cracking [24], [25] (by utilizing brute-force [26], birthday [27], rainbow table [28], or dictionary [29] attacks), phishing, replay, DoS/DDoS (such as Smurf [30], blackhole and BlackEnergy series [31], ping-of-death [32], teardrop [33]), malicious third-party intervention [34], malware (such as Trojan, Botnets, Rootkit, etc.), and side-channel attacks. Maintaining a secure environment for IoT devices is a formidable task owing to the tremendous growth of challenges, integration issues, and limitations of existing solutions, including security, privacy, and accuracy concerns.

Moreover, the identity of devices is also a contentious issue because the nodes in the transportation network are susceptible to cyberattacks [35]. These nodes can perceive their surroundings and adapt to and govern their physical environment [36]. This is mostly due to their adaptability and flexibility to adjust the runtime of system(s) processes via real-time computing [37]. Malicious servers or users can exploit device identity to penetrate security and access a vessel's confidential systems. NotPetya [38] is a modern illustration of this type of attack. It exploits system vulnerabilities to encrypt and disrupt data, and in some scenarios, attackers may extend such strategies to gain control of sensitive monitoring systems, including those used in maritime operations. Several factors can affect transportation systems that depend on identity information [39], [40], such as:

- Internal vulnerabilities: If a device installed on the vessel (or a monitor connected to the cloud server) is compromised, attackers can obtain recorded IDs, thereby compromising the vessel's overall security. The recent suspension of the U.S. carrier due to ECDIS strikes is an example of these types of attacks [41].
- Malware attacks: An adversary can implant malware in transportation infrastructure, allowing them to capture and control a specific vessel. An oil rig was recently captured by the cyber assailants by implanting spyware [42].
- Unauthorized access: It refers to bypassing security measures in order to gain access to a system, network, or data without authorization or permission. There have previously been various security breaches to access sensitive information, such as the Springfield station in the United States [43] utilizing a backdoor, and the Iranian infrastructure and nuclear facility information breach using Stuxnet [44].
- Availability of attacking tools for IoT devices: Due to widely available technology, anyone can initiate or carry out flooding attacks or cyber surveillance on any vessel.

This study explores the methodologies and challenges in integrating blockchain technology with IoT systems in smart transportation networks, focusing specifically on identity-based cryptography (IBC). It addresses critical issues such as the key-escrow problem, scalability limitations, and privacy concerns associated with existing authentication frameworks. To mitigate these challenges, the paper proposes a novel methodology that integrates BQC and QA within the IBE paradigm. These quantum-based techniques not only enhance data privacy and security but also optimize

resource allocation in large-scale IoT networks, such as UwGTs.

The rest of the article is structured as follows: Section II details the existing blockchain applications in smart transportation and identifies gaps in current methodologies. Section III discusses the inherent challenges of implementing IBE in resource-constrained IoT environments. Section IV introduces quantum-based solutions using BQC and QA to overcome these challenges. Section V synthesizes our findings and future research directions, and Section VI concludes the paper.

II. REVIEW OF AUTHENTICATION STRATEGIES IN SMART TRANSPORTATION SYSTEMS

There are numerous blockchain-based authentication methodologies designed to strengthen smart transportation infrastructures against malicious attacks. Collectively, these approaches seek to preserve the integrity of data in transit and to verify node identities within IoT environments while addressing the operational constraints inherent in decentralized architectures, such as limited bandwidth, heterogeneous hardware, and the lack of central trust authority. For instance, Gopinath et al. [45] proposed a cloud-based supervisory framework for continuous monitoring of the Internet of Underwater Things (IoUT); by integrating an energy-aware sensing stack with enhanced attribute-based encryption and adaptive routing, they demonstrated secure telemetry, yet their design is still limited by complex key-management procedures, propagation delay and elevated power consumption typical of subsea communication, and potential scalability problems as node density rises. Dependence on remote cloud resources may also expose the network to service interruptions unless an edge layer is introduced. In a related contribution, Yazdinejad et al. [46] used a permissionless ledger to develop a transparent, energy-efficient decentralized authentication mechanism for underwater wireless gateways. Their development integrates IoT devices in each cluster via peer-to-peer networks, thus eliminating repeated device authentication during inter-cluster transfers and enhancing throughput. However, a growing transaction volume can introduce bottlenecks, validation latency that undermines time-critical functions, and substantial energy and computational overhead despite the reported gains. Their implementation requires careful tuning of block-generation intervals and consensus difficulty to balance security with responsiveness. Gupta et al. [47] similarly presented pairing-based cryptography combined with an immutable blockchain to authenticate maritime IoT entities, recording signed transactions on-chain to prevent repudiation. However, as the overlay grows, communication overhead, single-point failure, incompatibility with established cryptographic suites, and the processing load associated with ledger maintenance remain open challenges, and the reliance on bilinear pairings can increase verification costs on resource-constrained sensors. **Table 1** highlights various authentication methodologies that utilize blockchain technologies along with their associated challenges.

While blockchain-based authentication methodologies provide robust solutions, researchers have also explored alternative approaches such as edge and fog computing, software-defined networking (SDN), and AI-based authentication strategies. Some of these approaches are discussed below:

- Hou et al. [48] introduced Vehicular Fog Computing (VFC), which leverages vehicles as infrastructure for communication and computation instead of traditional cellular networks and roadside units (RSUs). They explore using both parked and moving vehicles to pool resources across different vehicles, enhancing the quality of services and applications through distributed computing and communication. However, their model faces challenges such as scalability issues with the increasing number of vehicles and data, potential latency due to the dynamic nature of vehicular networks, and reliability concerns stemming from the variable availability of vehicles. Further challenges arise from maintaining robust security and privacy measures within decentralized networks, effectively controlling vehicular energy consumption, ensuring seamless integration with existing roadway and communication infrastructures, and addressing the complexities inherent in resource allocation across highly dynamic vehicular networks.
- Prathiba et al. [49] introduced a security-oriented framework designed explicitly for autonomous vehicles utilizing SDN combined with federated K-means clustering. Their proposed solution employs a continuously moving clustering mechanism known as MiCR to optimize the dissemination of safety-critical messages through a 5G-based Vehicle-to-Everything (V2X) communication architecture. Despite these advantages, the method remains primarily applicable to road transportation and faces notable limitations, including scalability constraints arising from growing vehicle density and data volumes, maintaining low latency and high reliability crucial for safety-oriented communications, and managing substantial communication overhead resulting from continuous data transmission. Additional concerns include considerable energy usage, integration complexities when interfacing with established transportation infrastructures, and the inherent challenges involved in managing advanced network technologies such as SDN.
- Trichili et al. [50] developed CNN-based encoding model for maritime data collection. Their approach leverages transfer learning techniques with a pre-trained neural network to expedite the training process by utilizing prior knowledge. The fundamental concept behind this method is to leverage the knowledge gained by a neural network to solve challenges in information gathering. Despite several advantages, their method, which employs CNN-based encoding combined with structured light techniques, encounters notable

TABLE 1. Methodology and challenges of blockchain integration with IoT devices.

Reference		Method Θ Challenge Δ
Aljuhani et al. [3]	Θ	Decentralized fog-computing framework that embeds blockchain-based access-control lists, providing resource provenance and data-integrity guarantees for smart-village IoT deployments.
	Δ	Blockchain layer and fog-node coordination add extra message exchange and processing at each foglet, inflating communication and computation overhead; as more edge devices join, throughput drops and latency rises, exposing scalability limits, while distributing ledgers across many fog nodes heightens privacy risk during inter-domain data flows.
Zhou et al. [4]	Θ	Identity-based signature plus lightweight hashing to authenticate underwater IoT traffic and keep an immutable, synchronized ledger across heterogeneous devices.
	Δ	The design still exposes smart-contract logic to potential misuse, and its signing/verification routines introduce measurable processing and energy overhead that rises with key length, increasing latency and limiting scalability on resource-constrained devices.
Xu et al. [6]	Θ	Customized peer-to-peer blockchain architecture tailored for ultra-low-energy foglets and designed to interoperate with, or migrate to, centrally managed IoT infrastructures.
	Δ	Scheme remains susceptible to identity- and reputation-based attacks; privacy-preserving capabilities are limited; non-deterministic consensus mechanism imposes an additional processing overhead that scales unfavorably, leading to throughput degradation as more fog nodes join the network.
Ibrar et al. [8]	Θ	Public-key infrastructure (PKI) for SDN-enabled fog networks; distributed storage; smart-contract-based synchronization.
	Δ	Incompatible with lightweight cryptographic schemes; latency and single-point-failure risk persist; path-selection adds appreciable processing overhead at the controller; scalability remains limited, as higher flow volumes still cause link congestion and disturbed flows.
Alladi et al. [10]	Θ	Broad survey of more than 75 blockchain-based security schemes for vehicular networks; analyzes PKI use within IoT/IoV devices, authentication and data-integrity techniques, and how different platforms and consensus mechanisms affect network scalability and flexibility.
	Δ	Security flaws remain unattended; consensus protocols still impose noticeable computational overhead on resource-constrained vehicles and RSUs; throughput remains far below real-time needs, so scalability is limited.
Li et al. [11]	Θ	Centralized and trustworthy Peer-to-Peer network; access control using blockchain; consensus protocol security.
	Δ	Communication overhead in IoT network; data transportation security from edge devices to public cloud is not measured; high computation complexity for node verification.
Gai et al. [12]	Θ	BP3-MTS: a blockchain-based, privacy-preserving positioning-data-sharing scheme that melds zk-SNARK proofs, Merkle commitments and smart contracts on an Ethereum-style edge network.
	Δ	zk-SNARK setup and proof generation impose noticeable processing overhead on edge nodes; block size and verification delay rise with transaction volume, straining bandwidth and storage and overlaying scalability; if an edge computing node is compromised, attackers can still analyze or tamper with transactions despite decentralization.
Gupta et al. [47]	Θ	Blockchain-based IBE scheme for maritime-IoT, enabling authenticated device interaction and immutable peer-to-peer logging of vessel data to enhance confidentiality and traceability.
	Δ	IBE computations and on-chain verification introduces noticeable cryptographic overhead for low-power sensors, and the workload escalates with message sizes or node count rise, limiting scalability under dense network traffic; typical ledger-level threats (e.g., double-spending) are not explicitly mitigated, leaving resilience gaps in high-volume settings.
Khan et al. [52]	Θ	Permissioned-blockchain framework that integrates consensus-validated blocks, secure timestamping, and IBE to protect user records within a decentralized public ledger.
	Δ	Combined consensus computation and IBE processing impose substantial computational and energy demands, thereby constraining throughput as the network scales; interoperability with resource-constrained edge devices is not demonstrated; key-update mechanism is comparatively cumbersome, delaying timely credential rotation.
Salman et al. [53]	Θ	Comprehensive survey of blockchain-based security services–encryption and authentication primitives, ACL-driven privacy control, and provenance logging–to safeguard resource and data integrity across distributed and cloud-IoT environments.
	Δ	Real-world adoption remains hindered by the significant computation and communication overhead imposed by consensus and cryptographic operations, which reduce throughput on resource-constrained IoT devices; performance degrades further as node counts and ACL update rates rise, revealing notable scalability limits; As ACL and key-management metadata are stored on-chain compromising true anonymity, leaving residual privacy vulnerabilities despite pseudonymous identifiers.
Wang et al. [54]	Θ	Decentralized, tamper-resistant ledger architecture intended to handle big-data streams from heterogeneous IoT devices while keeping integrity-maintenance costs low.
	Δ	Massive storage required; scalability and radio link failures in IoT networks; communication overhead; smart protocols vulnerability.
Ali et al. [55]	Θ	Comprehensive survey that promotes a trust-free peer-to-peer architecture for IoT, based on public-key infrastructure, smart-contract governance, and cross-layer synchronization mechanisms.
	Δ	Blockchain complexity and device heterogeneity continue to impede seamless interoperability; full-ledger replication and consensus maintenance impose substantial computational, storage, and bandwidth overheads on resource-constrained nodes, thereby constraining scalability and increasing latency; gateway-centered topologies retain a residual single-point-of-failure vulnerability.
Wang et al. [56]	Θ	Comprehensive analysis of cryptographic primitives underpinning peer-to-peer, trust-free blockchains, detailing how hash functions, digital signatures and zero-knowledge techniques sustain unforgeability and pseudonymity within decentralized public-ledger synchronization.

(Continued)

challenges such as scalability limitations when multiple operational modes are introduced, potential latency issues, and vulnerability to single points of failure in real-world applications. Additional problems arise from considerable communication overhead under variable environmental conditions, safeguarding transmitted

TABLE 1. *(Continued.)* **Methodology and challenges of blockchain integration with IoT devices.**

	Δ	Surveyed primitives demand substantial computational and energy resources, particularly memory-hard hashing and proof-of-work, thereby limiting scalability on lightweight or battery-powered devices; current privacy mechanisms remain susceptible to linkage analysis, leaving residual confidentiality gaps.
Casino et al. [57]	Θ	Provides a systematic, cross-sector review of PoW-based, trust-free blockchain systems, analyzing their robustness and classifying applications across finance, IoT, governance and other domains.
	Δ	Survey reveals limited understanding of interoperability and scalability, particularly where consensus mechanisms intensify communication and storage demands; PoW's computational and memory requirements remain beyond the capabilities of lightweight IoT devices, yet these constraints are not quantitatively evaluated.
Liu et al. [58]	Θ	Offers a wide-ranging, game-theoretic survey of blockchain consensus mechanisms, tamper-proof ledger construction and timestamping, analyzing how strategic behavior shapes security, mining management and energy-trading scenarios across diverse applications.
	Δ	The review does not address deployment on resource-constrained or mobile edge devices, whose limited CPU and battery capacity make classical PoW assumptions unsustainable; the schemes discussed still entail non-trivial computation and energy consumption, as the authors acknowledge in their sustainability analysis; throughput and overall scalability remain constrained by extended block-generation intervals, limited block size and queuing delays; regulatory and governance questions for permissioned or consortium ledgers are identified but left unresolved, indicating the need for future policy-aware models.
Conti et al. [59]	Θ	Systematic survey of Bitcoin, detailing the security and privacy properties of its PoW-based consensus protocol and the broader blockchain ecosystem.
	Δ	Block verification under PoW imposes considerable computational expenditure, and the protocol remains susceptible to a range of attacks, including double-spending, network-level eclipsing, and miner collusion, that threaten its long-term robustness.
Ferrag et al. [60]	Θ	Presents a comprehensive survey of blockchain techniques for IoT, emphasizing decentralized resource-management, anonymity services, and a taxonomy of threat-resistant architectures across multiple application domains.
	Δ	Identity- and reputation-oriented attacks remain challenging, while the computational, bandwidth, and storage demands of current blockchain protocols exceed the capabilities of many IoT devices, constraining scalability in practice.
Dinh et al. [61]	Θ	PoW consensus design that limits Sybil adversaries, embedding it within a distributed ledger that supports Turing-complete smart contracts and is empirically profiled with the BLOCKBENCH benchmark suite.
	Δ	PoW mining imposes substantial computational and energy demands, yielding very low throughput (≈ 7 tx/s) and extended confirmation delays; probabilistic model prevents the system from providing linear scalability, so performance degrades evidently under high-traffic conditions.
Li et al. [62]	Θ	Permissionless blockchain architecture in which an anonymous PoW consensus protocol coordinates distributed ledger replication, enabling transaction validation among mutually untrusted nodes with no reliance on external authorities.
	Δ	Design inherits classical PoW limitations: a miner collective controlling ≈51% of the hash rate can rewrite history and perform double-spending, while weak key generation exposes address linkability; substantial computation required for global consensus restricts throughput and remains impractical for resource-constrained IoT endpoints, leaving scalability and endpoint security issues unaddressed.
Ahmed et al. [63]	Θ	Introduces a scalable rural-agriculture IoT architecture that interconnects 6LoWPAN sensor clusters with a WiLD multihop backbone and fog-computing gateways; cross-layer duty-cycle MAC and adaptive routing scheme is employed to cut latency and energy consumption while maintaining end-device compatibility.
	Δ	Multihop WiLD backbone imposes accumulating processing and message load, so throughput falls as node density rises, and reliable operation still depends on clear line-of-sight links that are sensitive to weather-induced attenuation, limiting long-range viability; framework lacks integral end-to-end integrity controls, leaving data streams open to manipulation and tampering in an unsecured rural wireless environment.
Ahmad et al. [64]	Θ	Surveys a decentralized peer-to-peer framework that leverages a blockchain ledger and fine-grained timestamping to collect and authenticate high-volume IoT data streams in real time, eliminating reliance on central authority.
	Δ	PoW validation and global ledger replication impose significant computation and energy demands, while each node's need to store the ever-growing chain inflates local memory requirements and network traffic, thereby constraining scalability in resource-constrained IoT environments; consensus layer remains susceptible to double-spending and majority-hash-rate attacks, reflecting an underlying weakness in the incentive and trust model.
Mukkamala et al. [65]	Θ	Blockchain framework for social-business applications, outlining principles that integrate distributed-ledger storage with decentralized consensus algorithms to deliver trust, transparency, and auditability across peer-to-peer networks.
	Δ	Real-world deployment is limited by the substantial computational and latency overheads that existing consensus protocols impose on lightweight or mobile clients; developing a native cryptocurrency raises uncertain regulatory and formal-modelling questions, complicating compliance and system verification.
Zhang et al. [66]	Θ	Outlines a peer-to-peer IoT architecture in which each device receives a unique blockchain address; transactions are secured with digital signatures and hash-chain records.
	Δ	Deployment costs are not evaluated, while continuous ledger synchronization imposes processing and storage demands that many lightweight devices cannot meet; the absence of agreed data formats further impedes interoperability.
Hackius et al. [67]	Θ	Hybrid decentralized ledger for logistics data, secured by public–private-key signatures and cryptographic hashing, and assesses industry interest through a survey of 152 supply-chain professionals.
	Δ	Technological immaturity; regulatory uncertainty; industry resistance; lack of awareness.
Zyskind et al. [68]	Θ	Decentralized personal-data platform that combines off-chain storage with PoW blockchain serving as an automated access-control manager.
	Δ	Retains inherent PoW weaknesses: majority-hash-rate adversaries can rewrite history, and the high computational requirement raises sustainability and security concerns.

data against security breaches, elevated computational demands, and heightened energy use that exceeds the capacity of resource-constrained underwater hardware. Moreover, compatibility with existing infrastructure, privacy-related concerns, and reducing environmental impacts associated with deploying novel technological solutions in the marine environment remain potential areas for further investigation.

- Mirsadeghi et al. [51] proposed a trust-based authentication approach, specifically for clustered vehicular

ad hoc networks, that employs clustering to foster trust among vehicle nodes. Their trust-based authentication method for vehicular networks involves several challenges, including scalability limitations as network size increases, potential latency introduced by complex trust computation and clustering procedures, significant communication overhead in continuous monitoring, and inherent complexity involved in dynamically evolving trust relationships.

Each of these initiatives faces several challenges related to scalability under increased traffic loads, balancing energy and computational resource consumption, maintaining data security and integrity, and ensuring seamless compatibility with established infrastructure. Such persistent challenges highlight the need for ongoing research efforts to refine these approaches further, ensuring they effectively address the complex requirements of contemporary transportation networks. Blockchain integration and other approaches offer significant potential for enhancing IoT and smart transportation systems; however, addressing associated challenges is essential for practical adoption and long-term sustainability. As summarized in **Table 1**, integrating blockchain technology with IoT systems presents opportunities to tackle several challenges but also introduces new complexities. Various methodologies emphasize the effectiveness of blockchain in enhancing security, scalability, privacy, and integrity within IoT networks through solutions such as PKI, consensus mechanisms, and decentralized architectures. However, continual issues such as computational overhead, extensive storage requirements, and compatibility with lightweight IoT devices remain posing significant barriers across these solutions.

One of the critical concerns identified in **Table 1** involves preserving privacy and anonymity within blockchain-enabled IoT systems. Approaches employing IBE and decentralized public ledgers have been investigated to achieve privacy protection; however, these methods typically demand substantial computational resources, making them impractical for implementation on resource-limited IoT devices. Consequently, achieving an optimal balance between scalability and privacy remains a significant challenge, as demonstrated by multiple research studies. For instance, while Li et al. and Gupta et al. emphasize blockchain's effectiveness in ensuring data integrity and robust access control, they also acknowledge challenges such as considerable communication overhead and susceptibility to attacks, including double-spending vulnerabilities. Similarly, autonomous large-scale network solutions proposed by Gai et al. and Ahmed et al. depend heavily on extensive bandwidth and substantial storage capacity, further exacerbating scalability constraints.

Identity management poses a significant challenge within IoT systems, primarily because data exchanges among IoT devices frequently incorporate personal identity information, thus increasing vulnerability to data breaches and privacy violations. This issue becomes specifically critical in contexts such as green transportation networks or large-scale vehicular systems interconnected via fog devices, where secure communication protocols are essential for safeguarding identities without compromising network integrity. Identity-based management systems (IBMS), which rely heavily on encryption to secure user identity, have been proposed to address these concerns. However, studies by Zhou et al. and Salman et al. highlight ongoing vulnerabilities associated with cryptographic mechanisms and protocol inefficiencies. Shah et al. [69], for instance, investigated privacy issues arising from data aggregation within fog computing environments and proposed k-anonymity techniques as a countermeasure to enhance user anonymity. Similarly, Firouzi et al. [70] developed a unified shared-key mechanism enabling exclusive traceability of device identities by cloud servers, aiming to address issues of traceability, confidentiality, and non-repudiation. Despite their contributions, these methods still face persistent challenges, particularly related to key-escrow vulnerabilities due to reliance on centralized key-generation centres (KGC), which risk exposure of private keys and consequently weaken overall system security.

The methodologies presented in **Table 1** also underscore the significant computational complexity of blockchain technology, which limits its practicality for lightweight IoT devices, as emphasized in studies by Mukkamala et al. and Zhang et al. Additionally, the storage demands associated with decentralized ledgers pose significant obstacles, particularly in expansive IoT deployments, with studies such as those by Liu et al. and Hackius et al. highlighting the necessity for substantial storage infrastructure. Furthermore, latency and energy consumption remain persistent challenges in ensuring efficient blockchain operations, as demonstrated by Zhou et al. and Wang et al. Although blockchain technology offers considerable potential to improve security and scalability in IoT environments, its practical deployment continues to encounter notable technical and operational challenges. Privacy preservation, identity management, computational efficiency, and scalability are persistent themes in the challenges outlined by these studies. The integration of advanced cryptographic techniques, such as IBMS and k-anonymity, and innovative consensus mechanisms could mitigate some issues, but the key-escrow problem and computational overhead remain areas requiring further research and development.

III. SECURITY CHALLENGES IN IDENTITY-BASED ENCRYPTION

In IBE within IBMS, the public key is derived from identity information rather than being randomly generated. Compared to PKI, IBE simplifies key management but introduces challenges related to key-escrow and private key distribution. In cloud environments, KGC manages a master public/private key pair, verifies user or device identities, and generates corresponding secret keys. The KGC can generate private keys used to decrypt encrypted data.

In blockchain applications, key-escrow poses a security risk, as unauthorized parties can potentially access and decrypt transactions or smart contracts without the owner's consent [52], [71]. This issue hinders IBE adoption due to concerns over communication privacy. Researchers have explored ways to reduce reliance on the KGC [72], [73], [74], but challenges persist. The KGC typically maintains identity list, allowing it to link ciphertexts to specific users. To address this, an anonymous key-issuing protocol and an identity-certifying authority (ICA) have been proposed [75], [76], [77].

These protocols allow users to obtain secret keys while keeping their identities hidden from the KGC. However, the lack of formal security guarantees when the ICA authenticates users remains an issue. As shown in **Table 2**, studies based on this approach often lack formal validation to assess their effectiveness in addressing the key-escrow problem. Additionally, shifting trust from the KGC to the ICA does not fully resolve security concerns.

Table 2 outlines various IBC methods and their limitations across different applications, emphasizing the integration of IBE with blockchain to improve privacy and security in IoT systems, particularly in smart transportation. Each approach focuses on specific aspects, such as authentication, privacy preservation, and decentralization, but they also face challenges, including scalability, computational overhead, and key management.

For instance, Zhou et al. [4] developed an identity-based authentication (IBA) scheme that incorporates privacy preservation, traceability, and integrity for UwGTs. However, the absence of mathematical proof and real-world performance assessments highlights a common limitation in IBC implementations. Similarly, Gupta et al. [47] and Wang et al. [78] addressed authentication and privacy concerns, yet their methods encounter practical issues related to computational complexity and message loss, limiting real-world applicability. Similar challenges arise in certificateless encryption (CLE) approaches [86], [87], [88], [89], where users independently generate cryptographic keys without involving a centralized KGC. Although this decentralization improves security by avoiding key-escrow vulnerabilities, it increases complexity, particularly in extensive IoT networks. Conversely, registration-based encryption (RBE), as introduced by Garg et al. [90], [91], attempts to streamline key management by aggregating all user keys into a single master key maintained by the KGC; yet this strategy necessitates frequent updates and struggles with scalability concerns.

Blockchain technology offers a promising alternative to address IBC limitations, particularly regarding the centralization and key-escrow issue [92], [93], [94], [95], [96], [97]. Through decentralized key management, blockchain mitigates reliance on a single authoritative entity, thereby enhancing data privacy and reducing security vulnerabilities. This attribute is particularly critical in transportation networks, where robust and confidential communications are imperative. Blockchain's intrinsic attributes, including decentralization, immutability, and transparency, augment cryptographic security protocols in environments with numerous interconnected IoT devices. However, implementing blockchain-based IBE systems introduces additional computational overhead, posing a significant challenge in extensive deployments. Studies by Tzeng et al. [84] and Zhang et al. [82] have specifically identified computational demands and increased overhead as key limitations in their proposed methods, emphasizing that successful practical implementation requires carefully balancing security, operational efficiency, and usability.

Future research should prioritize developing post-quantum identity-based encryption methods capable of overcoming existing constraints while providing enhanced security and scalability. Given the continual growth of IoT and smart transportation ecosystems, combining advanced cryptographic mechanisms with scalable blockchain architectures could significantly improve the security, efficiency, and resilience of these networks.

IV. QUANTUM SECURITY ENHANCEMENTS

In this section, we introduce BQC and QA as innovative cryptographic solutions to address the key-escrow problem and optimize resource allocation within IBE enabled smart transportation systems. We detail the system model involving data owners, data consumers, and cloud servers, emphasizing the secure processing and transformation of encrypted data. BQC ensures that computations are performed without revealing sensitive information, maintaining data privacy. QA is utilized to efficiently manage high-dimensional search spaces and optimize data routing and energy distribution across transportation nodes, enhancing security and performance in the network.

A. SYSTEM MODEL

The IBE system architecture comprises data owner, data consumer, registry authority, and cloud server, as shown in **Fig. 2**. Both the data owner and data consumer are cloud clients. The registry authority is responsible for setting up the system, responding to registration queries, and issuing public parameters for data outsourcing.

Cloud servers offer storage services to preserve outsourced data and computation services for clients to alter stored files. To protect data privacy, entities use IBE to encrypt data before outsourcing it to the cloud. If a file is the result of IBE encryption for a particular data owner and is initially intended for one data consumer, that owner can generate an authorization token to share the data with multiple data consumers. The cloud server then converts the IBE ciphertext file into a transformed ciphertext format, allowing authorized data consumers to decrypt and access the original information.

B. THREAT MODEL

An IBE system may face the following active attacks.

TABLE 2. Methods and limitations of identity-based cryptography.

Reference		Method Θ Challenge Δ
Zhou et al. [4]	Θ	Identity-based signature plus lightweight hashing to authenticate underwater IoT traffic and keep an immutable, synchronized ledger across heterogeneous devices.
	Δ	The design still exposes smart-contract logic to potential misuse, and its signing/verification routines introduce measurable processing and energy overhead that rises with key length, increasing latency and limiting scalability on resource-constrained devices.
Gupta et al. [47]	Θ	Blockchain-based IBE scheme for maritime-IoT, enabling authenticated device interaction and immutable peer-to-peer logging of vessel data to enhance confidentiality and traceability.
	Δ	IBE computations and on-chain verification introduces noticeable cryptographic overhead for low-power sensors, and the workload escalates with message sizes or node count rise, limiting scalability under dense network traffic; typical ledger-level threats (e.g., double-spending) are not explicitly mitigated, leaving resilience gaps in high-volume settings.
Khan et al. [52]	Θ	Permissioned-blockchain framework that integrates consensus-validated blocks, secure timestamping, and IBE to protect user records within a decentralized public ledger.
	Δ	Combined consensus computation and IBE processing impose substantial computational and energy demands, thereby constraining throughput as the network scales; interoperability with resource-constrained edge devices is not demonstrated; key-update mechanism is comparatively cumbersome, delaying timely credential rotation.
Wang et al. [78]	Θ	Developed SIPAR, an identity-based conditionally privacy-preserving authentication scheme in which signature verification avoids costly bilinear pairings, keeps the system master key solely at the trusted authority (never in a vehicle's TPD), and lets any roadside unit revoke a misbehaving vehicle simply by updating its local secret and broadcasting the new public key, eliminating certificate-list exchanges.
	Δ	SIPAR's evaluation focuses on computation time and normal-link bandwidth; it omits analysis of performance under the high packet-loss rates typical of dense or fast-moving VANETs and provides only a basic handshake for entering a new RSU domain, leaving seamless cross-RSU re-authentication and reliability under adverse channel conditions unexplored.
Ali et al. [79]	Θ	Proposes an ECC-based IBS-CPPA that eliminates pairings and map-to-point operations, reducing each verification to a single point multiplication plus one addition while still guaranteeing authentication, anonymity, traceability, and non-repudiation.
	Δ	Messages are only signed, not encrypted, end-to-end confidentiality is absent, and the evaluation ignores wireless-link effects, leaving real-world packet loss and total delivery delay unmeasured.
Tangade et al. [80]	Θ	Developed TMHC, which combines identity-based signatures with lightweight HMAC to authenticate unlinkable beacons, while a roadside-authority assigns dynamic trust scores, cutting bandwidth and computation versus PKI schemes.
	Δ	Protocol still verifies each beacon individually; efficiency with batch signature checking in dense traffic has not been evaluated.
Zhang et al. [81]	Θ	Introduces a vehicular-cloud scheme that fuses dynamic identity-based authenticated asymmetric group key agreement with location-based encryption, letting users restrict data processing to chosen geographic regions while vehicles form a secure, anonymous cloud.
	Δ	Protocol assumes a reliable cloud and does not address multi-hop broadcasting when vehicles are widely dispersed, so its scalability in sparse networks remains untested.
Zhang et al. [82]	Θ	Introduced OTIBAAGKA, a one-round, identity-based asymmetric group key agreement that lets any vehicle (not a fully trusted RSU) distribute the group secret key; every pseudonym serves as a public key, removing external certificates, and a single short broadcast updates the group key for all members, thereby achieving operation without a trusted authority and lightweight, immediate key renewal inside the CMIX.
	Δ	All vehicles in a CMIX still encrypt with one shared symmetric key that is only refreshed on a fixed schedule; if a compromised or insider discloses this key, every message remains vulnerable until the next periodic update because the protocol lacks any prompt re-keying or revocation mechanism.
Karati et al. [82]	Θ	Introduced OTIBAAGKA, an anonymous, identity-based protocol in which Diffie–Hellman-style bilinear-pairing design lets each vehicle issue a one-time signature that is jointly verifiable, providing message authentication and provable unforgeability without traditional certificates.
	Δ	Every signature check still triggers multiple bilinear-pairing evaluations, among the costliest crypto operations, so the work does not resolve the resulting verification delay and CPU load that become acute when many beacons arrive at once.
Cui et al. [83]	Θ	Introduced SPACF, a pairing-free ECC identity-based authentication that combines cuckoo filters with binary search to speed batch signature verification at RSUs, avoiding tamper-proof hardware while maintaining message authenticity and conditional privacy.
	Δ	All private keys derive from a single master secret kept by the trusted authority, so a breach there would compromise every vehicle, an inherent key-escrow risk the author does not mitigate.
Tzeng et al. [84]	Θ	Presents an identity-based batch scheme in which pre-loaded secrets let an RSU authenticate any number of beacons with only two pairings and one point multiplication, yet still preserve vehicle anonymity and traceability.
	Δ	Producing pseudonyms, signing beacons, and, when a batch fails, reverting to per-message checks still incur pairing-heavy, multi-step computations that strain resource-limited nodes.
Lo et al. [85]	Θ	Developed an ECC identity-based authentication that swaps costly pairings for one-way hashes, allowing rapid batch verification while remaining unforgeable against adaptive chosen-message attacks.
	Δ	The author measured cryptographic speed but not radio-layer congestion, leaving the impact of packet loss in high-density traffic unexplored.

1. Impersonation: Cloud clients may attempt to gain unauthorized access to outsourced data by impersonating data owners or legitimate data consumers.
2. Malicious Cloud Servers: Cloud servers or attackers with access to cloud servers may seek to steal data containing personal identity information.

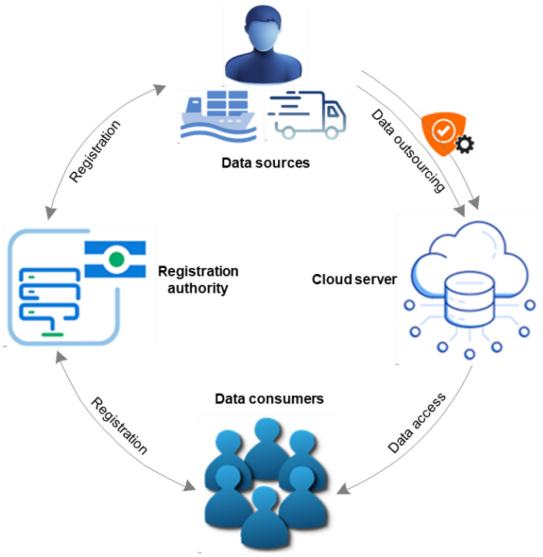

FIGURE 2. IBE mechanism for data outsourcing.

3. Misuse of Authorization Tokens: Cloud servers may exploit data owners' authorization tokens to transform encrypted data that is not authorized for sharing.

Given these realistic threats, we need to define a secure IBE system that complies at least with the security objectives listed below.

- Data security: To ensure data security, one effective measure is to encrypt data before outsourcing it. This way, authorized users who possess the right decryption keys can access the data. Cloud servers and unauthorized clients cannot access the encrypted data.
- Manageable transformation: Any data transformation on the cloud server requires an authorization token approved by the data owner. It must be infeasible for the cloud server or any other unauthorized clients to infer a valid authorization token for transforming unrelated files or obtaining identity information from encrypted data.

C. IBE ALGORITHM

The constructed algorithm consists of setup, registration, encryption, authorization, transformation, and decryption.

1. Setup: $(1^{\lambda}, m) \rightarrow (P_k, M_k)$ – The algorithm for setting up the registration authority takes the security parameter λ as input and permits a maximum number of authorized data consumers m to access the data. The output includes the public key P_k for the system and a master key M_k for the registry authority.
2. Registration: $(ID, P_k, M_k) \rightarrow S_{k-ID}$ – Registry authority requires the public parameter P_k, the master key M_k, and an identity $ID \in \{0, 1\}^*$ to generate a private key S_{k-ID}.
3. Encryption: $(ID, P_k, M) \rightarrow C_{T-ID}$ – The data owner inputs the public parameter P_k, the message M to be encrypted, and an identity ID to produce an IBE ciphertext C_{T-ID}.
4. Authorization: $(P_k, S_{k-ID}, C_{ID}) \rightarrow T_{ID \rightarrow C_{ID}}$ – The data owner inputs the public parameter P_k, their private key S_{k-ID}, and a set of consumer identities C_{ID}. The algorithm produces an authorization token $T_{ID \rightarrow C_{ID}}$ enabling transformation for the specified consumers.
5. Transformation: $(P_k, T_{ID \rightarrow C_{ID}}, C_{T-ID}) \rightarrow C_{T-C_{ID}}$ – The cloud server uses P_k, the authorization token $T_{ID \rightarrow C_{ID}}$, and the ciphertext C_{T-ID} to produce a transformed ciphertext $C_{T-C_{ID}}$.
6. Decryption: $(P_k, S_{k-ID'}, C_{T-ID}/C_{T-C_{ID}}) \rightarrow M/\perp$ – The data consumer utilizes their unique identity ID', along with the public parameter P_k, private key $S_{k-ID'}$, and either ciphertext C_{T-ID} or $C_{T-C_{ID}}$ to decrypt and obtain the message M. If the $ID = ID'$ for C_{T-ID} or $ID' \in C_{ID}$ for $C_{T-C_{ID}}$, the algorithm outputs the original message M; otherwise, it outputs a null symbol $\perp$.

To set up the algorithm $(1^{\lambda}, m) \rightarrow (P_k, M_k)$, the following conditions must be satisfied:

- When decrypting an IBE ciphertext, $(ID, P_k, M,) \rightarrow C_{T-ID}$, using a private key $(ID', P_k, M_k) \rightarrow S_{k-ID'}$, the decryption algorithm $(P_k, C_{T-ID}, S_{k-ID'})$ will always output the plaintext message M if and only if the identifier used to generate the ciphertext matches the identifier associated with the private key, such as $ID = ID'$.
- Given a transformed ciphertext $(P_k, T_{ID \rightarrow C_{ID}}, C_{T-ID}) \rightarrow C_{T-C_{ID}}$ and a private key $(P_k, M_k, ID') \rightarrow S_{k-ID'}$, the decryption algorithm $(P_k, C_{T-C_{ID}}, S_{k-ID'})$ will always output the plaintext message M if and only if $ID' \in C_{ID}$.

The initial requirement is straightforward; only the authorized data consumer is permitted to decrypt any IBE ciphertext. However, in the case of transformed ciphertext, the authorization token utilized in the transformation must be generated by the entity who intercepted the original ciphertext. This condition ensures that only the data consumers whose identities are mentioned in the authorization token can decrypt the transformed ciphertext.

To address the outlined requirements, we develop an intuitive solution that leverage BQC and QA within the IBE framework. This approach ensures data security and efficiency in solving optimization challenges in smart transportation systems, with particular attention to overcoming the key-escrow issue.

D. BLIND QUANTUM COMPUTATION FOR SECURE IBE

Blind Quantum Computation allows a data owner to outsource the encryption process to a quantum server without revealing sensitive information, thus preserving data privacy. In the IBE context, BQC allows secure delegation of key generation and encryption processes to the cloud server without exposing the private key or identity-related information.

1) BQC-ENHANCED IBE SYSTEM ARCHITECTURE

- Data Owner: Encrypts data without revealing identity.
- Data Consumer: Authorized users who can decrypt the data.
- Registry Authority (RA): Sets up public parameters and issues private keys based on identities.
- Quantum Cloud Server (QCS): Performs encryption and transformation computations while remaining "blind" (i.e., it cannot access the actual data or identities).

2) SETUP PHASE

- The RA initializes the system using a security parameter λ, generating public key P_k, and master secret key M_k. This initialization process is classical and outputs public parameters, allowing authorized data consumers' identities to be recognized within the IBE framework.

3) KEY GENERATION WITH BQC

- The data owner initiates a BQC protocol with the QCS by preparing a quantum state $|\psi\rangle|$ that encodes their identity ID and public parameters P_k.
- The QCS operates on $|\psi\rangle|$ blindly, gaining no information about the encoded data or the identity.
- After the QCS completes the computation and returns the quantum state, the data owner performs post-processing to extract the encrypted private key S_{k-ID} without revealing its structure to the QCS.

4) ENCRYPTION WITH BQC

- For encryption, the data owner again uses BQC, sending the encrypted identity ID and message M to the QCS as a quantum state.
- The QCS processes this state according to the encryption protocol, unaware of the underlying values.
- The resulting IBE ciphertext C_{T-ID} is then sent back to the data owner or stored in the cloud.

5) AUTHORIZATION & TRANSFORMATION

- Using BQC, the data owner generates an authorization token $T_{ID\to C_{ID}}$, designating specific data consumers.
- The QCS transforms the ciphertext C_{T-ID} into $C_{T-C_{ID}}$ based on $T_{ID\to C_{ID}}$, making it accessible only to the designated consumers.

6) DECRYPTION

- Data consumers can decrypt the transformed ciphertext with their private keys using classical methods if their identities match those in $C_{T-C_{ID}}$.
- Since BQC prevents the QCS from learning identity and key information, key-escrow risks are mitigated, hence no single entity has direct access to both identity and private key data.

By employing BQC, private keys are generated and encrypted without exposing them to the QCS or any centralized KGC. The RA maintains system integrity without direct access to private keys, thus eliminating a single point of failure.

E. QUANTUM ANNEALING FOR OPTIMIZATION IN IBE-ENABLED SMART TRANSPORTATION SYSTEMS

Quantum Annealing optimizes resource allocation in a smart transportation network, handling tasks such as data routing and energy distribution. Within an IBE framework, QA also manages high-dimensional search spaces inherent in large IoT networks.

1) QA-BASED OPTIMIZATION PROCESS: PROBLEM FORMULATION

- Objective: Minimize data latency and maximize security across transportation nodes.
- Variables: Define binary variables x_i, where $x_i = 1$ indicates an active and secured node, and $x_i = 0$ otherwise.
- Cost Function: Define an objective function $H(x) = \sum_i E_i x_i + \sum_{i,j} C_{ij} x_i x_j$, where E_i is the energy cost for node i and C_{ij} is the communication cost between nodes i and j.

2) ENCODE THE OBJECTIVE FUNCTION

Use the IBE system's secure communication channels to share initial parameters and embed the optimization objective into $H(x)$. The RA translates transportation data into this initial Hamiltonian $H(x)$, embedding identity-based constraints.

3) INITIALIZING ANNEALING

A quantum annealer starts in a superposition of states representing all possible active/inactive node configurations. It then gradually transitions from higher-energy states (sub-optimal configurations) to a low-energy state that optimizes latency and data flow.

4) QUANTUM EVOLUTION

Quantum tunneling effects allow the annealer to navigate solution space efficiently. The quantum annealer converges on an optimal network configuration that balances security (through authorized nodes) and efficient data transmission paths, following IBE's authorization constraints.

5) RESULT EXTRACTION AND SYSTEM UPDATE

Once the optimal configuration is identified, the system is updated with these optimized parameters. The network adapts in real time, leveraging secure IBE authorizations and minimizing bottlenecks.

By embedding authorization constraints into the quantum annealer, only configurations meeting specific identity requirements are valid. This design mitigates the key-escrow problem since keys are not stored centrally but are managed dynamically within the optimized network, preventing any single entity from holding complete key information.

F. FORMULATION OF QUANTUM-ANNEALED OPTIMIZATION PROBLEM IN IBE-ENABLED SMART TRANSPORTATION SYSTEMS

The integration of IBE into resource-constrained smart transportation systems necessitates efficient optimization of

data routing and communication strategies, particularly to reduce computational delays, energy usage, and weaknesses associated with cryptographic transformations. QA serves as an effective method to address this optimization challenge, by mapping the routing problem into a Quadratic Unconstrained Binary Optimization (QUBO) formulation compatible with existing quantum hardware.

Let $\mathcal{N} = \{1, 2, \ldots, N\}$ represent the collection of nodes within the smart transportation system, such as sensors or vehicles, and $\mathcal{G} = \{1, 2, \ldots, G\}$ signify gateway or edge computing nodes capable of decrypting and processing encrypted data. For each node $i \in \mathcal{N}$, a set of precomputed routing paths $\mathcal{P}_i$ may be defined, and let $\mathcal{P} = \bigcup_{i=1}^{N} \mathcal{P}_i$ denote the complete set of potential routing paths available within the entire network.

For each path $p \in \mathcal{P}$, we define a binary decision variable:

$$x_p = \begin{cases} 1, \text{ if path p is selected for transmission;} \\ 0, \qquad\qquad \text{otherwise.} \end{cases}$$

Each path p is associated with three metrics: 1) $L_p \rightarrow$ estimated end-to-end latency (ms); 2) $E_p \rightarrow$ estimated energy cost (mJ); and 3) $R_p \rightarrow$ escrow risk, defined as the number of cryptographic transformation requests involving the BQC server for intermediate key derivation. The objective function is to minimize the total weighted cost across all selected paths:

$$\min_x H(x) = \sum_{p \in \mathcal{P}} \left(\alpha L_p + \beta \mathrm{E}_p + \gamma R_p\right) x_p$$

where $\alpha, \beta, \gamma > 0$ are system-defined weights reflecting the trade-off among latency, energy, and security risk.

To ensure feasible and efficient routing, the following constraints should be considered:

- Unique path selection: Each node must be assigned exactly one path. Let $C_{pi} = 1$ if path p corresponds to node i, and 0 otherwise:

$$\sum_{p \in \mathcal{P}} C_{pi} x_p = 1, \ \forall i \in \mathcal{N}$$

- Gateway capacity limits: Each gateway $g \in \mathcal{G}$ has a maximum processing capacity B_g. Let $\mathcal{P}_g$ be the set of paths terminating at gateway g:

$$\sum_{p \in \mathcal{P}_g} x_p \leq B_g, \ \forall g \in \mathcal{G}$$

These constraints are integrated into the QUBO model using penalty functions, producing the following formulation:

$$Q(x) = H(x) + \lambda_1 \sum_{i \in \mathcal{N}} \left(\sum_{p \in \mathcal{P}} C_{pi} x_p - 1 \right)^2 + \lambda_2 \sum_{g \in \mathcal{G}} \left(max\left(0, \sum_{p \in \mathcal{P}_g} x_p - B_g\right)\right)^2$$

where λ_1 and λ_2 are penalty coefficients that enforce constraint compliance.

Illustrative Scenario: Consider a maritime transportation network consisting of $N = 50$ vehicle-mounted IoT nodes and $G = 3$ roadside edge gateways. Each node is pre-assigned a set of $k = 3$ candidate paths based on radio range, congestion estimates, and link stability. For each path p, approximate values of latency L_p, energy usage E_p, and escrow risk R_p are derived from system-level models informed by historical data and device specifications. Using a total of 150 decision variables (paths), the QUBO model can be mapped onto current QA hardware with fewer than 200 logical qubits, depending on embedding efficiency.

This theoretical scenario demonstrates how routing decisions can be jointly optimized for performance and quantum security, offering significantly reduced search complexity compared to classical combinatorial methods, especially under real-time constraints.

G. FEASIBILITY OF IMPLEMENTATION AND EMPIRICAL VALIDATION

To assess the implementation complexity and empirical feasibility, we outline a multi-stage validation plan that transitions from simulation to deployment.

1) QUBO SIMULATION AND SOFTWARE PROTOTYPING

Initial implementation can be carried out using the D-Wave Ocean SDK, allowing the QUBO model to be defined, tested, and solved using either classical QUBO solvers, e.g., simulated annealing or tabu search, or publicly accessible quantum annealers. The software layer integrates with a Python-based simulation of the IBE and BQC protocol stack, using estimated latency, energy, and key-transformation risk values.

2) VALIDATION METRICS

To evaluate system-level feasibility, several metrics can be computed through simulation, such as 1) average end-to-end latency across all active paths; 2) total energy consumption per transmission cycle; 3) number of BQC interactions, as a proxy for escrow risk; and 4) optimization runtime and convergence consistency. These metrics allow comparison against traditional deterministic routing schemes and classical optimization techniques.

3) HARDWARE-IN-THE-LOOP INTEGRATION

A hardware-in-the-loop testbed could be constructed using embedded devices, such as Raspberry Pi or similar, to emulate sensors and gateways. Precomputed values for latency and energy consumption can be measured under various network loads, enabling realistic model calibration.

4) SCALABILITY ASSESSMENT VIA EMULATION

To assess system behavior at scale, ns-3 network simulator can be used to model hundreds of nodes and multiple

gateway configurations. The quantum optimization layer remains external, interfaced via API, and solves updated QUBO instances as node mobility or traffic patterns evolve.

V. DISCUSSION

The integration of blockchain and IBE into IoT systems, particularly in the context of smart transportation networks, offers significant opportunities for enhancing security, privacy, and scalability. By leveraging blockchain's inherent properties, such as decentralization, transparency, and immutability, coupled with the cryptographic flexibility of IBE, these systems can address key security challenges like data integrity and unauthorized access. However, the practical deployment of these technologies is hindered by several challenges, including computational overhead, scalability constraints, and key management vulnerabilities.

A critical concern in current implementations is the reliance on a centralized KGC, which introduces risks such as key-escrow, single points of failure, and privacy breaches. Our proposed approach leverages BQC to decentralize key management and mitigate the key-escrow problem. By enabling secure delegation of cryptographic operations to quantum servers without revealing private keys or identity-related information, BQC significantly strengthens the security framework. This ensures that even in untrusted environments, sensitive data remains protected.

Furthermore, the dynamic nature of smart transportation networks, characterized by fluctuating environmental conditions and high node mobility, necessitates real-time optimization of resources. QA addresses this need by formulating resource allocation, data routing, and energy distribution as combinatorial optimization problems. By efficiently navigating high-dimensional search spaces, QA identifies optimal configurations for IoT nodes, reducing latency and improving system adaptability to changing conditions. This quantum-enhanced optimization approach is critical for maintaining operational efficiency in large-scale, resource-constrained IoT ecosystems.

A. KEY ADVANTAGES OF THE PROPOSED FRAMEWORK

The integration of BQC and QA within the framework of blockchain and IBE brings numerous significant advantages. These address some of the most pressing challenges in securing and scaling IoT-based smart transportation systems.

1) PRIVACY PRESERVATION

BQC ensures that sensitive identity-related data and private cryptographic keys are never exposed to external parties, including quantum cloud services or unauthorized entities. This reduces the potential risk of identity misuse during cryptographic operations. Moreover, by decentralizing key generation procedures, BQC effectively mitigates vulnerabilities, including key-escrow, ensuring no centralized authority can dominate the management or control over cryptographic keys. This feature is particularly essential in contexts such as UwGTs, where IoT devices frequently transmit essential environmental data, demanding rigorous confidentiality measures to protect user identities.

2) DECENTRALIZED SECURITY

Blockchain's decentralized ledger, combined with secure identity-based cryptographic mechanisms, provides a robust security architecture. By eliminating the dependency on centralized authorities, such as KGC, this framework significantly reduces the risk of single points of failure. This inherent decentralization ensures protection from unauthorized modifications, including data breaches, SQL injections, or malicious third-party interventions, ensuring end-to-end data integrity.

3) SCALABILITY AND EFFICIENCY

QA optimizes resource allocation, data routing, and energy management in dense IoT networks, such as those found in smart transportation systems. By efficiently addressing combinatorial optimization challenges, QA allows networks to dynamically respond to changing operational conditions and node mobility. This scalability ensures that large-scale IoT networks can sustain high performance without compromising on security, even in resource-constrained environments. The framework addresses the computational limitations of traditional cryptographic methods, making it suitable for lightweight IoT devices operating with limited power and memory.

4) ROBUSTNESS AGAINST ATTACKS

Incorporating BQC effectively counters various cybersecurity threats, including code-reuse attacks, fake data injection, and phishing attempts, by ensuring cryptographic keys remain hidden from unauthorized entities. Quantum-enhanced cryptographic techniques offer resilience against advanced attacks, including those targeting centralized key repositories or exploiting network vulnerabilities. This is especially critical in maritime environments and smart transportation infrastructures, where attacks such as malware implantation or DoS/DDoS traps could disrupt operations.

5) IMPROVED RESOURCE UTILIZATION

Implementing QA for dynamic allocation of resources substantially reduces transmission latency and improves throughput within IoT communication networks. Such optimization is essential for maintaining operational efficiency in high-density interconnected IoT environments, such as real-time data collection from underwater sensor networks or advanced smart road transportation infrastructures.

B. CRITICAL COMPARISON WITH LEGACY BLOCKCHAIN-ONLY SCHEMES

Blockchain, PKI, and CLE have significantly advanced distributed security, however, each exhibits inherent limitations that constrain their applicability in heterogeneous, large-scale, and resource-constrained IoT environments. Based

on the quantitative and qualitative analysis presented in Tables 1 and 2, this subsection offers a critical comparison of these classical approaches and outlines how the proposed framework integrating BQC and QA addresses their deficiencies.

1) COMPUTATIONAL AND ENERGY OVERHEAD

Blockchain systems employing consensus mechanisms such as PoW introduce substantial computational and energy demands, often resulting in low throughput (e.g., $\leq$ 7 tx/s in Bitcoin-class systems) [61]. These requirements are not feasible for IoT devices with limited processing and power capabilities, as evidenced in several studies [8], [12], [54]. The proposed method mitigates this by delegating key generation and ciphertext transformation to a blind quantum server, thereby removing PoW from the client-side process. This reduces local resource consumption without compromising security.

2) SCALABILITY LIMITATIONS

Permissioned blockchains and lightweight consensus protocols, such as PBFT and Proof-of-Authority, exhibit throughput saturation as the network scales, due to increased consensus traffic and replication overhead. These effects are particularly significant in dense IoT settings. The integration of QA enables efficient real-time optimization of resource allocation, such as routing and power budgeting, producing low-latency, high-throughput configurations that support near-linear scalability.

3) TRUST CENTRALIZATION IN PKI

Traditional PKI systems rely on certificate authorities (CAs), introducing single points of failure and increasing administrative complexity. Certificate issuance, revocation, and renewal introduce latency and communication overhead, which are particularly challenging for IoT nodes with limited or unstable connectivity. The proposed method replaces the CA with BQC-based key generation, wherein private keys are generated inside blind quantum circuits inaccessible to any classical party. This removes reliance on centralized authority while maintaining strong identity assurance.

4) INCOMPLETE ESCROW MITIGATION IN CLE

While CLE improves PKI by decentralizing key management, it still depends on the key-generation authority to issue partial private keys. This reliance introduces a significant risk of key-escrow, as compromised authority could enable large-scale decryption. In contrast, the proposed approach ensures that neither the registration authority nor the quantum server alone has sufficient information to derive user private keys, thereby efficiently eliminating escrow-related vulnerabilities while preserving the deployment simplicity of IBE.

5) STORAGE OVERHEAD AND LEDGER SYNCHRONIZATION

Traditional replica blockchain architectures necessitate that each participating node stores the entire ledger, which presents considerable challenges for IoT devices with constrained storage capacity. This limitation is widely reported across surveyed studies. By incorporating QA-based replica placement, the proposed system ensures that only selected nodes maintain the full ledger, while others operate as lightweight clients. Post-quantum-secure proof allows these clients to verify transactions without extensive local storage, thus preserving ledger integrity with reduced overhead.

6) PRIVACY AND METADATA EXPOSURE

Conventional blockchain privacy enhancements, such as mixers and zero-knowledge proofs, remain vulnerable to metadata leakage and correlation attacks. The proposed framework addresses this by integrating identity constraints directly into the QA Hamiltonian and performing sensitive operations via BQC. This ensures that both message content and associated metadata remain concealed, enhancing resistance to both passive and active surveillance.

C. CHALLENGES AND FUTURE RESEARCH DIRECTIONS

Despite the advantages, several challenges must be addressed to realize the full potential of quantum-enhanced cryptographic solutions in IoT systems. These challenges span technological readiness, system compatibility, scalability, and policy considerations.

1) QUANTUM INFRASTRUCTURE READINESS

The implementation of quantum-enhanced methodologies requires access to reliable quantum computing hardware. Current quantum technologies remain in their growing stages, with limited scalability and availability. Moreover, the cost of developing and deploying quantum infrastructure for real-world IoT systems, such as smart transportation networks, is another barrier that must be addressed through research and investment.

2) INTEGRATION WITH EXISTING SYSTEMS

Ensuring the compatibility of quantum-based solutions with current blockchain platforms and IoT protocols is a complex task. For instance, legacy IoT devices may not have the computational capacity to interface with quantum-enhanced encryption protocols. Hence, blockchain systems must be modified to incorporate IBE with quantum-ready consensus mechanisms. Moreover, hybrid cryptographic models that combine classical and quantum techniques could provide a transitional path to fully quantum systems.

3) SCALABILITY IN REAL-WORLD DEPLOYMENTS

While QA provides efficient optimization for large networks, empirical validation in real-world settings is essential to address scalability issues. Factors such as latency, energy consumption, and the complexity of network configurations must be thoroughly evaluated. Moreover, IoT networks in smart transportation systems involve diverse nodes with

varying capabilities, from lightweight devices to high-performance servers. Adapting quantum methodologies to such heterogeneous environments remains a challenge.

4) COMPUTATIONAL COMPLEXITY AND RESOURCE CONSTRAINTS

Despite BQC and QA methodologies reducing computational demands compared with conventional cryptographic approaches, they continue to necessitate substantial quantum and classical computational resources. Achieving an optimal balance between these intensive resource requirements and the limited capacities inherent to lightweight IoT devices is particularly challenging. Future research should prioritize optimizing quantum algorithms to enable their efficient implementation on currently available quantum computing hardware.

5) REGULATORY AND POLICY IMPLICATIONS

Quantum-enabled cryptographic solutions must comply rigorously with international data security standards and privacy regulations. Ensuring adherence with frameworks such as the GDPR and NIST cryptographic standards is imperative when deploying these technologies in cross-border transportation systems. Regulatory entities must carefully evaluate the implications of quantum cryptographic approaches for identity management and data protection within sectors such as maritime transport and autonomous vehicle networks. Furthermore, a multidisciplinary collaboration involving policymakers, technology developers, and end-users is essential for developing governance structures that adequately balance innovation with security and privacy.

Future research should emphasize rigorous empirical evaluations of quantum-based cryptographic techniques, comparing their practical performance directly with traditional cryptographic methods. Additionally, developing hybrid quantum-classical methodologies could facilitate transitioning theoretical advances into tangible applications. Addressing these challenges can establish a robust foundation for future IoT implementations, ensuring enhanced security and operational efficiency within smart transportation infrastructures.

VI. CONCLUSION

The integration of quantum computing approaches, specifically BQC and QA, within IBE frameworks, presents substantial potential for enhancing the security of smart transportation systems. Employing BQC can effectively mitigate the longstanding issue of key-escrow inherent in traditional IBE schemes by allowing secure computations on encrypted data without disclosing sensitive identity-related information or private cryptographic keys. Additionally, QA provides a robust methodology for optimizing both operational and security aspects in real-time, significantly improving the efficiency and robustness of transportation networks. This analysis highlights the pressing need and practical viability of integrating quantum-based cryptographic methods to address existing limitations encountered by IBE schemes within complex IoT scenarios. Subsequent research efforts should concentrate on validating these quantum technologies through empirical assessment of their performance and scalability in actual smart transportation deployments. The continued evolution of quantum computing will likely yield even more sophisticated tools for securing and managing the next generation of intelligent transportation systems, making this an exciting area of ongoing and future exploration.

REFERENCES

[1] T. Qiu, N. Chen, K. Li, M. Atiquzzaman, and W. Zhao, "How can heterogeneous Internet of Things build our future: A survey," *IEEE Commun. Surveys Tut.*, vol. 20, no. 3, pp. 2011–2027, 3rd Quart., 2018, doi: 10.1109/COMST.2018.2803740.

[2] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tut.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015, doi: 10.1109/COMST.2015.2444095.

[3] A. Aljuhani, P. Kumar, R. Kumar, A. Jolfaei, and A. K. M. N. Islam, "Fog intelligence for secure smart villages: Architecture and future challenges," *IEEE Consum. Electron. Mag.*, vol. 12, no. 5, pp. 12–21, Sep. 2023, doi: 10.1109/MCE.2022.3193268.

[4] Z. Zhou, B. B. Gupta, A. Gaurav, Y. Li, M. D. Lytras, and N. Nedjah, "An efficient and secure identity-based signature system for underwater green transport system," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 9, pp. 16161–16169, Sep. 2022, doi: 10.1109/TITS.2022.3148166.

[5] J. Vogt, H. D. Schotten, and H. Wieker, "Intelligent transportation system protocol interoperability evaluation," *IEEE Open J. Intell. Transp. Syst.*,vol. 6, pp. 67–94, 2025, doi: 10.1109/OJITS.2025.3531549.

[6] M. Xu and L. Liu, "Sender-receiver role-based energy-aware scheduling for Internet of Underwater Things," *IEEE Trans. Emerg. Topics Comput.*, vol. 7, no. 2, pp. 324–336, Apr.–Jun. 2019, doi: 10.1109/TETC.2016.2632749.

[7] M. K. Moghimi and F. Mohanna, "Reliable object recognition using deep transfer learning for marine transportation systems with underwater surveillance," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2515–2524, Feb. 2023, doi: 10.1109/TITS.2022.3168806.

[8] M. Ibrar, L. Wang, N. Shah, O. Rottenstreich, G.-M. Muntean, and A. Akbar, "Reliability-aware flow distribution algorithm in SDN-enabled fog computing for smart cities," *IEEE Trans. Veh. Technol.*, vol. 72, no. 1, pp. 573–588, Jan. 2023, doi: 10.1109/TVT.2022.3202195.

[9] C. K. Dehury, S. N. Srirama*, P. K. Donta, and S. Dustdar, "Securing clustered edge intelligence with blockchain," *IEEE Consum. Electron. Mag.*, vol. 13, no. 1, pp. 22–29, Jan. 2024, doi: 10.1109/MCE.2022.3164529.

[10] T. Alladi, V. Chamola, N. Sahu, V. Venkatesh, A. Goyal, and M. Guizani, "A comprehensive survey on the applications of blockchain for securing vehicular networks," *IEEE Commun. Surveys Tut.*, vol. 24, no. 2, pp. 1212–1239, 2nd Quart., 2022, doi: 10.1109/COMST.2022.3160925.

[11] X. Li, X. Yin, and J. Ning, "Trustworthy announcement dissemination scheme with blockchain-assisted vehicular cloud," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 1786–1800, Feb. 2023, doi: 10.1109/TITS.2022.3220580.

[12] K. Gai et al., "Blockchain-based privacy-preserving positioning data sharing for IoT-enabled maritime transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2344–2358, Feb. 2023, doi: 10.1109/TITS.2022.3190487.

[13] G. Elghazaly, R. Frank, S. Harvey, and S. Safko, "High-definition maps: Comprehensive survey, challenges, and future perspectives," *IEEE Open J. Intell. Transp. Syst.*, vol. 4, pp. 527–550, 2023, doi: 10.1109/OJITS.2023.3295502.

[14] K. Dulaj, A. Alhammadi, I. Shayea, A. A. El-Saleh, and M. Alnakhli, "Harnessing machine learning for intelligent networking in 5G technology and beyond: Advancements, applications and challenges," *IEEE Open J. Intell. Transp. Syst.*, vol. 6, pp. 605–633, 2025, doi: 10.1109/OJITS.2025.3564361.

[15] S. Sai, V. Chamola, K.-K. R. Choo, B. Sikdar, and J. J. P. C. Rodrigues, "Confluence of blockchain and artificial intelligence technologies for secure and scalable healthcare solutions: A review," *IEEE Internet Things J.*, vol. 10, no. 7, pp. 5873–5897, Apr. 2023, doi: 10.1109/JIOT.2022.3232793.

[16] J. Du, E. Gelenbe, C. Jiang, H. Zhang, and Y. Ren, "Contract design for traffic offloading and resource allocation in heterogeneous ultra-dense networks," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 11, pp. 2457–2467, Nov. 2017, doi: 10.1109/JSAC.2017.2760459.

[17] T. Abera et al., "C-FLAT: control-flow attestation for embedded systems software," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2016, pp. 743–754, doi: 10.1145/2976749.2978358.

[18] D. D. Chen, M. Woo, D. Brumley, and M. Egele, "Towards automated dynamic analysis for Linux-based embedded firmware," in *Proc. NDSS*, 2016, p. 1.

[19] A. Francillon and C. Castelluccia, "Code injection attacks on Harvard-architecture devices," in *Proc. 15th ACM Conf. Comput. Commun. Secur.*, 2008, pp. 15–26, doi: 10.1145/1455770.1455775.

[20] R. Roemer, E. Buchanan, H. Shacham, and S. Savage, "Return-oriented programming: Systems, languages, and applications," *ACM Trans. Inf. Syst. Secur.*, vol. 15, no. 1, pp. 1–34, 2012, doi: 10.1145/2133375.2133377.

[21] H. Alemzadeh, D. Chen, X. Li, T. Kesavadas, Z. T. Kalbarczyk, and R. K. Iyer, "Targeted attacks on teleoperated surgical robots: Dynamic model-based detection and mitigation," in *Proc. 46th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, 2016, pp. 395–406, doi: 10.1109/DSN.2016.43.

[22] V. N. Gudivada, S. Ramaswamy, and S. Srinivasan, "Data management issues in cyber-physical systems," in *Transportation Cyber-Physical Systems*. Amsterdam, The Netherlands: Elsevier, 2018, pp. 173–200, doi: 10.1016/B978-0-12-814295-0.00007-1.

[23] F. Shrouf, J. Ordieres, and G. Miragliotta, "Smart factories in industry 4.0: A review of the concept and of energy management approached in production based on the Internet of Things paradigm," in *Proc. IEEE Int. Conf. Ind. Eng. Eng. Manag.*, 2014, pp. 697–701, doi: 10.1109/IEEM.2014.7058728.

[24] J. Blocki, B. Harsha, and S. Zhou, "On the economics of offline password cracking," in *Proc. IEEE Symp. Security Privacy (SP)*, 2018, pp. 853–871, doi: 10.1109/SP.2018.00009.

[25] L. Davi, A. Dmitrienko, A.-R. Sadeghi, and M. Winandy, "Privilege escalation attacks on android," in *Proc. 13th Int. Conf. Inf. Secur.*, 2010, pp. 346–360, doi: 10.1007/978-3-642-18178-8_30.

[26] J. Owens and J. Matthews, "A study of passwords and methods used in brute-force SSH attacks," in *Proc. USENIX Workshop Large-Scale Exploits Emergent Threats (LEET)*, 2008, pp. 1–8.

[27] M. Bellare and T. Kohno, "Hash function balance and its impact on birthday attacks," in *Proc. Int. Conf. Theory Appl. Cryptogr. Tech. Adv. Cryptol. (EUROCRYPT)*, 2004, pp. 401–418, doi: 10.1007/978-3-540-24676-3_24.

[28] P. Papantonakis, D. Pnevmatikatos, I. Papaefstathiou, and C. Manifavas, "Fast, FPGA-based Rainbow Table creation for attacking encrypted mobile communications," in *Proc. 23rd Int. Conf. Field Program. Logic Appl.*, 2013, pp. 1–6, doi: 10.1109/FPL.2013.6645525.

[29] A. Narayanan and V. Shmatikov, "Fast dictionary attacks on passwords using time-space tradeoff," in *Proc. 12th ACM Conf. Comput. Commun. Secur.*, 2005, pp. 364–372, doi: 10.1145/1102120.1102168.

[30] S. Kumar, "Smurf-based distributed denial of service (DDoS) attack amplification in Internet," in *Proc. 2nd Int. Conf. Internet Monit. Prot. (ICIMP)*, 2007, pp. 25–25, doi: 10.1109/ICIMP.2007.42.

[31] M. Al-Shurman, S. M. Yoo, and S. Park, "Black hole attack in mobile ad hoc networks," in *Proc. 42nd Annu. ACM Southeast Conf.*, 2004, pp. 96–97, doi: 10.1145/986537.986560.

[32] F. Yihunie, E. Abdelfattah, and A. Odeh, "Analysis of ping of death DoS and DDoS attacks," in *Proc. IEEE Long Island Syst., Appl. Technol. Conf. (LISAT)*, 2018, pp. 1–4, doi: 10.1109/LISAT.2018.8378010.

[33] C. Sun, K. Lv, C. Hu, and H. Xie, "A double-layer detection and classification approach for network attacks," in *Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, 2018, pp. 1–8, doi: 10.1109/ICCCN.2018.8487460.

[34] M. Mut-Puigserver, M. A. Cabot-Nadal, and M. M. Payeras-Capellà, "Removing the trusted third party in a confidential multiparty registered eDelivery protocol using blockchain," *IEEE Access*, vol. 8, pp. 106855–106871, 2020, doi: 10.1109/ACCESS.2020.3000558.

[35] T. Li, M. Shang, S. Wang, and R. Stern, "Detecting subtle cyber-attacks on adaptive cruise control vehicles: A machine learning approach," *IEEE Open J. Intell. Transp. Syst.*, vol. 6, pp. 11–23, 2025, doi: 10.1109/OJITS.2024.3522969.

[36] S. Gries, M. Hesenius, and V. Gruhn, "Cascading data corruption: About dependencies in cyber-physical systems: poster," in *Proc. 11th ACM Int. Conf. Distrib. Event-Based Syst.*, 2017, pp. 345–346, doi: 10.1145/3093742.3095092.

[37] A. Di Ferdinando, P. Ezhilchelvan, M. Dales, and J. Crowcroft, "A QoS-negotiable middleware system for reliably multicasting messages of arbitrary size," in *Proc. 9th IEEE Int. Symp. Object Component-Orient. Real-Time Distrib. Comput. (ISORC)*, 2006, p. 8, doi: 10.1109/ISORC.2006.10.

[38] S. Goel and B. Nussbaum, "Attribution across cyber attack types: Network intrusions and information operations," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1082–1093, 2021, doi: 10.1109/OJCOMS.2021.3074591.

[39] M. L. Thomas, "Maritime hacking using land-based skills," in *Proc. 14th Int. Conf. Cyber Confl., Keep Mov.! (CyCon)*, 2022, pp. 249–263, doi: 10.23919/CyCon55549.2022.9811049.

[40] I. Ashraf et al., "A survey on cyber security threats in IoT-enabled maritime industry," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2677–2690, Feb. 2023, doi: 10.1109/TITS.2022.3164678.

[41] M. S. Awan and M. A. Al Ghamdi, "Understanding the vulnerabilities in digital components of an integrated bridge system (IBS)," *J. Mar. Sci. Eng.*, vol. 7, no. 10, p. 350, 2019, doi: 10.3390/jmse7100350.

[42] Z. Shauk. "Malware on the offshore rig: Danger lurks where the chips fail." 2013, Accessed: May 15, 2025. [Online]. Available: https://www.houstonchronicle.com/business/energy/article/Malware-on-the-offshore-rig-Danger-lurks-where-4470723.php

[43] V. L. Do, L. Fillatre, I. Nikiforov, and P. Willett, "Security of SCADA systems against cyber–physical attacks," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 32, no. 5, pp. 28–45, May 2017, doi: 10.1109/MAES.2017.160047.

[44] M. Brunner, H. Hofinger, C. Krauß, C. Roblee, P. Schoo, and S. Todt, *Infiltrating Critical Infrastructures with Next-Generation Attacks*, Fraunhofer Inst. Secure Inf. Technol., Munich, Germany, 2010.

[45] M. P. Gopinath et al., "A secure cloud-based solution for real-time monitoring and management of Internet of underwater things (IOUT)," *Neural Comput. Appl.*, vol. 31, no. 1, pp. 293–308, 2019, doi: 10.1007/s00521-018-3774-9.

[46] A. Yazdinejad, R. M. Parizi, G. Srivastava, A. Dehghantanha, and K.-K. R. Choo, "Energy efficient decentralized authentication in Internet of underwater things using blockchain," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, 2019, pp. 1–6, doi: 10.1109/GCWkshps45667.2019.9024475.

[47] B. B. Gupta, A. Gaurav, C.-H. Hsu, and B. Jiao, "Identity-based authentication mechanism for secure information sharing in the maritime transport system," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2422–2430, Feb. 2023, doi: 10.1109/TITS.2021.3125402.

[48] X. Hou, Y. Li, M. Chen, D. Wu, D. Jin, and S. Chen, "Vehicular fog computing: A viewpoint of vehicles as the infrastructures," *IEEE Trans. Veh. Technol.*, vol. 65, no. 6, pp. 3860–3873, Jun. 2016, doi: 10.1109/TVT.2016.2532863.

[49] S. B. Prathiba, G. Raja, A. K. Bashir, A. A. AlZubi, and B. Gupta, "SDN-assisted safety message dissemination framework for vehicular critical energy infrastructure," *IEEE Trans. Ind. Informat.*, vol. 18, no. 5, pp. 3510–3518, May 2022, doi: 10.1109/TII.2021.3113130.

[50] A. Trichili, C. B. Issaid, B. S. Ooi, and M.-S. Alouini, "A CNN-based structured light communication scheme for Internet of Underwater Things applications," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10038–10047, Oct. 2020, doi: 10.1109/JIOT.2020.2988979.

[51] F. Mirsadeghi, M. K. Rafsanjani, and B. B. Gupta, "A trust infrastructure based authentication method for clustered vehicular ad hoc networks," *Peer Peer Netw. Appl.*, vol. 14, pp. 2537–2553, Jul. 2021, doi: 10.1007/s12083-020-01010-4.

[52] S. Khan, A. Jadhav, I. Bharadwaj, M. Rooj, and S. Shiravale, "Blockchain and the identity based encryption scheme for high data security," in *Proc. 4th Int. Conf. Comput. Methodol. Commun. (ICCMC)*, 2020, pp. 1005–1008, doi: 10.1109/ICCMC48092.2020.ICCMC-000187.

[53] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surveys Tut.*, vol. 21, no. 1, pp. 858–880, 1st Quart., 2019, doi: 10.1109/COMST.2018.2863956.

[54] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-enabled smart contracts: Architecture, applications, and future trends," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 11, pp. 2266–2277, Nov. 2019, doi: 10.1109/TSMC.2019.2895123.

[55] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tut.*, vol. 21, no. 2, pp. 1676–1717, 2nd Quart., 2019, doi: 10.1109/COMST.2018.2886932.

[56] L. Wang, S. Xiaoying, L. Jing, S. Jun, and Y. Yixian, "Cryptographic primitives in blockchains," in *J. Netw. Comput. Appl.*, vol. 127, pp. 43–58, Feb. 2019, doi: 10.1016/j.jnca.2018.11.003.

[57] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of Blockchain-based applications: current status, classification and open issues," *Telematics Inform.*, vol. 36, pp. 55–81, Mar. 2019, doi: 10.1016/j.tele.2018.11.006.

[58] Z. Liu et al., "A survey on blockchain: A game theoretical perspective," *IEEE Access*, vol. 7, pp. 47615–47643, 2019, doi: 10.1109/ACCESS.2019.2909924.

[59] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Commun. Surveys Tut.*, vol. 20, no. 4, pp. 3416–3452, 4th Quart., 2018, doi: 10.1109/COMST.2018.2842460.

[60] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the Internet of Things: Research issues and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019, doi: 10.1109/JIOT.2018.2882794.

[61] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, Jul. 2018, doi: 10.1109/TKDE.2017.2781227.

[62] Y. Li, X. Cheng, Y. Cao, D. Wang, and L. Yang, "Smart choice for the smart grid: Narrowband Internet of Things (NB-IoT)," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1505–1515, Jun. 2018, doi: 10.1109/JIOT.2017.2781251.

[63] N. Ahmed, D. De, and I. Hussain, "Internet of Things (IoT) for smart precision agriculture and farming in rural areas," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4890–4899, Dec. 2018, doi: 10.1109/JIOT.2018.2879579.

[64] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018, doi: 10.1016/j.future.2017.11.022.

[65] R. R. Mukkamala, R. Vatrapu, P. K. Ray, G. Sengupta, and S. Halder, "Blockchain for social business: Principles and applications," *IEEE Eng. Manag. Rev.*, vol. 46, no. 4, pp. 94–99, 4th Quart., 2018, doi: 10.1109/EMR.2018.2881149.

[66] Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the Internet of Things," *Peer Peer Netw. Appl.*, vol. 10, pp. 983–994, Jul. 2017, doi: 10.1007/s12083-016-0456-1.

[67] N. Hackius and M. Petersen, "Blockchain in logistics and supply chain: trick or treat?" in *Proc. Digit. Supply Chain Manag. Logist., Smart Digit. Solut. Ind. Environ. Hambg. Int. Conf. Logist. (HICL)*, 2017, pp. 3–18, doi: 10.15480/882.1444.

[68] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Security Privacy Workshops*, 2015, pp. 180–184, doi: 10.1109/SPW.2015.27.

[69] D. R. Shah, D. A. Dhawan, and V. Thoday, "An overview on security challenges in cloud, fog, and edge computing," in *Proc. Data Sci. Secur. IDSCS*, 2022, pp. 337–345, doi: 10.1007/978-981-19-2211-4_29.

[70] F. Firouzi, B. Farahani, and A. Marinšek, "The convergence and interplay of edge, fog, and cloud in the AI-driven Internet of Things (IoT)," *Inf. Syst.*, vol. 107, Jul. 2022, Art. no. 101840, doi: 10.1016/j.is.2021.101840.

[71] N. Lasla, M. Al-Ammari, M. Abdallah, and M. Younis, "Blockchain based trading platform for electric vehicle charging in smart cities," *IEEE Open J. Intell. Transp. Syst.*, vol. 1, pp. 80–92, 2020, doi: 10.1109/OJITS.2020.3004870.

[72] K. Emura, S. Katsumata, and Y. Watanabe, "Identity-based encryption with security against the KGC: A formal model and its instantiations," *Theor. Comput. Sci.*, vol. 900, pp. 97–119, Sep. 2022, doi: 10.1016/j.tcs.2021.11.021.

[73] R. A. Mallah, D. López, and B. Farooq, "Cyber-security risk assessment framework for blockchains in smart mobility," *IEEE Open J. Intell. Transp. Syst.*, vol. 2, pp. 294–311, 2021, doi: 10.1109/OJITS.2021.3106863.

[74] A. Alrajhi, K. Roy, L. Qingge, and J. Kribs, "Detection of road condition defects using multiple sensors and IoT technology: A review," *IEEE Open J. Intell. Transp. Syst.*, vol. 4, pp. 372–392, 2023, doi: 10.1109/OJITS.2023.3237480.

[75] S. S. Chow, "Removing escrow from identity-based encryption: New security notions and key management techniques," in *Proc. Int. Workshop Public Key Cryptogr.*, 2009, pp. 256–276, doi: 10.1007/978-3-642-00468-1_15.

[76] J. Hur, D. Koo, S. O. Hwang, and K. Kang, "Removing escrow from ciphertext policy attribute-based encryption," *Comput. Math. Appl.*, vol. 65, no. 9, pp. 1310–1317, 2013, doi: 10.1016/j.camwa.2012.02.005.

[77] J. Hur, "Improving security and efficiency in attribute-based data sharing," *IEEE Trans. Knowl. Data Eng.*, vol. 25, no. 10, pp. 2271–2282, Oct. 2013, doi: 10.1109/TKDE.2011.78.

[78] Y. Wang, H. Zhong, Y. Xu, J. Cui, and G. Wu, "Enhanced security identity-based privacy-preserving authentication scheme supporting revocation for VANETs," *IEEE Syst. J.*, vol. 14, no. 4, pp. 5373–5383, Dec. 2020, doi: 10.1109/JSYST.2020.2977670.

[79] I. Ali, T. Lawrence, and F. Li, "An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs," *J. Syst. Archit.*, vol. 103, Feb. 2020, Art. no. 101692, doi: 10.1016/j.sysarc.2019.101692.

[80] S. Tangade, S. S. Manvi, and P. Lorenz, "Trust management scheme based on hybrid cryptography for secure communications in VANETs," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5232–5243, May 2020, doi: 10.1109/TVT.2020.2981127.

[81] L. Zhang, X. Meng, K.-K. R. Choo, Y. Zhang, and F. Dai, "Privacy-preserving cloud establishment and data dissemination scheme for vehicular cloud," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 3, pp. 634–647, May/Jun. 2020, doi: 10.1109/TDSC.2018.2797190.

[82] L. Zhang, "OTIBAAGKA: A new security tool for cryptographic mix-zone establishment in vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 12, pp. 2998–3010, 2017, doi: 10.1109/TIFS.2017.2730479.

[83] J. Cui, J. Zhang, H. Zhong, and Y. Xu, "SPACF: A secure privacy-preserving authentication scheme for VANET with cuckoo filter," *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 10283–10295, Nov. 2017, doi: 10.1109/TVT.2017.2718101.

[84] S.-F. Tzeng, S.-J. Horng, T. Li, X. Wang, P.-H. Huang, and M. K. Khan, "Enhancing security and privacy for identity-based batch verification scheme in VANETs," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3235–3248, Apr. 2017, doi: 10.1109/TVT.2015.2406877.

[85] N.-W. Lo and J.-L. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 5, pp. 1319–1328, May 2016, doi: 10.1109/TITS.2015.2502322.

[86] Q. Huang and D. S. Wong, "Generic certificateless encryption secure against malicious-but-passive KGC attacks in the standard model," *J. Comput. Sci. Technol.*, vol. 25, pp. 807–826, Jul. 2010, doi: 10.1007/s11390-010-9367-4.

[87] G. Yang and C. H. Tan, "Certificateless cryptography with KGC trust level 3," *Theor. Comput. Sci.*, vol. 412, no. 39, pp. 5446–5457, 2011, doi: 10.1016/j.tcs.2011.06.015.

[88] W. Yang, F. Zhang, and L. Shen, "Efficient certificateless encryption withstanding attacks from malicious KGC without using random oracles," *Secur. Commun. Netw.*, vol. 7, no. 2, pp. 445–454, 2014, doi: 10.1002/sec.826.
[89] Y.-H. Hung, S.-S. Huang, Y.-M. Tseng, and T.-T. Tsai, "Efficient anonymous multireceiver certificateless encryption," *IEEE Syst. J.*, vol. 11, no. 4, pp. 2602–2613, Dec. 2017, doi: 10.1109/JSYST.2015.2451193.
[90] S. Garg, M. Hajiabadi, M. Mahmoody, and A. Rahimi, "Registration-based encryption: Removing private-key generator from IBE," in *Proc. 16th Int. Conf. Theory Cryptogr. (TCC)*, 2018, pp. 689–718, doi: 10.1007/978-3-030-03807-6_25.
[91] S. Garg, M. Hajiabadi, M. Mahmoody, A. Rahimi, and S. Sekar, "Registration-based encryption from standard assumptions," in *Proc. 22nd IACR Int. Workshop Public Key Cryptogr.*, 2019, pp. 63–93, doi: 10.1007/978-3-030-17259-6_3.
[92] M. A. Simplicio Jr., M V. M. Silva, R. C. A. Alves, and T. K. C. Shibata, "Lightweight and escrow-less authenticated key agreement for the Internet of Things," *Comput. Commun.*, vol. 98, pp. 43–51, Jan. 2017, doi: 10.1016/j.comcom.2016.05.002.
[93] Q. Wei, F. Qi, and Z. Tang, "Remove key escrow from the BF and Gentry identity-based encryption with non-interactive key generation," *Telecommun. Syst.*, vol. 69, pp. 253–262, May 2018, doi: 10.1007/s11235-018-0461-1.
[94] D. Abbasinezhad-Mood, A. Ostad-Sharif, S. M. Mazinani, and M. Nikooghadam, "Provably secure escrow-less Chebyshev chaotic map-based key agreement protocol for vehicle to grid connections with privacy protection," *IEEE Trans. Ind. Informat.*, vol. 16, no. 12, pp. 7287–7294, Dec. 2020, doi: 10.1109/TII.2020.2974258.
[95] P. Li, J. Su, and X. Wang, "iTLS: Lightweight transport-layer security protocol for IoT with minimal latency and perfect forward secrecy," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6828–6841, Aug. 2020, doi: 10.1109/JIOT.2020.2988126.
[96] F. Haidar, M. Makassikis, M. Sall, H. Bakhti, A. Kaiser, and B. Lonc, "Experimentation and assessment of pseudonym certificate management and misbehavior detection in C-ITS," *IEEE Open J. Intell. Transp. Syst.*, vol. 2, pp. 128–139, 2021, doi: 10.1109/OJITS.2021.3085366.
[97] J. Yang, J. Liu, H. Song, J. Liu, and X. Lei, "Blockchain-based conditional privacy-preserving authentication protocol with implicit certificates for vehicular edge computing," in *Proc. 7th Int. Conf. Cloud Comput. Big Data Analytics (ICCCBDA)*, 2022, pp. 210–216, doi: 10.1109/ICCCBDA55098.2022.9778897.

HAFIZ MUHAMMAD WASEEM received the B.S. degree in electronics engineering from the COMSATS Institute of Information Technology in 2014, the M.S. degree in electrical engineering from the Institute of Space Technology, Pakistan, in 2018, and the Ph.D. degree in computer engineering from Gachon University, South Korea, in 2023. He worked in the telecommunications sector as an assistant manager from 2014 to 2018 and later served as an Assistant Professor with Gachon University from 2024 to 2025. He is currently affiliated with the Warwick Manufacturing Group, University of Warwick, U.K. His research focuses on quantum computing, information security, and quantum AI.

NOOR MUNIR received the B.S. degree in mathematics from the University of Wah, Pakistan, in 2017, and the M.S. and Ph.D. degrees in mathematics from the Institute of Space Technology (IST), Islamabad, in 2022 and 2019, respectively. She is a Postdoctoral Research Fellow with the Department of Engineering Sciences, University of Oxford. She was an Assistant Professor with the Department of Information Security, Gachon University, South Korea, from 2023 to 2024. From 2017 to 2022, she worked as a Research Associate with the Cyber and Information Security Lab, IST. Her research interests include AI threat detection, red teaming, cryptanalysis, and machine learning–based vulnerability assessment.

SEONG OUN HWANG (Senior Member, IEEE) received the B.S. degree in mathematics from Seoul National University in 1993, the M.S. degree in information and communications engineering from the Pohang University of Science and Technology in 1998, and the Ph.D. degree in computer science from the Korea Advanced Institute of Science and Technology, South Korea. He worked as a Software Engineer with LGCNS Systems, Inc., from 1994 to 1996. He also worked as a Senior Researcher with the Electronics and Telecommunications Research Institute (ETRI) from 1998 to 2007. He worked as a Professor with the Department of Software and Communications Engineering, Hongik University from 2008 to 2019. He is currently a Professor with the Department of Computer Engineering, Gachon University. His research interests include cryptography, cybersecurity, and artificial intelligence. He is also an Editor of *ETRI Journal*.