Ad Hoc Networks 166 (2025) 103669

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

AI-optimized elliptic curve with Certificate-Less Digital Signature for zero trust maritime security

Mohammed Al-Khalidi [a,*], Rabab Al-Zaidi [b], Tarek Ali [a], Safiullah Khan [a], Ali Kashif Bashir [a]

[a] *Department of Computing and Mathematics, Manchester Metropolitan University, Manchester, UK*
[b] *School of Science, Engineering and Environment, University of Salford, Salford, Manchester, UK*

ARTICLE INFO

Keywords:
Internet of Marine Things
Zero trust security
Certificate-less digital signature
Elliptic Curve Cryptography
Artificial intelligence
Genetic Algorithm
Particle Swarm Optimization

ABSTRACT

The proliferation of sensory applications has led to the development of the Internet of Things (IoT), which extends connectivity beyond traditional computing platforms and connects all kinds of everyday objects. Marine Ad Hoc Networks are expected to be an essential part of this connected world, forming the Internet of Marine Things (IoMaT). However, marine IoT systems are often highly distributed, and spread across large sparse areas which makes it challenging to implement and manage centralized security measures. Despite some ongoing efforts to establish network connectivity in such environment, securing these networks remains an unreached goal. The use of Certificate-Less Digital Signatures (CLDS) with Elliptic Curve Cryptography (ECC) shows great promise in providing secure communication in these networks and achieving zero trust IoMaT security. By eliminating the need for certificates and associated key management infrastructure, CLDS simplifies the key management process. ECC also enables secure communication with smaller key sizes and faster processing times, which is crucial for resource-limited IoMaT devices. In this paper, we introduce CLDS using ECC as a means of securing IoT networks in a marine environment, creating a zero trust security framework for Internet of Marine Things (IoMaT). To increase security and robustness of the framework, we optimize the ECC parameters using two vital artificial intelligence algorithms, namely Genetic Algorithm (GA) and Particle Swarm Optimization (PSO). Evaluation results demonstrate a reduction in ECC parameter generation time by over 40% with GA optimization and 20% with PSO optimization. Additionally, the computational cost and memory usage for major ECC attacks increased significantly by up to 40% and 67% for Rho attacks, 34% and 53% for brute-force attacks, and 30% and 67% for improved hybrid attacks, respectively.

1. Introduction

The proliferation of internet-connected devices, such as sensors, machines, and cameras that form the Internet of Things (IoT), is rapidly increasing. According to the International Data Corporation (IDC), it is projected that there will be around 41.6 billion interconnected IoT devices, producing 79.4 zettabytes (ZB) of data by 2025 [1]. In line with this, the IoT is seeking to interconnect built-in sensors to collect and act upon data across a marine network. The UK Office of Communications (Ofcom) has included Very High Frequency (VHF) in the radio spectrum allocated for IoT applications as part of the upcoming 6G Networks. This move is aimed at encouraging Machine-to-Machine (M2M) communication and facilitating wireless connectivity over longer distances [2]. However, as the Internet of Marine Things (IoMaT) expands its capabilities to include advanced applications such as fleet management, cargo tracking, and container temperature monitoring; ensuring its security is becoming increasingly crucial. Presently, the marine system lacks mechanisms for data integrity and security, relying solely on trust. The current management of vessel tracking and collision avoidance in the marine environment relies on the Automatic Identification System (AIS), a maritime electronic system that enables ships and other vessels to automatically transmit and receive information such as their identity, position, speed, and course. However, AIS was developed in the 1990s when cybersecurity threats were not a significant concern, and it lacks any authentication or encryption measures, rendering it vulnerable to cyber attacks [3]. Although extensive research has been conducted to enhance the security of the AIS in marine data communication, the safety of its usage has not been fully guaranteed due to its critical security vulnerabilities. Our previous work in [4] has revealed that the AIS has no inherent security and contains numerous easily exploitable flaws. AIS functions as a self-reporting system that utilizes VHF radio links in the marine environment, making it susceptible to falsification, especially when the

[*] Corresponding author.
E-mail address: m.al-khalidi@mmu.ac.uk (M. Al-Khalidi).

https://doi.org/10.1016/j.adhoc.2024.103669
Received 14 May 2024; Received in revised form 27 August 2024; Accepted 17 September 2024
Available online 3 October 2024

message's authentication is not included in the system's architecture. Furthermore, like their onshore equivalents, marine onboard information technology and operational technology systems are susceptible to hacking, and such breaches could pose a significant danger to the safety and security of ships, ports, marine facilities, consumers, and other components of the maritime transportation system [5]. Cyber attacks on critical infrastructure, such as transportation, have emerged as one of the top five risks in 2020. These attacks have become more frequent in various sectors, including healthcare and energy, and have even caused disruptions in entire cities [6].

IoMaT security faces many challenges inherited from the marine environment that consists of vast bodies of water such as oceans and seas. In such environment, setting up a fixed infrastructure for secure communication, including public key infrastructure (PKI) and the associated key distribution and management is challenging and expensive. Our previous work in [7] shows that Marine Ad-hoc Networks are considered the most efficient and cost-effective networking solution for the IoMaT. They allow ships to communicate with each other using Very High Frequency (VHF) and the AIS system already available on majority of ships without the need for a centralized infrastructure. These networks are formed dynamically based on the proximity of ships which makes them well-suited for environments where the network structure is unpredictable. However, this needs to be coupled with an efficient security solution that is becoming vital in such zero trust environment with emerging IoMaT services such as cargo tracking and temperature monitoring.

To address the challenges of IoMaT zero trust security identified above, this paper proposes the use of Identity-Based Encryption (IBE) solutions such as Certificate-Less Digital Signatures (CLDS) that eliminate the need for a PKI. IBE is a type of public-key cryptography that simplifies the key management aspect of traditional public-key cryptography by using easily human-readable identities as public keys [8]. In traditional public-key cryptography, users need to obtain and manage public keys from a central authority or a PKI. In IBE or IBE based CLDS systems, users can use identities such as email addresses or usernames directly as public keys [9]. IBE based CLDS is particularly suitable for ad hoc networks due to its inherent characteristics that align with the challenges posed by such dynamic and decentralized environments.

Another challenge for IoMaT zero trust security is the low bandwidth offered by marine VHF technology, which operates at 9600 bps. Therefore, it is necessary to keep key lengths to minimum [10]. To address this challenge, this paper proposes using Elliptic Curve Cryptography (ECC) with IBE based CLDS which provides a high level of security with shorter key lengths compared to traditional cryptosystems like RSA. ECC operations are computationally more efficient compared to operations in finite fields used in other public-key cryptosystems [11]. This efficiency is crucial in IBE based CLDS systems, where frequent key operations may be required, especially in dynamic and rapidly changing environments like ad hoc networks.

1.1. Paper contributions

In summary, the key contributions of our work are as follows:

- The proposal of a zero trust security framework for IoMaT using IBE based CLDS. In ad hoc networks, where nodes may join or leave dynamically, managing traditional public–private key pairs becomes challenging. IBE based CLDS simplifies this process, making key distribution more flexible and scalable by eliminating the need for certificates and associated key management infrastructure.
- To increase the efficiency and security of the cryptographic operations, we use ECC and optimize its parameters using two Artificial Intelligence (AI) algorithms, namely Genetic Algorithm (GA) and Particle Swarm Optimization (PSO). These algorithms are known for their ability to explore large solution spaces. With our proposed solution, they are used to optimize the key generation processes by searching through different parameter configurations and tuning the ECC parameters. Evaluation results show 20%–40% reduction in ECC parameter generation time, and an increase in computational cost and memory usage for major ECC attacks by up to 40% and 67% for Rho, Brute-Force, and improved hybrid attacks respectively.
- The evaluations presented in the paper also provide valuable insights into ECC attacks' performance and attack vector optimization in zero trust environments. An improved hybrid attack was designed to overcome the limitations of the Rho attack and Brute-Force attack. This assault sought to achieve a middle ground between the probabilistic characteristics of the Rho assault and the deterministic characteristics of the Brute-Force attack. The enhanced Assault demonstrated competitive performance metrics, encompassing a reasonable memory utilization, and computational expenditure between Rho and Brute-Force as demonstrated in the evaluation section.

The remaining sections of this paper are organized as follows. Section 2 presents the related work, while a background is presented in Section 3 including the vulnerabilities of IoT marine sensory data in 3.1, an overview of Elliptic Curve Cryptography in 3.2, and a discussion on Identity Based Encryption and the related key escrow problem in 3.3. The proposed framework and zero trust security model of IoMaT is presented in Section 4, while the experimentation and results evaluation is detailed in Section 5. Finally, the paper is concluded in Section 6.

2. Related work

The sensory information gathered by maritime navigation systems is at high risk of being compromised by a cyber attack, which is now considered to be just as dangerous as a physical attack on these systems. This represents a significant shift in the threat landscape for maritime navigation systems. Efforts are underway to enhance the security and reliability of Automatic Identification System (AIS) data [12]. A potential solution to improve the security of the AIS and achieve message integrity and broadcast authentication is to introduce an authentication protocol. However, implementing a shared session key may result in high communication overhead [13]. In [14] an authentication protocol was introduced to enhance the security of the AIS. This protocol is founded on the principles of Timed Efficient Stream Loss-tolerant Authentication (TESLA), which not only ensures message integrity and authentication but also has the capability to endure packet loss. Other efforts [15,16] focus on improving authenticity and confidentiality within the network by eliminating computational delays and bolstering the verification of mobile nodes. [17] suggests AISChain, which is an AIS data platform based on blockchain technology. To ensure the legitimacy of the data origin, AISChain employs a consortium blockchain, allowing only authorized parties to engage, and permitting only validated AIS data to be logged within the chain. However, Blockchain systems usually face scalability issues, especially when dealing with a large volume of data transactions, as is often the case with AIS marine data. In [18] the authors examine the AIS landscape as a crucial information source for enhancing Maritime Situational Awareness (MSA). They pinpoint its weaknesses and obstacles in ensuring secure navigation and shipping, with a special emphasis on the threat of spoofing. In [19] a suggested framework enables the classification of different vulnerability types, attacks, and exploits, along with their potential impact, which can vary from severe (such as threats to vessel stability and safety) to less significant (like a decrease in entertainment or service quality). This framework used a taxonomy that supports the creation of adversarial cyber models, risk mitigation, and resiliency plans as applied to the maritime industry, using the AIS as a specific illustration of the approach.

There are also methods that seek to employ a central authority to verify the identity of AIS data providers through the issuance of certificates. To support the security of AIS, a combination of Public Key Cryptography and Identity-Based Authentication and encryption schemes have been employed [20]. Although these methods hold promise for addressing the security concerns of current AIS, they face notable challenges in terms of message overhead and key exchanges, in addition to the key escrow problem. In [21] a trusted party, referred to as a notary, has been utilized to validate certificates as well. Convergence allows notaries at the client side to validate communications with websites. This method minimizes the vulnerability in case a Certificate Authority is compromised, but it comes at the cost of a substantial increase in network traffic. Clients have the ability to identify attacks by comparing records with an unauthenticated key. Because the effectiveness of notary-based methods depends on the notary servers, it is crucial that these servers have sufficient resources, especially when it comes to bandwidth capacity.

Numerous efforts have been dedicated to enhancing the security and pinpointing vulnerabilities in AIS data and the maritime domain. Table 1 categorizes the relevant research in this field based on the research methodology, strengths, and weaknesses. It is important to acknowledge that although these approaches hold promise in resolving security concerns associated with the marine environment, they are only effective for small clusters of authorized users and are burdened by high message overhead requirements and key exchanges. Our proposed framework utilizes a different technology than the current AIS, serving as a carrier for our data through VHF technology. We employ AI to optimize the keys generated using ECC in CLDS, addressing the IBE key escrow problem. Our novel framework offers security and authentication for all the sensory data collected in the marine environment.

3. Background

IoT has experienced rapid growth over the past decade, with projections suggesting that there will be over 41.6 billion connected IoT devices by 2025 [1]. However, security has been identified as a major weakness in the growth of IoT [33].

3.1. Vulnerability of IoT marine sensory data

Marine security involves a range of security requirements, including authentication and confidentiality. Despite its widespread use, the current AIS system used in the marine industry is not secure, leaving it vulnerable to various types of attacks, including spoofing. The AIS protocol is designed to exchange short messages with a specific format, but these messages are shared on the same AIS channel. When the AIS protocol was first created, the primary aim was to enable the sharing of location data between all vessels and shore stations, with no regard for security at the time. However, securing the data has become essential to prevent potential crises. For instance, since July 2018, thousands of false signals resulting from Global Navigation Satellite System (GNSS) spoofing have been detected in Shanghai, highlighting the urgent need for security measures in the marine industry [34]. In 2019, more than 20 coastal sites in southern China were subject to spoofing attacks [34]. Additionally, the locations of twelve ships as reported by their AIS were inaccurate by thousands of miles and they appeared to be moving in a circular area northwest of San Francisco [35]. The US Department of Homeland Security, the Pentagon, and the Commerce Department have been advised to limit their use of GPS systems for positioning and navigation due to the risks associated with hacking [36].

Manipulating GPS data to deceive ships into believing that they are located elsewhere is a significant security concern, and extensive research is being conducted to find a solution to this problem [37–39]. As IoT applications and use cases are emerging, marine data networks and applications are increasingly being foreseen as an integral part of the IoT picture. Therefore, a secure and reliable communication system at sea is becoming a pressing requirement to enable a wide range of Internet of Marine Things (IoMaT) applications and use cases including but not limited to sensory data acquisition and cartography systems, IoMaT supply chain and warehouse management, crew safety and welfare, marine habitat and conservatory zone protection, etc.

Our proposed solution aims is to ensure the authenticity and confidentiality of IoMaT data. To achieve this, we propose leveraging the IBE algorithm and Elliptic Curve Cryptography (ECC). This approach will provide unambiguous evidence that AIS messages are authentic and can be trusted in the IoMaT.

3.2. Elliptic curve cryptography

Elliptic curve cryptography (ECC) is a robust cryptographic method that was introduced by Koblitz [41] and Miller [42] in the 1980s. This approach offers excellent security with minimal key size. For instance, a 160-bit ECC key can provide the same level of security as a 1024-bit RSA key, as demonstrated in Table 2. ECC has been utilized to create various cryptographic protocols and schemes for devices with limited resources, such as smart cards, PDAs, and smart devices. It has attracted significant interest in recent years, especially in the development of key agreement, digital signature, encryption, and user authentication techniques that are relevant in areas such as IoT, cloud computing, VANET, wireless networks, and more [43].

All public key cryptosystems rely on a mathematically complex problem that is difficult to solve. By "difficult to solve," we mean that even with the most advanced computers available today, it is still impractical in terms of time and resources to solve the problem. Popular public key cryptosystems like Rivest–Shamir–Adleman (RSA) and Diffie–Hellman are based on the challenge of factoring large integers or solving discrete logarithm problems. In contrast, Elliptic Curve Cryptography operates on the properties of points on an elliptic curve, making it distinct from these other cryptosystems [44]. Due to the relatively high computing resources needed to compute discrete logarithms, elliptic curve cryptosystems can significantly reduce the size of encryption keys. This smaller key size results in faster execution of various cryptographic operations. Research indicates that the generation of RSA keys takes significantly longer than elliptic curve-based cryptosystems with a comparable level of security, as shown in Table 2

Elliptic curve-based cryptosystems offer several benefits compared to RSA cryptosystems:

- Smaller Key Sizes: The keys used in elliptic curve-based cryptosystems are much smaller than those used in RSA cryptosystems for the same level of security. For example, an elliptic curve cryptosystem with a key length of 233 bits provides the same level of security as an RSA cryptosystem with a key length of 2240 bits. This makes elliptic curve-based cryptosystems more efficient in terms of computation and storage [45].
- Superior performance in cryptographic operations, such as key and digital signature generation. Due to the smaller size of keys, these operations can be carried out significantly faster than RSA. For example, generating a key of size 233 bits in ECC is approximately 40 times faster than generating a key of size 2240 bits in RSA [46].
- Resistance to attacks: Elliptic curve cryptography is less susceptible to certain types of attacks, such as those based on the number field sieve algorithm for integer factorization, which is a threat to RSA [47].
- Lower power consumption: Elliptic curve cryptography requires fewer CPU cycles and less power consumption than RSA, making it a better choice for battery-powered devices [46].
- Elliptic curve cryptography is believed to be more resistant to quantum computing attacks than RSA, making it a more future-proof option for long-term security [48,49].

Table 1
An overview of research in marine security.

Ref.	Method	Strengths	Weaknesses
[12]	Focuses on improving AIS data security	Enhances security and reliability of AIS data	General approach, no specific solution provided
[13]	Introduces shared session key for AIS authentication	Improves message integrity and broadcast authentication	High communication overhead
[14]	Timed Efficient Stream Loss tolerant Authentication	Ensures message integrity, authentication, and endures packet loss	High implementation complexity
[15], [16]	Eliminates computational delays and enhances node verification	Strengthens network security	Specific details on methodology not provided
[17]	Uses consortium blockchain for AIS data legitimacy	Ensures legitimacy of data origin; validates AIS data	Scalability issues with large data volumes
[18]	Examines AIS vulnerabilities	Identifies weaknesses and obstacles in secure navigation	Focus on vulnerability identification, not on specific mitigation
[19]	Provides a taxonomy for vulnerability types, attacks, and impacts	Supports creation of cyber models, risk mitigation, and resiliency plans	Framework approach, no immediate practical solution
[21]	Notary-based certificate validation	Reduces vulnerability if Certificate Authority is compromised	Increases network traffic, relies on server resources
[22]	Enhances maritime cybersecurity using drone tech and 5G	Utilization of drone technology with 5G for enhanced security	Scalability issues, high network congestion, unclear robustness against real-world attacks
[23]	PKC methods are used for securing AIS	Proposes Protected AIS software to address security vulnerabilities in AIS	The proposed method faces challenges in public key distribution and scalability, making it ineffective for a global AIS network.
[24]	Proposed S3 information-sharing scheme and analyzed the e-Navigation architecture and AIS communication	Introducing a 3-step authentication process and explicit ship-to-ship authentication using Maritime Mobile Service Identity (MMSI).	No specific measures to prevent unauthorized access or additional security requirements beyond SR-1 are mentioned.
[25]	Proposed Threshold Level Hierarchical Identity-Based Signature (TLHIBS) scheme with batch verification for ADS-B	Proposed an efficient TLHIBS scheme, demonstrated its security, and implemented batch verification	TLHIBS schemes are not well-suited for practical deployment due to their complexity. They require a resource-intensive hash-to-point operation and involve costly certification management.
[26], [27], [7]	Proposes a novel IoT-enabled system for marine data acquisition and cartography based on Ship Ad-hoc Networks (SANET's)	Proposes novel low-cost AIS system using existing ship infrastructure.	No attempt to address the security of the proposed IoT system in the marine environment.
[28]	Identity-Based Public Cryptography, Three-tiered security approach for AIS.	Proposed maritime IBC for AIS security enhancement.	Limited scope of security considerations and the complexity of implementing Public Key Infrastructure (PKI) in global maritime environments.
[29]	Certificateless IBC to enhance AIS security.	Proposes a scheme using self-generated authentication certificates and anonymous signatures to improve energy-efficient ship verification.	The scheme's security relies on secure channels, which, if compromised, endanger the entire system.
[30]	Proposed a framework for vessel delay prediction using logistic regression to address data-sharing challenges in maritime law enforcement.	Uses Cheon-Kim-Kim-Song (CKKS) homomorphic encryption for confidential data sharing and machine learning training.	Homomorphic encryption's high computational cost limits its use in large-scale machine learning, like CNNs.
[31]	Prevent AIS spoofing and ensure message integrity	Proposed PKC authentication system for AIS messages to prevent spoofing by addressing Replay attacks.	High communication overhead and slow implementation process
[32]	Proposed protocol: multitarget authentication, key exchange for secure communication	End-to-end authentication transmission model with device and server responsibilities	Lack of data authenticity verification methods at the receiving end

Table 2
RSA vs ECC: Key length comparison [40].

Security (In Bits)	RSA Key Length Required	ECC Key Length Required	Generation time RSA (second)	Generation time ECC (second)
80	1024	160	0.16	0.08
112	2048	224	7.47	0.18
128	2048	256	9.89	0.27
192	3072	384	133.90	0.64
256	15 360	521	679.06	1.44

3.3. *Identity base encryption*

In IoMaT systems, the use of well-known identifiers, such as a node ID, as public keys allows for the encoding of security policies directly into encryption and authentication methods. This eliminates the need for certificates and Certification Authorities, which can be challenging to manage. In 1984, Adi Shamir presented the idea of IBC, a public key cryptography system that employs everyday identifiers like email addresses or phone numbers in place of public keys to perform encryption and verify signatures. This strategy simplifies cryptographic systems by eliminating the necessity of creating and overseeing user certificates and the associated expensive infrastructure. It also simplifies cryptography for unprepared users, as messages can be encrypted for users before they interact with any system components. The result is a powerful encryption solution that is easy to implement and manage, without the overhead and cost inherent in traditional security solutions [50]. Overall, IBE offers a powerful encryption solution that is both easy to implement and manage [50]. IBE relies on a trusted third party called the Private Key Generator (PKG), which generates a public/private key pair at the beginning of the process. The public key is then made available to all users of the system and is referred to as the master public key, while the private key is kept by the PKG and is referred to as the master private key.

One of the main advantages of IBE is that it eliminates the need for managing a public key infrastructure, which can be a complex and costly process. Additionally, since the PKG handles all cryptographic operations, there is no need for client-side installation, which makes the system more user-friendly. Another benefit is that messages and keys do not need to be backed up or stored for extended periods of time, which simplifies the storage, backup, and recovery process [51]. Without a PKI, there is less public information that could be revealed to those who do not have a need to know it. In a PKI system, every application or individual linked to the certificate repository might potentially gain extensive insights into the infrastructure. However, this capability might not be necessary for most applications [50]. Despite the advantages discussed above, a main disadvantage of using IBC is its key escrow property, where the Key Generation Centre (KGC) has knowledge of every user's private key. This gives the PKG significant power to impersonate any user. While some applications may activate this property for the benefit of database recovery in case a user's private key is lost, in many other applications (including our IoMaT application) it is considered a major vulnerability where the centralization of private keys raises major security and privacy concerns. If the PKG was to be compromised or compelled to disclose the private keys, it could lead to unauthorized access to encrypted data and misuse of sensitive information. We have eliminated this vulnerability in our IoMaT application by using certificate-less public key cryptography (CL-PKC), as discussed in Section 4.

4. IoMaT zero trust framework and security model

In this section, we will provide a brief overview of the proposed zero trust framework and security model for the IoMaT. The proposed scheme is based on IBE using Certificate-Less Public Key Cryptography (CL-PKC) proposed in [52] to enhance the security of the AIS marine data acquisition system and ensure the authenticity and confidentiality of the data transmitted through the network. We further add a timestamp method for signature generation, which helps to prevent the threat of *replay attack*.

The proposed scheme is based on elliptic curve cryptography (ECC) and incorporates two important features of CL-PKC, namely, encryption and signature through scalar multiplication, which simplifies the cryptographic process. Additionally, it only requires a single hash function, while other similar schemes require multiple complicated mapping functions. These properties provide significant advantages over existing schemes and make the proposed scheme a promising solution for the current AIS marine data acquisition system.

Below, we discuss the key features of this framework and how it addresses the security challenges associated with the current AIS marine data acquisition system.

4.1. *IoMaT shared key and private key generation scheme*

In IBE based CL-PKC, the use of master public keys and master private keys plays a crucial role in the derivation of user-specific public and private keys, and also helps address the challenges associated with key management and distribution. It allows for efficient and secure key generation without the need for a centralized certificate authority. A user's private key consists of two parts, the first part is the partial private key corresponding to the ID which is generated by the KGC, and the other part is derived from the first. It is generated by the users themselves and is unknown to others. The user further selects a public key associated with this self-generated private key.

In the proposed IoMaT system, each network node (ship) obtains the shared keys (master private key and master public key) from the sink node (SN) on shore before starting its operation in what we refer to as an offline activity. The SN acts as the PKG and as a marine cryptography data collector at the same time, as illustrated in the Fig. 1. The Sink Node (SN) will also act as a verifier of messages sent by ships, while the ships will act as signers as shown in Fig. 1. This eliminates the need for a Trusted Third Party (TTP) in certificate generation, and the shared key is generated based on public system parameters. The main components of the proposed IoMaT Security framework are detailed below:

- **PKG:** Trusted third party (in our scenario the SN), it is tasked with the responsibility of creating system parameters and generating partial private keys for all nodes associated with the IoMT system.
- **Signer:** The collector of sensory data (ships), that will generate the signature and the encrypted message.
- **Verifier:** The SN which will receive all the encrypted messages and the signatures from ships in the IoMT system. SN will verify the message–signature pair and decrypt the received messages to extract the sensory information.

For our IoMaT system, we build on the efficient IBE based CL-PKC scheme proposed in [53], where readers interested in the mathematical concepts of the scheme are referred to. Table 3 defines the mathematical terms and abbreviations used in the algorithms specifically adapted for our IoMaT system below.

- **Setup:** This algorithm is run by the PKG in the Sink Node (SN). It is used to set up a certificate-less public key system. According to the security parameter l, an elliptic curve E over the finite field F_q is defined by the set of parameters (q, a, b, G, n, h), hence l determines the level of security (e.g., key length). The system's master private key *mpk* is selected randomly by the PKG from the interval [1, n-1] and should be kept secret by the SN/PKG. The SN/PKG also computes the master public key *msk*, where $msk = mpk \times G$. The system public parameters *params* are: $\{F\_q,\ E/F\_q,\ G,\ msk,\ H\}$. The Sink Public Key, Sink ID, and public parameters

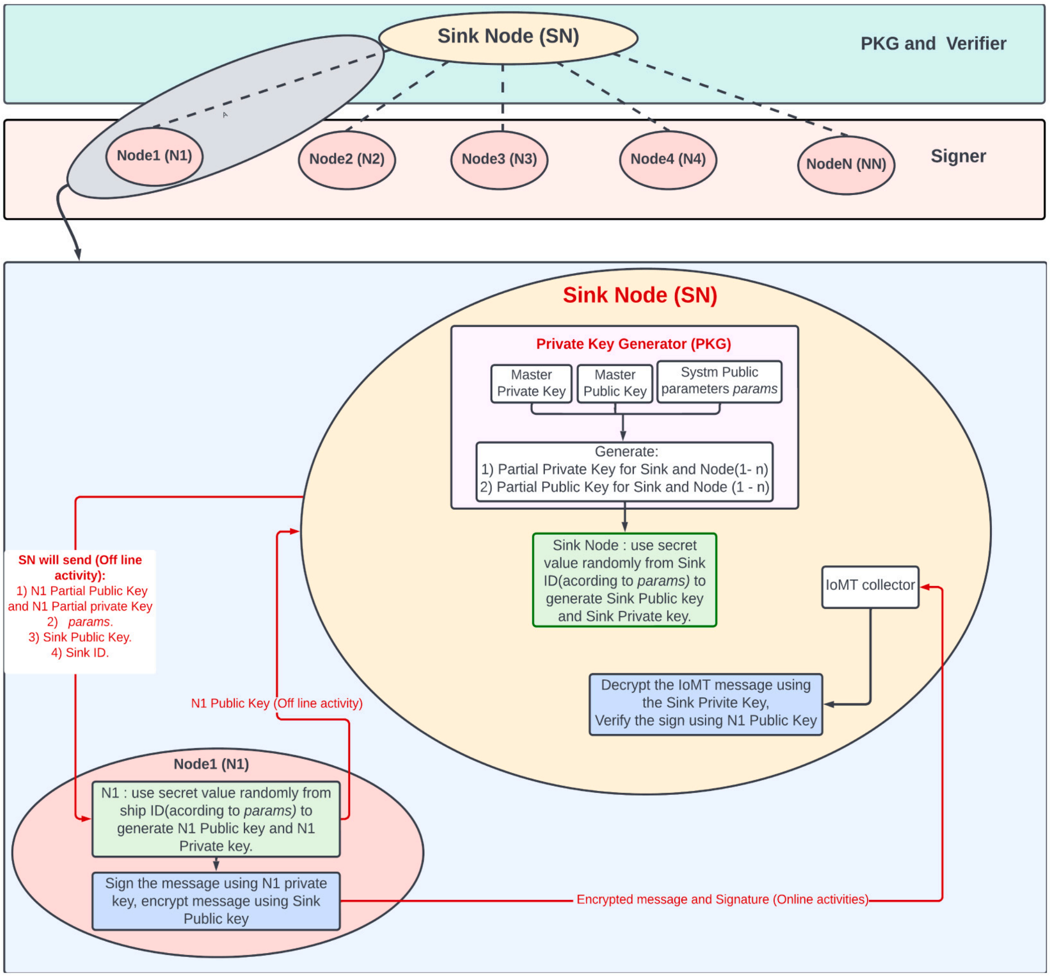
Sink Node (SN)
PKG and Verifier
Node1 (N1)
Node2 (N2)
Node3 (N3)
Node4 (N4)
NodeN (NN)
Signer
Sink Node (SN)
Private Key Generator (PKG)
Master Private Key
Master Public Key
Systm Public parameters *params*
Generate:
1) Partial Private Key for Sink and Node(1- n)
2) Partial Public Key for Sink and Node (1 - n)
Sink Node : use secret value randomly from Sink ID(acording to *params)* to generate Sink Public key and Sink Private key.
IoMT collector
Decrypt the IoMT message using the Sink Privite Key, Verify the sign using N1 Public Key
SN will send (Off line activity):
1) N1 Partial Public Key and N1 Partial private Key
2) *params*.
3) Sink Public Key.
4) Sink ID.
N1 Public Key (Off line activity)
Node1 (N1)
N1 : use secret value randomly from ship ID(acording to *params)* to generate N1 Public key and N1 Private key.
Sign the message using N1 private key, encrypt message using Sink Public key
Encrypted message and Signature (Online activities)

Fig. 1. Zero trust framework and Security model of IoMaT.

params should be known by all ships. This setup procedure can be expressed as:

$$params, msk, mpk, ID = \text{Setup}(1^l). \tag{1}$$

- **Partial Key Extraction:** This algorithm is also run in the SN by the PKG, which takes the system parameters *params*, master private key and a Node ID (ship ID) as input and outputs a partial private key d_{ID} and a partial public key R_{ID}. The partial key extraction algorithm can be represented as:

  $$(d_{ID}, R_{ID}) = \text{PartialKeyExtract}(params, mpk, ID). \tag{2}$$

  This ensures that the user's private key is dependent on their identity, but since the full private key also requires the user's secret input (generated by the user independently), the PKG does not have full control over the user's private key. This addresses the key escrow problem present in IBE.
- **Key Generation:** This algorithm is run by the nodes (ships). In this phase, the ship combines the partial private key obtained from the PKG with their own secret information to generate the complete key pair: the private key and the public key. Each ship should first: choose a secret value Z_{ID} randomly for a ship ID according to the system public parameters *params*. Secondly: generate the private key S_{ID} for a ship ID from *params*, d_{ID}, Z_{ID} and ID. Finlay: construct the public key P_{ID} according to *params*, R_{ID}, and Z_{ID}. The key generation algorithm can be represented as:

  $$(S_{ID}, P_{ID}) = \text{Keygeneration}(params, partialkey, Z_{ID}, ID). \tag{3}$$
- **Encryption:** This algorithm represents the encryption process used to secure the message m so that it can be safely transmitted to the SN. It is also run by the ship (IoMaT sensory data collector), which takes *params*, the receiver's ID (SN ID), the SN public key P_{ID}, and the IoMaT message m to be encrypted as input, and outputs a cipher text c which is the encrypted IoMaT message. The encryption algorithm can be represented as:

  $$c = \text{Encryption}(params, P_{ID}, ID, m). \tag{4}$$
- **Decryption:**
  The decryption algorithm is run by the receiver (SN), which takes *params*, SN ID, SN private key S_{ID}, and the cipher text (IoMaT encrypted Message) c as input, and outputs the corresponding plain text m. The SN ID is used both in the encryption and decryption processes, ensuring that the keys are bound to the SN's identity. The decryption algorithm can be represented as:

  $$m = \text{Decryption}(params, S_{ID}, ID, c). \tag{5}$$

4.2. IoMaT signing and verification scheme

The IoMaT authentication process involves verifying the ownership of sensory data collected by participating ships. Overall, this authentication scheme ensures that only authorized ships can collect and sign the sensory data, and the authenticity of the data can be verified by the shore stations. To sign and verify the IoMaT sensory data, the following algorithms are utilized:

Table 3
Definition of the terms and abbreviations used in the IoMaT security model.

Notation	Description
PKG	Private Key Generator
IBC	Identity Base Encryption
CL-PKC	CertificateLess Public Key Cryptography
IoMaT	Internet of Marine Things
params	Public system parameters for the certificate-less public key system
l	The security parameter in the certificate-less public key system refers to the bit size of the private key used in the ECC algorithm.
q	A large prime
F_q	A finite field with q elements (0, q-1)
E	An elliptic curve over the finite field F_q, who should have a subgroup with a large prime order.
G	A base point on the elliptic curve E
$data_{IoMaT}$	IoMaT sensory data
m_{IoMaT}	IoMaT message
SN	Sink Node
n	A large prime, which is defined to be the order of a subgroup on E
s	The master private key of the certificate-less public key system
H	A cryptographic hash function, who can map arbitrary strings to strings of l bits
msk	The master public key of the certificate-less public key system
d_{ID}	Partial private key
R_{ID}	Partial public key
$Time_{IoMaT}$	Time stamp for the IoMaT sensory data
S_{ID}	Signatory's private key
mpk	The system's master private key, which is selected randomly from the interval [1, n-1] by the PKG and should be kept secret by the Sink Node (PKG)
Z_{ID}	Secret value generated in each node randomly for a ship ID according to the system public parameters *params*
P_{ID}	Public key for ship ID which is generated by key generation algorithm from system public parameters, partial public key of the ship and secret value of the node which is generated randomly for each node
S_{ID}	Private key for ship ID which is generated by key generation algorithm from system public parameters, partial private key of the ship and secret value of the node which is generated randomly for each node

- **Signature:** This algorithm is run by the ship (generator of the IoMaT sensory data). The ship first needs to attach the IoMaT data with the time to generate the IoMaT message as shown in equation (6) below:

$$m_{IoMaT} = (data_{IoMaT}, Time_{IoMaT}) \tag{6}$$

  Then hash m_{IoMaT} to generate the digest. The ship will encrypt the digest (message) using *params*, the signatory's ID, and the signatory's private key S_{ID} to generate the encrypted message (digital signature), which will be attached with the time again to generate the final signature of the IoMaT message as shown below:

$$S_{IoMaT} = ((Hash(m_{IoMaT}), params, ID, S_{ID}), Time_{IoMaT}) \tag{7}$$

- **Verifying Authentication:** This algorithm is run by the message receiver (SN), which takes *params*, the master public key msk, the signatory's ID, the signatory's public key P_{ID}, message m_{IoMT} and its signature S_{IoMT} as input, and outputs the verification result as authentic or unauthentic.
  To verify the authenticity of an IoMaT message, first, the IoMaT signature message S_{IoMaT} is split into its digital signature and time of IoMaT message $Time_{IoMaT}$. Then, the digital signature is decrypted using the corresponding public key of the asymmetric key-pair to recover the original digest $Hash(m_{IoMaT})$. This digest is then compared with another digest generated by attaching the IoMaT data m_{IoMaT} (recovered by decryption in Section 4.2 above) to the time of IoMaT message (separated from S_{IoMaT}), and hashing the composed message. If both digests match, then the IoMaT data is considered genuine. If the digests do not match, the message is considered to be forged, and it is ignored, as shown in Fig. 2. Any attempt to modify the IoMT data, time, or signature will result in an erroneous digest and an unauthenticated message, indicating the possibility of a spoofing attack or a public key tampering attack. In such cases, the system will automatically ignore the message.

4.3. Optimizing elliptic curve cryptography with artificial intelligence

ECC can be applied to various cryptographic operations such as encryption, key exchange, and digital signatures, and forms the foundation of our IoMaT framework and security model. In addition to the advantages of ECC detailed in Section 3.2, Machine Learning algorithms can be used to analyze large datasets, identify patterns, and make informed decisions about the selection of optimal ECC parameters, leading to more efficient and secure cryptographic systems [54]. To reach optimum optimization results, it is important to clearly define the optimization objectives, such as minimizing computation time, maximizing security, or achieving a balance between security and efficiency. The appropriate machine learning model will depend on the nature of the optimization task [55]. In this paper, Genetic Algorithms (GAs) and Particle Swarm Optimization (PSO) [56] have been used to optimize the ECC parameters that underpin the IBE based CLDS (also known as Certificate-Less Public Key Cryptography (CL-PKC) scheme) explained throughout Section 4 above.

Genetic Algorithms [57] are primarily used for optimization and search problems. Unlike traditional machine learning algorithms that learn from data, GAs operate on a population of potential solutions to iteratively evolve and improve those solutions over multiple generations. These characteristics of GAs make them well-suited for the challenges associated with optimizing ECC parameters. The selection of optimal

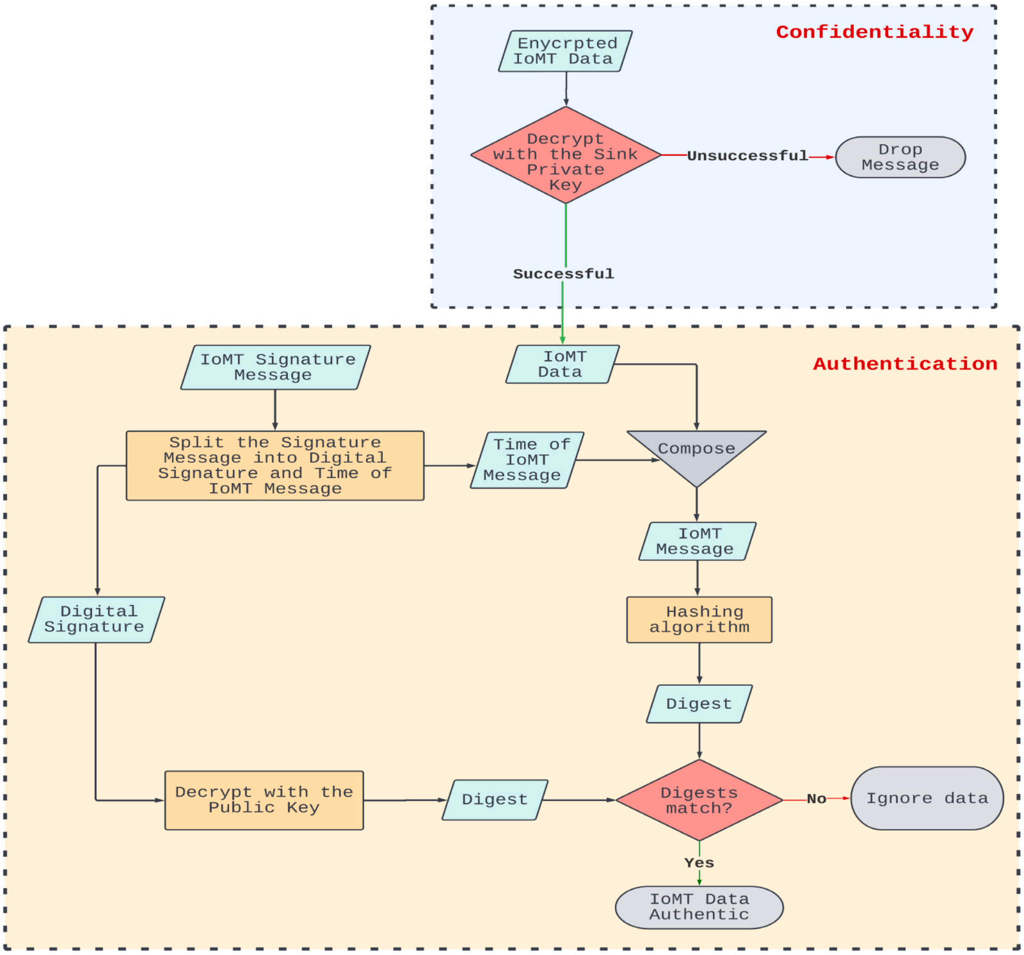

Fig. 2. Verifying the confidentiality and the authentication of IoMaT data.

ECC parameters often involves exploring a high-dimensional solution space. GAs excel at navigating and searching such spaces, making them effective for finding solutions that meet specific optimization criteria. Solutions that perform well according to defined objectives are more likely to be selected for reproduction, leading to a convergence towards optimal or near-optimal solutions over time. Algorithm 1 shows the steps required for ECC Parameter Generation using Genetic Algorithm.

Algorithm 1 Genetic Algorithm for ECC Parameter Generation

```
Input: Population size, number of generations, mutation rate
Initialize population with random parameters
Define target ECC parameters (e.g., prime curve order and generator)
Define fitness function
for $gen = 1$ to generations do
    Evaluate fitness for each individual in the population
    Select individuals for reproduction (roulette wheel selection)
    Create the next generation through crossover
    Mutate some individuals in the new generation
    Replace old population with the new generation for selected indices
end for
Display the best parameters found
```

On the other hand, Particle Swarm Optimization (PSO) [58] is a stochastic optimization algorithm that uses a population of particles to iteratively explore the solution space. This stochastic nature helps PSO avoid getting stuck in local optima and encourages a more thorough exploration of the parameter space. PSO is designed for global optimization problems, where the objective is to find the global optimum in a search space. ECC parameter optimization often requires exploring a high-dimensional solution space for optimal parameter sets, and PSO excels at searching globally. Similar to GAs, PSO uses a population-based approach. The particles in PSO represent potential solutions, and their interactions help guide the exploration towards promising regions of the solution space. Algorithm 2 shows the steps required for ECC Parameter Generation using Particle Swarm Optimization.

5. Experimentation and results evaluation

In ECC, where the discrete logarithm problem is a fundamental security assumption, the choice of elliptic curve parameters is crucial to resist attacks. The experimentation presented in this section measures the security and robustness of AI-based ECC optimization for the IoMaT security framework proposed in this paper against three types of attacks, namely, Pollard's Rho Attack, Brute-Force Attack, and an Improved Hybrid Attack (combination of Rho and Brute-Force).

5.1. Experimentation environment and parameters

The experiment utilized a robust computing environment featuring an Intel(R) Xeon(R) Gold 5118 CPU @ 2.30GHz with dual processors, providing a combined processing power of 4.58 GHz. Accompanied by a substantial 320 GB of installed RAM, all of which was usable, the system boasted impressive memory capacity for handling complex computational tasks. The GPU employed was a powerful P5000

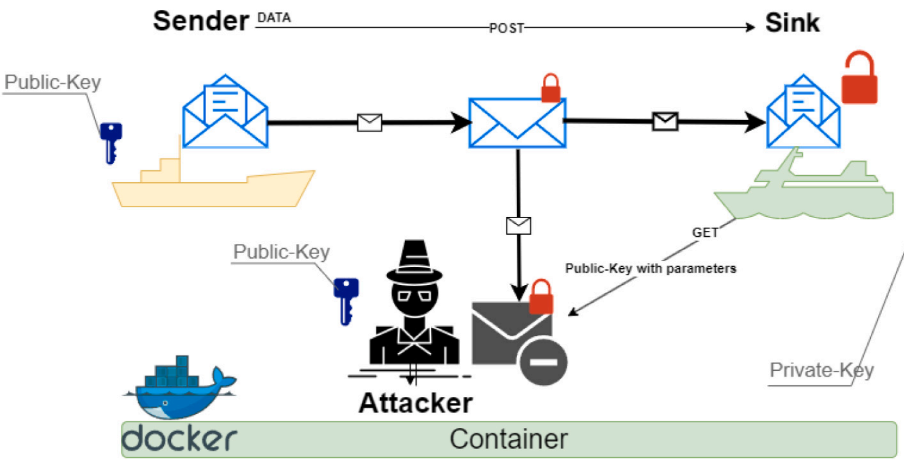

Fig. 3. Experiment of secure data transmission in IoMaT.

Algorithm 2 Particle Swarm Optimization for ECC Parameter Generation

```
Initialize population of particles with random elliptic curve parameters
Initialize velocity and position of each particle
Set personal best positions and fitness values for each particle
Set global best position and fitness value
for each iteration do
    for each particle do
        Update velocity using PSO formula & update position of particle
        Evaluate fitness of the particle based on ECC performance
        if fitness is better than personal best then
            Update personal best position and fitness
            if fitness is better than global best then
                Update global best position and fitness
            end if
        end if
    end for
end for
Result: Global best position represents optimized ECC parameter
```

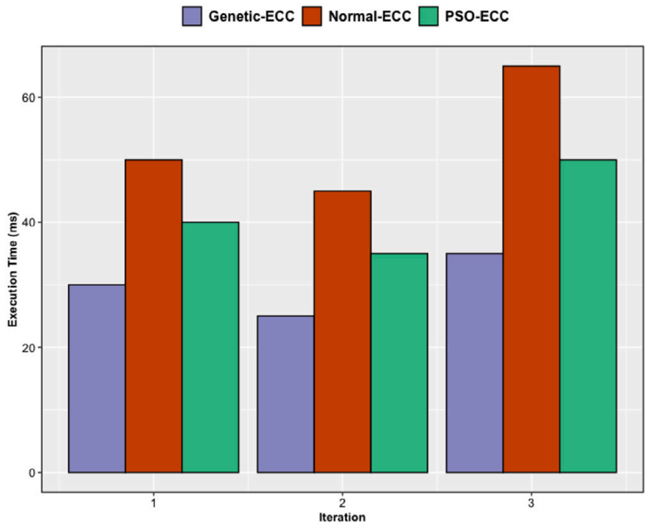

Fig. 4. Key generation execution times for normal, GA, and PSO optimized ECC.

16GB, enhancing the system's capabilities for graphics-intensive applications and parallel processing. Operating on a 64-bit system architecture with an x64-based processor, the experimental setup was geared towards high-performance computing, making it particularly suitable for tasks demanding substantial computational power and memory resources. The simulation of the experiment was conducted using both Python and MATLAB to leverage their computational modeling and data visualization.

The experiment assessed the effectiveness of the attacks on a short Weierstrass elliptic curve with the following parameters: $a = 2$, $b = 2$, $p = 17$, generator point $G = [5, 1]$, and order $n = 19$. These parameters define the elliptic curve used as the basis for our optimization experiments. The Normal ECC, GA Optimised ECC, and PSO optimized ECC algorithms were built in Python based on the implementation presented in [59]. The GA initializes a population of elements, and each element is a list representing potential ECC parameters. The parameters are the constants a and b, the prime number p, the generator point G representing points (x, y), the group order n and the cofactor h. New generations of elements are produced through iterative genetic operations including selection, crossover, and mutation. The PSO algorithm on the other hand initiates particles, where each particle is a list representing potential ECC parameters (same parameters as the GA above). The algorithm updates their velocities and positions, evaluates fitness, and identifies the best ECC parameter set through the optimal particle. Each run of the GA and PSO algorithms generates different ECC parameters with 256 bits. Examples of results from each algorithm are presented in Tables 4 and 5. Both GA and PSO algorithms utilize the same fitness function and include an early exit function if there is no improvement in the global best fitness for 20 iterations.

To simulate the IoMaT system, synthetic sensor readings were generated for the experiment. For each sample in the specified range, it creates a timestamp, a list of 14 random sensor values between 0 and 100, and a location identifier. Normal ECC, GA Optimised ECC, and PSO optimized ECC were used to generate the ECC parameters for IoMaT data encryption and authentication using IBE based CL-PKC as shown in Fig. 3.

5.2. Evaluation of ECC parameter generation time

Fig. 4 provides a comparison over three iterations between Normal ECC, GA Optimised ECC, and PSO optimized ECC in terms of execution time, i.e., the time required to generate a key. As shown in the figure, both optimization algorithms reduce the execution time as compared to normal ECC. GA optimized ECC provides the highest time saving, reducing the execution time by at least 40% followed by 20% for PSO optimized ECC. This demonstrates the effectiveness of the optimization

Table 4
Genetic algorithm elliptic curve parameters.

Parameter	Value
p	115767130820087599459538954692358951247030224109395739362935575451362653121881
a	82668451696756646536022584792679617953143499903333982127051599447032143644350
b	31262911590843934649816008012647167705950283794118219265317671124686435858889
G	(4, 85979675977080917334583745052287783606266506743942787408981321849099496180308)
n	115767130820087599459538954692358951247030224109395739362935575451362653121880
h	1

Table 5
Particle swarm optimization elliptic curve parameters.

Parameter	Value
p	83920875675429201076002743705901489967077637562817356440692877235699677907597
a	73916884511138539486074209032992425010519602193355559340498379053138310070272
b	18466552033214128305449972063322860268226711933935550031901591713321110 7328
G	(2, 52816158108397424543262331025570826905013942926608742347720195343450586800572)
n	115774182072552649979109848030856073124984770867872005566907726709010164875264
h	1

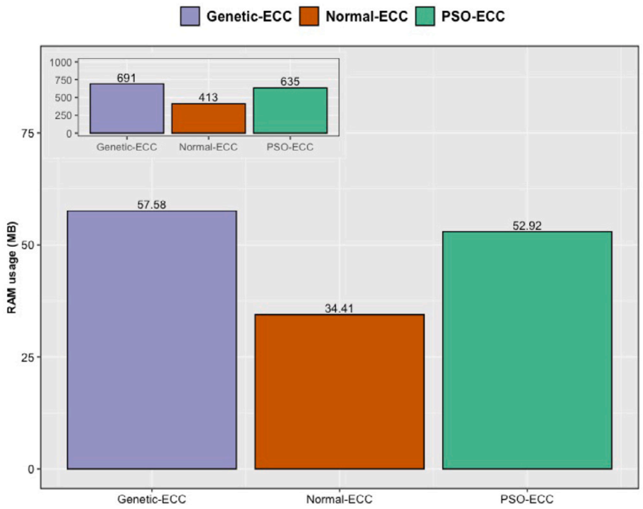

Fig. 5. Average and total memory usage for Rho attack against normal, GA, and PSO optimized ECC (inset graph shows the total).

algorithms in finding a set of parameters that lead to faster key generation while enhancing security properties (as can be seen from the following results).

5.3. Evaluation of ECC optimization performance against Rho Attack

The Rho Attack, also known as Pollard's Rho Algorithm, is a probabilistic algorithm used for solving the discrete logarithm problem, particularly in the context of elliptic curve cryptography (ECC) and modular arithmetic. The algorithm operates on a probabilistic basis, signifying that it does not assure a solution within a predetermined duration, but instead offers an anticipated running time with a high degree of certainty. Figs. 5 and 6 show the memory usage and computational cost for Rho Attack against Normal, GA, and PSO optimized ECC over 12 iterations. As can be seen from Fig. 5, GA optimized ECC increases the memory usage of Rho Attack by 67% on average and in total compared to 53% for PSO optimized ECC. On the other hand, GA optimized ECC increases the computational cost for Rho in terms of number of CPU cycles by 17% on average compared to approximately 40% for PSO optimized ECC as can be seen from Fig. 6.

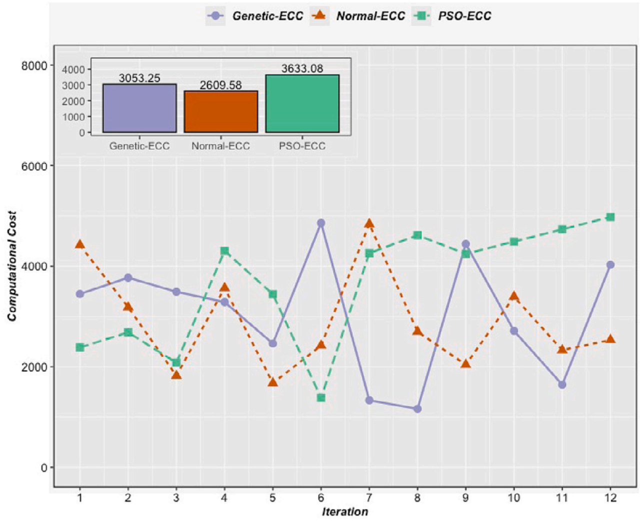

Fig. 6. Computational cost for Rho Attack against Normal, GA, and PSO optimized ECC (inset graph shows the average).

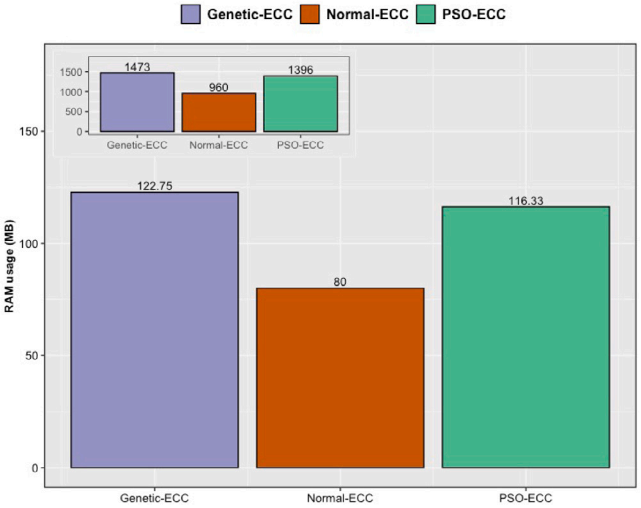

Fig. 7. Average and total memory usage for Brute-Force Attack against Normal, GA, and PSO optimized ECC (inset graph shows the total).

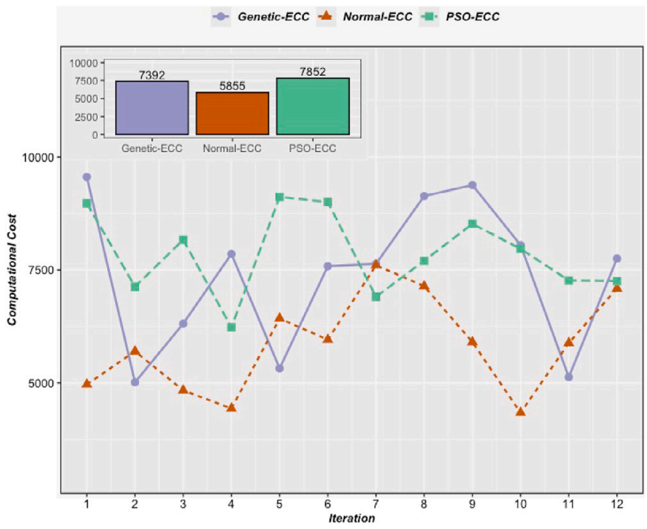

Fig. 8. Computational cost for Brute-Force Attack against Normal, GA, and PSO optimized ECC (inset graph shows the average).

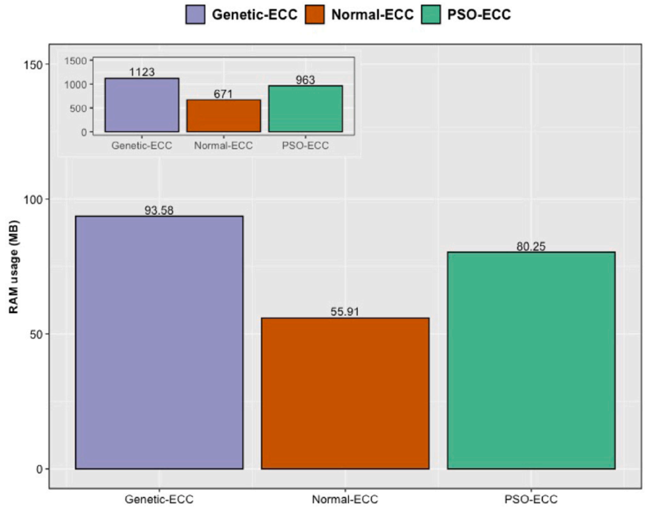

Fig. 9. Average and total memory usage for improved attack against Normal, GA, and PSO optimized ECC (inset graph shows the total).

5.4. Evaluation of ECC optimization performance against Brute-Force Attack

A Brute-Force Attack tries all possible keys until it gets the right one. The attack necessitates a comprehensive examination of every conceivable configuration, thereby rendering it 'theoretically' assured of success provided there is an ample allocation of temporal and computational assets. Such attack is highly time-consuming and resource-intensive, especially with large key sizes. Therefore, the attack demonstrated more significant computing expenses and memory use due to the extensive search approach as can be seen in Figs. 7 and 8. The figures show the memory usage and computational cost for Brute-Force Attack against Normal, GA, and PSO optimized ECC over 12 iterations. As can be seen from Fig. 7, GA optimized ECC increases the memory usage of Brute-Force Attack by 53% on average and in total compared to 45% for PSO optimized ECC. However, GA optimized ECC increases the computational cost for Brute-Force in terms of number of CPU cycles by 26% on average compared to approximately 34% for PSO optimized ECC as can be seen from Fig. 8.

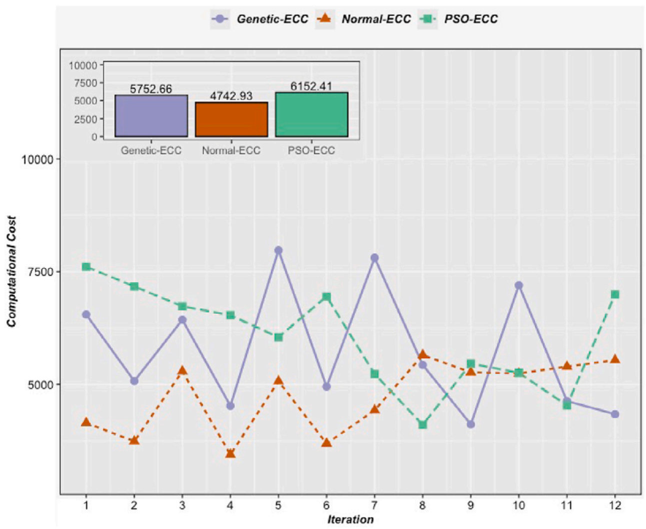

Fig. 10. Computational cost for improved attack against Normal, GA, and PSO optimized ECC (inset graph shows the average).

Table 6
Attack success rate.

ECC types	Attack types	Success per 1800 iteration
Normal	Rho	1
	Brute Force	✗
	Improved	1
Genetic	Rho	✗
	Brute Force	✗
	Improved	✗
PSO	Rho	✗
	Brute Force	✗
	Improved	✗

5.5. Evaluation of ECC optimization performance against improved attack

An Improved Attack was designed to overcome the limitations of the Rho Attack and Brute-Force Attack. This assault sought to achieve a middle ground between the probabilistic characteristics of the Rho assault and the deterministic characteristics of the Brute-Force Attack. That is, it takes probabilistic steps to decrease the size of the solution space and then applies brute force targeted in this smaller space. This means it is likely to create a resource demand that will be moderate relative to that of the pure Rho or Brute-Force methods, while maximizing attack efficiency and performance. The Enhanced Assault demonstrated competitive performance metrics, encompassing a reasonable memory utilization, and computational expenditure between Rho and Brute-Force as can be seen in Figs. 9 and 10. Ultimately, the evaluation offers valuable insights into the trade-offs involved in various attack methods on elliptic curves, considering parameters such as memory use and computational cost. As can be seen from Fig. 9, GA optimized ECC increases the memory usage of the improved attack by 67% on average and in total compared to 43% for PSO optimized ECC. On the other hand, GA optimized ECC increases the computational cost for the improved attack in terms of number of CPU cycles by 21% on average compared to approximately 30% for PSO optimized ECC as can be seen from Fig. 10.

5.6. Evaluation of Rho, brute-force, and improved attack success rate

Finally, Table 6 shows the total number of successful and failed attacks launched against Normal, GA optimized, and PSO optimized ECC over 1800 iterations for each type of attack. It can be clearly seen from the figure that no attack was able to succeed against any of the optimized ECC approaches. The only successful attacks observed were the Rho and Improved attack against Normal ECC parameter generation. Table 6 along with Figs. 4 to 10 demonstrate the efficiency of GA and PSO algorithms in increasing the security and robustness of ECC for the IoMaT security framework proposed in this paper.

6. Conclusions and future work

This paper has presented a framework and security model for the Internet of Marine Things (IoMaT) using CLDS with ECC which makes key generation and distribution more flexible and scalable. CLDS eliminates the need for certificates and associated key management infrastructure, while ECC enables secure communication with smaller key sizes and faster processing times. The presented solution solves the key escrow problem in current IBE proposals, and addresses the marine environment's unique challenges, such as network disruption and physical attacks on devices. To further increase security and robustness, we optimize the ECC parameters using two vital artificial intelligence algorithms, namely Genetic Algorithm (GA) and Particle Swarm Optimization (PSO). Evaluation results have shown a reduction in ECC parameter generation time by at least 20%, while increasing computational cost and memory usage for major ECC attacks by up to 40% and 67% respectively. The evaluations have not only demonstrated the efficiency of the solution, but also provided valuable insights into ECC attacks' performance and attack vector optimization. As future work, advanced techniques like Multi-Party Computation (MPC) could be employed to further mitigate the risk of forgery, where the generation of the partial private key involves multiple independent parties, reducing the risk that any single party (like the PKG) could forge keys.

CRediT authorship contribution statement

Mohammed Al-Khalidi: Writing – review & editing, Writing – original draft, Visualization, Validation, Software, Project administration, Formal analysis, Data curation, Conceptualization. **Rabab Al-Zaidi:** Writing – review & editing, Writing – original draft, Methodology, Investigation. **Tarek Ali:** Writing – original draft, Validation, Software, Data curation. **Safiullah Khan:** Writing – review & editing, Validation. **Ali Kashif Bashir:** Writing – review & editing, Supervision, Project administration.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

References

[1] V. Bozicevic, 41.6 Billion IoT devices will be generating 79.4 zettabytes of data in 2025, 2019.

[2] Ofcom, More radio spectrum for the Internet of Things, 2024, URL: http://stakeholders.ofcom.org.uk/consultations/radio-spectrum-internet-of-things/.

[3] S. Khandker, H. Turtiainen, A. Costin, T. Hämäläinen, Cybersecurity attacks on software logic and error handling within AIS implementations: A systematic testing of resilience, IEEE Access 10 (2022) 29493–29505.

[4] M. Al-Khalidi, R. Al-Zaidi, J. Woods, M. Reed, E. Pereira, Securing marine data networks in an IoT environment, in: 2019 7th International Conference on Future Internet of Things and Cloud (FiCloud), IEEE, 2019, pp. 125–132.

[5] International Maritime Organization, Maritime security and piracy 2022, 2024, URL: https://www.imo.org/en/OurWork/Security/Pages/MaritimeSecurity.aspx.

[6] World Economic Forum, Global risks report 2020, 2020, URL: https://reports.weforum.org/global-risks-report-2020/wild-wide-web/.

[7] R. Al-Zaidi, J.C. Woods, M. Al-Khalidi, H. Hu, Building novel VHF-based wireless sensor networks for the internet of marine things, IEEE Sens. J. 18 (5) (2018) 2131–2144.

[8] E.S. Babu, A.K. Dadi, K.K. Singh, S.R. Nayak, A.K. Bhoi, A. Singh, A distributed identity-based authentication scheme for internet of things devices using permissioned blockchain system, Expert Syst. 39 (10) (2022) e12941.

[9] M. Abdalla, E. Kiltz, G. Neven, Generalized key delegation for hierarchical identity-based encryption, in: Computer Security–ESORICS 2007: 12th European Symposium on Research in Computer Security, Dresden, Germany, September 24—26, 2007. Proceedings 12, Springer, 2007, pp. 139–154.

[10] S.P. Fuller, Satisfying naval low data rate mobile communication requirements, 1997, NASA 19980201757.

[11] K. Javeed, A. El-Mursy, D. Gregg, EC-crypto: Highly efficient area-delay optimized elliptic curve cryptography processor, IEEE Access (2023).

[12] R.E. Litts, D.C. Popescu, O. Popescu, Authentication protocol for enhanced security of the automatic identification system, Nav. Eng. J. 133 (4) (2021) 127–137.

[13] A. Aziz, P. Tedeschi, S. Sciancalepore, R. Di Pietro, SecureAIS-securing pairwise vessels communications, in: 2020 IEEE Conference on Communications and Network Security, CNS, IEEE, 2020, pp. 1–9.

[14] S. Sciancalepore, P. Tedeschi, A. Aziz, R. Di Pietro, Auth-AIS: secure, flexible, and backward-compatible authentication of vessels AIS broadcasts, IEEE Trans. Dependable Secure Comput. 19 (4) (2021) 2709–2726.

[15] S. Honarbakhsh, L.B.A. Latif, B. Emami, et al., Enhancing security for mobile ad hoc networks by using identity based cryptography, Int. J. Comput. Commun. Eng. 3 (1) (2014) 41.

[16] V.L. Narayana, C. Bharathi, Identity based cryptography for mobile ad hoc networks, J. Theor. Appl. Inf. Technol. 95 (5) (2017) 1173.

[17] Y. Duan, J. Huang, J. Lei, L. Kong, Y. Lv, Z. Lin, G. Chen, M.K. Khan, AISChain: Blockchain-based AIS data platform with dynamic bloom filter tree, IEEE Trans. Intell. Transp. Syst. (2022).

[18] A. Androjna, M. Perkovič, I. Pavic, J. Mišković, AIS data vulnerability indicated by a spoofing case-study, Appl. Sci. 11 (11) (2021) 5015.

[19] G.C. Kessler, J.P. Craiger, J.C. Haass, A taxonomy framework for maritime cybersecurity: A demonstration using the automatic identification system, TransNav: Int. J. Mar. Navig. Saf. Sea Transp. 12 (3) (2018) 429.

[20] A. Goudosis, S. Katsikas, Secure ais with identity-based authentication and encryption, TransNav: Int. J. Mar. Navig. Saf. Sea Transp. 14 (2) (2020) 287–298.

[21] A. Alrawais, A. Alhothaily, X. Cheng, C. Hu, J. Yu, SecureGuard: A certificate validation system in public key infrastructure, IEEE Trans. Veh. Technol. 67 (6) (2018) 5399–5408.

[22] A. Vangala, S. Agrawal, A.K. Das, S. Pal, N. Kumar, P. Lorenz, Y. Park, Big data-enabled authentication framework for offshore maritime communication using drones, IEEE Trans. Veh. Technol. (2024).

[23] G. Kessler, Protected AIS: A demonstration of capability scheme to provide authentication and message integrity, TransNav: Int. J. Mar. Navig. Saf. Sea Transp. 14 (2) (2020) 279–286.

[24] S.-h. Oh, D. Seo, B. Lee, S3 (secure ship-to-ship) information sharing scheme using ship authentication in the e-navigation, Int. J. Secur. Appl. 9 (2) (2015) 97–110.

[25] D. He, N. Kumar, K.-K.R. Choo, W. Wu, Efficient hierarchical identity-based signature with batch verification for automatic dependent surveillance-broadcast system, IEEE Trans. Inf. Forensics Secur. 12 (2) (2016) 454–464.

[26] R. Al-Zaidi, J. Woods, M. Al-Khalidi, H. Hu, An IOT-enabled system for marine data acquisition and cartography, Trans. Netw. Commun. 5 (1) (2017).

[27] R.J. Mohsin, J. Woods, M. Al-Khalidi, (AMDC) algorithm for wireless sensor networks in the marine environment, Int. J. Adv. Comput. Sci. Appl. 6 (6) (2015).

[28] A. Goudossis, S.K. Katsikas, Towards a secure automatic identification system (AIS), J. Mar. Sci. Technol. 24 (2019) 410–423.

[29] S. Jegadeesan, M.S. Obaidat, P. Vijayakumar, M. Azees, SEAT: secure and energy efficient anonymous authentication with trajectory privacy-preserving scheme for marine traffic management, IEEE Trans. Green Commun. Netw. 6 (2) (2021) 815–824.

[30] P. Sun, C. Cai, Y. Zhang, D.W. Yip, A. Esmradi, A confidentiality preserved data sharing framework for decision support in the maritime law enforcement, Mar. Policy 167 (2024) 106244.

[31] G. Wimpenny, J. Šafář, A. Grant, M. Bransby, Securing the automatic identification system (AIS): Using public key cryptography to prevent spoofing whilst retaining backwards compatibility, J. Navig. 75 (2) (2022) 333–345.

[32] J. Ye, X. Cao, Z. Guo, et al., Secure marine environment communication: A multiobject authentication protocol based on secret sharing, Int. J. Intell. Syst. 2023 (2023).

[33] J. Canedo, A. Skjellum, Using machine learning to secure IoT systems, in: 2016 14th Annual Conference on Privacy, Security and Trust, PST, IEEE, 2016, pp. 219–222.

[34] K.Z. Xiaojun, Background: GNSS spoofing in China and beyond, 2024, URL: https://www.riskintelligence.eu/background-and-guides/background-gnss-spoofing-in-china-and-beyond.

[35] D. Goward, AIS mystery: 12 ships appear to cross continents and drive in circles, 2024, URL: https://blog.geogarage.com/2020/06/ais-mystery-12-ships-appear-to-cross.html.

[36] U.S. issues renewed mariner warning on GPS interference, 2024, URL: https://maritime-executive.com/article/u-s-issues-renewed-mariner-warning-on-gps-interference.

[37] D.-K. Lee, D. Miralles, D. Akos, A. Konovaltsev, L. Kurz, S. Lo, F. Nedelkov, Detection of GNSS spoofing using NMEA messages, in: 2020 European Navigation Conference, ENC, IEEE, 2020, pp. 1–10.

[38] A. Bazyar, M.S.M. Mosavi, A.A. Rahmati, M. Moazedi, A Novel and Low-Cost Technique for Generating GPS Spoofing Data in order to Protection from Marine Navigation Systems, IRANIAN JOURNAL OF MARINE TECHNOLOGY, 2015.

[39] V. Hassani, N. Crasta, A.M. Pascoal, Cyber security issues in navigation systems of marine vessels from a control perspective, in: International Conference on Offshore Mechanics and Arctic Engineering, Vol. 57748, American Society of Mechanical Engineers, 2017, V07BT06A029.

[40] M. Suárez-Albela, T.M. Fernández-Caramés, P. Fraga-Lamas, L. Castedo, A practical performance comparison of ECC and RSA for resource-constrained IoT devices, in: 2018 Global Internet of Things Summit, GIoTS, IEEE, 2018, pp. 1–6.

[41] N. Koblitz, Elliptic curve cryptosystems, Math. Comput. 48 (177) (1987) 203–209.

[42] V.S. Miller, Use of elliptic curves in cryptography, in: Conference on the Theory and Application of Cryptographic Techniques, Springer, 1985, pp. 417–426.

[43] A. Karati, S.H. Islam, G. Biswas, A pairing-free and provably secure certificateless signature scheme, Inform. Sci. 450 (2018) 378–391.

[44] A.S. Bhala, V.P. Kshirsagar, M.B. Nagori, M.K. Deshmukh, Performance comparison of elliptical curve and rsa digital signature on arm7, in: Proceedings of International Conference on Information and Network Technology, ICINT 2011, 2011.

[45] K. Magons, Applications and benefits of elliptic curve cryptography, in: SOFSEM (Student Research Forum Papers/Posters), 2016, pp. 32–42.

[46] F. Mårlind, I. Butun, Activation of lorawan end devices by using public key cryptography, in: 2020 4th Cyber Security in Networking Conference, CSNet, IEEE, 2020, pp. 1–8.

[47] M. Mumtaz, L. Ping, Forty years of attacks on the RSA cryptosystem: A brief survey, J. Discrete Math. Sci. Cryptogr. 22 (1) (2019) 9–29.

[48] J. Wang, L. Liu, S. Lyu, Z. Wang, M. Zheng, F. Lin, Z. Chen, L. Yin, X. Wu, C. Ling, Quantum-safe cryptography: crossroads of coding theory and cryptography, Sci. China Inf. Sci. 65 (1) (2022) 111301.

[49] M.K. Misra, R. Mathur, R. Tripathi, On post quantum wireless communication security, in: 2021 5th International Conference on Information Systems and Computer Networks, ISCON, IEEE, 2021, pp. 1–6.

[50] C. Youngblood, An introduction to identity-based cryptography, 2005, pp. 1–7, CSEP 590TU.

[51] K. Lee, Comments on "Secure data sharing in cloud computing using revocable-storage identity-based encryption", IEEE Trans. Cloud Comput. 8 (4) (2020) 1299–1300.

[52] S.S. Al-Riyami, K.G. Paterson, Certificateless public key cryptography, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2003, pp. 452–473.

[53] X. Yao, X. Han, X. Du, A light-weight certificate-less public key cryptography scheme based on ECC, in: 2014 23rd International Conference on Computer Communication and Networks, ICCCN, IEEE, 2014, pp. 1–8.

[54] B. Padma, D. Chandravathi, L. Pratibha, Defense against frequency analysis in elliptic curve cryptography using k-means clustering, in: 2021 International Conference on Computing, Communication, and Intelligent Systems, ICCCIS, IEEE, 2021, pp. 64–69.

[55] S. Kumar, D. Sharma, Key generation in cryptography using elliptic-curve cryptography and genetic algorithm, Eng. Proc. 59 (1) (2023) 59.

[56] B. Raj, I. Ahmedy, M.Y.I. Idris, R.M. Noor, A hybrid sperm swarm optimization and genetic algorithm for unimodal and multimodal optimization problems, IEEE Access 10 (2022) 109580–109596.

[57] H.H. Zhang, Z.S. Xue, X.Y. Liu, P. Li, L. Jiang, G.M. Shi, Optimization of high-speed channel for signal integrity with deep genetic algorithm, IEEE Trans. Electromagn. Compat. 64 (4) (2022) 1270–1274.

[58] E. Zhang, S. Zhang, T. Yang, X. Zhu, L. Chen, Y. Zhang, X. Yang, L. Zhang, Improved particle swarm optimization with less manual intervention for photonic inverse design, IEEE Photonics Technol. Lett. (2023).

[59] F. Tellez, J. Ortiz, Comparing AI algorithms for optimizing elliptic curve cryptography parameters in third-party E-commerce integrations: A pre-quantum era analysis, 2023, arXiv preprint arXiv:2310.06752.

Mohammed Al-Khalidi received the Ph.D. degree from the University of Essex, U.K. He is a Senior Lecturer of Cyber Security with the Department of Computing and Mathematics, Manchester Metropolitan University, U.K. He has been awarded research funding by UKRI's Global Challenges Research Fund and other government bodies focussing on AI Security. He has also been involved in EU projects, including POINT (awarded best Internet project by the Future Internet Assembly). His work has been published at high class journals and conferences and filed into a patent. His past assignments include a Lecturer with the Department of Computer Science, Edge Hill University, and a Research Officer with the School of Computer Science and Electronic Engineering, University of Essex. Prior to that, he worked in industry as a Senior Core Network Engineer at several leading mobile telecommunication companies. His research interests include AI security, IoT security, mobile computing, cloud computing, and information centric networks.

Rabab Al-Zaidi received the Ph.D. degree from the University of Essex and has worked in many universities, including the University of Essex, Anglia Ruskin University, and the University of Central Lancashire. She is an active academic and researcher with more than 15 years of experience. She is currently working as a Lecturer with the School of Science, Engineering and Environment, University of Salford, U.K. She has significant research contributions in the field of cloud computing, Internet of Things, network security, sensor networks, mobile ad-hoc networks, and information-centric networks.

Tarek Ali is a Research Assistant in AI Security at the Department of Computing and Mathematics, Manchester Metropolitan University, UK. He holds a bachelor's degree in Electronics and Communications from Damascus University and an M.Sc. in Computer Science with DISTINCTION from MMU where he is currently working towards his Ph.D. degree in Intelligent and Secure Mobility Management in 6G and Beyond Networks. In addition to his research, Tarek has contributed to the academic community as a peer reviewer for several scholarly journals, providing critical evaluations to advance the field of AI Security. He has also attended multiple conferences, staying up to date on the latest developments and engaging with fellow researchers in his field.

Safiullah Khan received the B.Sc. in electronic engineering from the University of Engineering and Technology, Peshawar, Pakistan, in 2013, the M.Sc. in electrical engineering from COMSATS University Islamabad, Abbottabad campus, Pakistan, in 2017. and the Ph.D. degree in computer engineering from Gachon University, Seongnam, South Korea, in 2023. He worked as project engineer with the R&D department of the National Radio and Telecommunication Corporation, Haripur, Pakistan, for two years. Currently, he is a lecturer with the Department of Computing and Mathematics, Manchester Metropolitan University, UK. His research interests include efficient hardware implementations of cryptographic protocols, post-quantum cryptography, and blockchain.

Ali Kashif Bashir holds the position of Professor of Computer Networks and Cybersecurity at the Manchester Metropolitan University, UK. He is the leader of Secure and Intelligent Systems Research Theme; Future Networks Lab, and IoT/Cybersecurity testbed. Throughout his career, Ali has presented more than 50 keynote speeches on an international scale and produced over 300 research articles. He has obtained over £4 million in external funding from UK, South Korean, Japanese, European, Asian, and Middle Eastern agencies. His students have won best paper awards, best Ph.D. thesis awards, and several other recognitions. He is a senior member of IEEE, a member of several technical societies, and a Distinguished Speaker of ACM. He received the Clarivate Highly Cited Researcher Award in 2023. He was listed as IEEE Featured Author in 2021, and highly cited 2% of researchers by Stanford University in 2021 and 2022. He is EIC of IEEE Technology, Policy and Ethics, and Journal of Autonomous Intelligence, Advisory Board Member of IEEE Transactions on Consumer Electronics, and AE of IEEE Transactions on Network Science and Engineering.