Secure User Authentication Model Using Identity-Based Encryption (IBE) Scheme: Challenges, Techniques, and Trends

Raja Farah Sharima Raja Muhamad Danial[1], Nazhatul Hafizah Kamarudin[2], Abdul Ghafar Jaafar[3]
Centre for Cyber Security-Faculty of Information Science and Technology,
Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor, Malaysia [1, 2]
Faculty of Artificial Intelligence, Universiti Teknologi Malaysia (UTM), 54100 Kuala Lumpur, Malaysia [3]

***Abstract*—User authentication is the crucial component in ensuring that digital identities are securely authenticated when performing sensitive digital transactions. Building resilience against emerging cyber threats like identity theft and Man-in-the-Middle (MITM) attacks remains an ongoing challenge. Identity-Based Encryption (IBE) is a cryptographic method in the category of public key cryptography that allows the use of unique identifiers, such as email addresses, as public keys for encryption, making key management easier than traditional public key cryptography. This study presents a comprehensive overview of secure authentication techniques using IBE schemes proposed by researchers, emphasizing techniques that have been explored and introduced. The review examines current IBE schemes, including blockchain-based techniques, and analyzes the security features, application domains, implementation requirements, and challenges. By incorporating findings from previous works, this study identifies common challenges that impede real-world implementation and suggests a potential approach for combining alternative security methods to improve authentication robustness. The purpose of this work is to provide researchers and practitioners with a comprehensive review of secure authentication models, as well as practical insights to assist in developing an implementable authentication solution for real-world secure digital transactions.**

***Keywords*—User authentication; Identity-Based Encryption (IBE); digital identity; network security**

I. Introduction

The rapid growth of digital services has made secure user authentication a fundamental and crucial requirement for any digital transaction provided by service providers, whether private or Government agencies. Many domains, such as finance, healthcare and the Internet of Things (IoT), have increasingly relied on digital identities to enable access to sensitive services and data. Consequently, the authentication process has become a critical security control, as failures in identity verification can result in severe consequences such as identity theft, unauthorized access, privacy breaches, and financial losses.

Identity authentication methods have gone through evolution since they were introduced, that is, Single-Factor Authentication (SFA), Two-Factor Authentication (2FA) and Multi-Factor Authentication (MFA) [1]. All these authentication methods can be combined with additional factors to further strengthen the security level of user identity information, such as security tokens, user biometric information, cryptographic or encryption methods, secure environment, and many others.

An identity-based cryptographic method, called Identity-Based Encryption (IBE), was introduced by [2]. It is an extension of the Public Key Encryption (PKE) method, where the user's public key is some special information about the user, for example, the user's email address. This means that a sender who has access to the system's public parameters can use the text value of the recipient's name or email address as a key to encrypt the message they want to send. This approach simplifies key management and reduces the need for Public Key Infrastructure (PKI).

However, the IBE method can only provide examples of identity-based signatures. Hence, in order to address the problems encountered, various improved IBE methods have been introduced by researchers from time to time. In 2001, Dan Boneh and Matthew K. Franklin helped to solve the IBE issue by introducing a pair-based cryptography named the Boneh–Franklin scheme [3] and [4] has introduced an encryption method based on the quadratic residue, that is, the message is encrypted one bit at a time, but suffers from inefficiency due to the high expansion of the ciphertext. The IBE method by [5] uses bilinear coupling, which provides a different approach to IBE.

Although the IBE method has been improved, it faces a limited usage issue due to the absolute trust that is essential to the Private Key Generator (PKG) [6] and [7]. The PKG can generate any user's private key and potentially decrypt (or sign) messages without permission, and this is a weakness of the IBE method [8]. Therefore, various alternative systems and continuous studies are needed to reduce the level of trust required in PKG [9]. Certificate-based encryption, secure key production cryptography, and certificateless cryptography [10] are among the alternative systems that have been developed to release the PKG component.

The evolution of the IBE has reflected significant advances in cryptographic practice aimed at improving security, efficiency, and usability. Accordingly, ongoing research is expected to help strengthen the level of security and reliability of cryptographic systems against emerging cyber threats. Thus, this study aims to conduct a comprehensive analysis of the IBE schemes currently in use that are efficient and effective. By

knowing the most practical and secure IBE schemes, this study will provide potential possible combinations of technologies in further enhancing the user identification and securing user's personal information security and privacy in performing digital services. This study also aims to provide future research on developing an ideal and general model of user authentication that can be adopted by any field, with the ability to mitigate possible security risk and be one of the factors to increase users' confidence and trust to use digital services.

A. Motivation

The main purpose of this study is to examine the current method used for the user identity authentication process using the IBE scheme, as well as emerging technologies that is suitable for adaptation to increase the level of security and privacy of the user's personal data. The primary motivation of this study is as follows:

- Examine the IBE scheme that is effective and secure for user identity authentication.
- Assess the advantages, limitations, or challenges of all IBE schemes currently used.
- Identify opportunities for enhancement and innovation in user identity authentication.
- Minimize cybersecurity risks related to user identity authentication, such as Man-in-the-Middle (MITM), identity theft, and phishing.
- Gain knowledge on issues related to user identity authentication.

B. Contributions

There are several contributions from this review study that may help other researchers on user authentication methods and cybersecurity issues by addressing significant barriers, synthesizing knowledge, and investigating potential future works or innovations related to IBE.

Besides, this study will provide useful direction for researchers, programmers, as well as organizations intending to deploy or enhance the security level of user authentication methods in their applications.

The contributions include the following:

- Provide a comprehensive analysis of the current landscape of user authentication methods, highlighting their key application fields, key advantages and critical security challenges.
- Discusses significant challenges in user authentication techniques and proposes feasible and relevant perspectives for improvement.
- Provide significant insights on user authentication model applicable across various fields.
- Provide ongoing efforts to further improve the resilience and robustness of user authentication methods by highlighting areas that require further research especially related to security issues.

C. Research Questions

In achieving the objectives of this study, four (4) research questions have been identified with its rationale and are detailed as follows:

- RQ1: What fields of study use the IBE scheme?
- RQ2: What is the problem statement of the previous research IBE scheme?
- RQ3: What are the limitations or weaknesses faced in using the IBE scheme?
- RQ4: What are the new technologies or trends in the IBE authentication field?

The research questions are determined to explore the current user authentication model using the IBE scheme. This study will investigate and discuss all questions outlined in detail.

D. Research Objectives

Based on the research questions, information on common themes of fields, problems, limitations and new technologies will be identified. The research questions are also used to achieve the following research objectives:

- RO1: to explore application fields which used IBE as an authentication method done by previous researchers.
- RO2: to understand problems addressed or issues faced by previous researchers on the IBE authentication method.
- RO3: to recognize limitations or weaknesses faced by the current IBE scheme proposed or tested.
- RO4: to explore new technologies or models that can further enhance the scheme.

E. Paper Organization

The organization of this study is designed to address all the research questions and research objectives outlined.

The study structures are as follows:

- Section II presents and analyzes related previous works.
- Section III details the research methodology used, including the search strategy and the inclusion and exclusion criteria.
- Section IV reviews the implementation of IBE scheme in various fields.
- Section V presents issues and challenges faced in IBE scheme.
- Section VI details out the limitations in IBE scheme.
- Section VII provides information on future perspectives and enhancements.
- Section VIII discusses issues related to IBE scheme and ways to overcome.
- Section IX concludes and summarizes the analysis and findings of the study based on the research objectives.

List of abbreviations used in this study is listed in Table I below:

TABLE I. LIST OF ABBREVIATIONS

Acronym	Definition
2FA	Two-Factor Authentication
BC-IBE	Backward Compatible Identity-Based Encryption
CA	Central Authority
DKER	Decryption Key Exposure Resistance
DRIBE	Delegated Revocable Identity-Based Encryption
GDPR	General Data Protection Regulation
IBE	Identity-Based Encryption
IoT	Internet of Things
KGC	Key Generation Center
LWE	Learning with Errors
MFA	Multi-Factor Authentication
MITM	Man-in-the-Middle
MPTCP	Multi-Path TCP
PKE	Public Key Encryption
PKG	Private Key Generator
PKI	Public Key Infrastructure
RIBE	Revocable Identity-Based Encryption
RHIBE	Revocable Hierarchical Identity-Based Encryption
SFA	Single-Factor Authentication

II. RELATED WORKS

Numerous relevant studies have been carried out to examine, analyze and evaluate different user authentication models. A study on the trust issue faced in Identity-Based Encryption conducted by [8] has highlighted the need for a more secure and deployable privacy solution by reducing the probability of privacy breaches to an arbitrarily small value. Based on a study conducted by [11] on numerous IBE schemes, the main problem that exists in the IBE scheme, which is escrow, has been identified, and suggested that dependency on PKG needs to be overcome to address the issue of trust in third parties, since it will indirectly affect the privacy of communication between users.

The Revocable Hierarchical Identity-Based Encryption (RHIBE) scheme introduced and discussed by [12] focuses on adaptively secure construction methods to address the weaknesses in previous methods that can only achieve selective security, rather than adaptive security. Similarly, since revocation functionality is crucial in cryptographic systems and existing RIBE schemes require long public parameters or composite-order groups, [13] has presented study on an efficient Revocable Identity-Based Encryption (RIBE) scheme. Furthermore, the need for a secure Identity-Based Encryption scheme with perfect forward secrecy for network security protocols to address classic IBE which lacks the perfect forward secrecy have been discussed by [14].

In protecting the privacy of data in Internet of Things (IoT) applications, [15] has proposed an effective and useful IBE method with a Revocable IBE (RIBE) feature where the Private Key Generator (PKG) can cancel the user's account if the private key has been exposed. While issues on compatibility requirements due to existing systems will lose access to previous ciphertexts after the key update process has been discussed in detail by [16]. The study in [17]'s paper has addressed the efficient key revocation in RIBE schemes by exploring delegating update key generation to a cloud server due to inefficiencies with the update key sizes issue faced in previous schemes.

Additionally, a study conducted by [18] has discussed the issue of privacy in smart contracts and the challenges of implementing smart contracts that preserve privacy, because it was found that transaction details are openly disclosed in traditional smart contracts. Therefore, researchers introduce a smart contract privacy protection mechanism and develop a new blockchain model to preserve smart contract privacy.

As a result of the study carried out by [19], there are various challenges related to digital identity management in the context of Web 3.0, especially in the need to obtain a more private, secure and manageable Internet experience. Issues of difficulty in ensuring interoperability between various platforms and privacy rules in a decentralized environment are also discussed.

In addition, researchers also found that the most important and main problem is the transition from a traditional identity system to a self-sovereign identity system that allows users to manage the sharing of their personal information independently without involving a Central Authority (CA) in increasing the level of user control and security [19].

Comparison of the authentication scheme features is detailed in Table II. A summary of previous works is described in Table III. Fig. 1 illustrates the Identity-Based Encryption (IBE) architecture.

IBE provides more secure and enhanced security features compared to traditional authentication models. But IBE has its own limitations and advantages as well. The main limitations of IBE are inherent weaknesses and issues such as reliance on PKG which requires centralized trust, and if compromised, it will lead to a single point of failure issue. In addition, the key revocation difficulty issue in the basic IBE scheme also causes compromised key revocation to affect the implementation of IBE in dynamic user environments. Although IBE has some limitations, it has many advantages and has been widely used in many fields such as banking, IoT and healthcare.

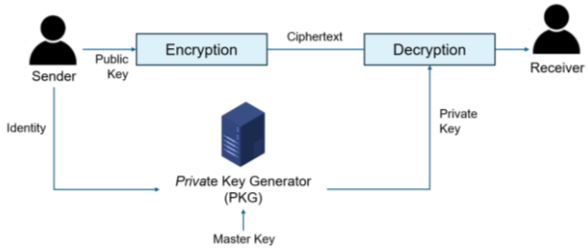

Fig. 1. IBE architecture.

TABLE II. COMPARISON OF AUTHENTICATION SCHEMES

Authentication Scheme	Security Focus	Threats Addressed	Technologies Integrated	Real-World Applicability
Single-Factor Authentication (SFA)	Basic identity verification using a single factor (knowledge, possession or inherence).	Weak passwords, phishing, credential stuffing, brute-force attacks.	Passwords, PINs, swipe cards, biometric fingerprints or facial recognition.	Personal or computer devices (password of the smartphone, computer, laptop), email logins.
Two-Factor Authentication (2FA)	Requires two different authentication factors to strengthen security. Typically using one knowledge factor and one possession or inherence factor.	Phishing, password guessing, credential stuffing.	Combination of password and OTP (One Time Password via SMS / mobile applications), hardware tokens, combination of password and biometric information.	Online banking, email, corporate VPNs, social media accounts.
Multi-Factor Authentication (MFA)	Requires two or more different authentication factors to create multiple layers of defense and enhanced security level.	Stolen credentials, phishing, brute force, Man-in-the-Middle (MITM) attacks, replay attacks, account takeovers.	Passwords, biometrics information (fingerprint, facial recognition), hardware keys (USB/NFC), push notifications.	Industry standard to secure sensitive accounts in fields of healthcare, IoT, government systems, financial services, enterprise environments.
Identity-Based Encryption (IBE)	Cryptographic authentication method using identity-linked encryption keys rather than static passwords.	Impersonation, unauthorized data access, interception, Man-in-the-Middle (MITM) attacks via cryptographic means.	Public Key Infrastructure (PKI) (public keys are derived from user identities), secure key management, encryption algorithms.	Secure messaging, email encryption, IoT environments and applications requiring encrypted communications linked to identity.

TABLE III. SUMMARY OF PREVIOUS RESEARCH

Paper	Issue Discussed	Contribution
[8]	Overcoming trust issue in IBE scheme	Review a privacy scheme without non-collusion assumptions to allow users to reduce private key exposure probability by employing multiple intermediate CAs for enhanced privacy and the scheme separates the PKG from the intermediate CAs.
[11]	Comprehensive study and analysis on numerous IBE schemes	Provides detailed information on numerous IBE schemes with its advantages, disadvantages and potential attacks.
[12]	Adaptive security of IBE scheme	Provides proof on adaptive security under simple static assumptions and addresses challenges of dual system encryption in Revocable Hierarchical Identity-Based Encryption (RHIBE) through security proof.
[13]	Revocation requirements in IBE scheme	Proposes a Revocable Identity-Based Encryption (RIBE) scheme that achieves adaptive security, Decryption Key Exposure Resistance (DKER), and constant-size public parameters over prime-order bilinear groups by employing the Seo-Emura technique, which combines specific IBE schemes to enhance security and efficiency.
[14]	Importance of perfect forward secrecy	Provide details of Learning with Errors (LWE) problem based on Quantum Identity-Based Encryption (QIBE) scheme and its advantages.
[15]	Importance of secure communication in Internet of Things (IoT) applications	Proposes an efficient RIBE scheme for IoT applications with its detail algorithms and utilizes ISO/IEC 18033-5 SM9 encryption for security.
[16]	Compatibility requirements in IBE scheme	Introduction of Backward Compatible Identity-Based Encryption (BC-IBE) to solve backward compatibility problems in IBE systems and supports revocation of expired private keys.
[17]	Exploring delegation of update key generation	Introduces the concept of RIBE that can be delegated (Delegated Revocable Identity-Based Encryption (DRIBE)) where the process of delegation of update key generation to the cloud server will be implemented.
[18]	Preserving privacy in smart contracts	Introduce privacy-protection mechanisms for smart contracts and develop a new blockchain model for privacy-preserving smart contracts. Details comparison of computation and storage overheads with existing schemes are also provided.
[19]	Challenges related to digital identity management	Provide information on digital identity evolution and how users or organizations use digital identities to control their online appearance inside the Web 3.0 architecture.
This paper	User authentication using IBE scheme in secure and privacy-protected environment	This paper provides comprehensive reviews on various IBE schemes across different fields and functions. Findings from trustworthy databases are combined and classified, offering distinct points of view based on deployment fields, issues, challenges and integration of evolving technologies in proposing future and further research areas. This will aid in identifying important gaps and offer a roadmap for the enhanced and advancement of user authentication methods that are deployable in various fields.

The advantage of IBE is that it does not require distribution of public keys, as they will be derived from known identities hence a separate PKI is not required. This will simplify and increase the efficiency of key management and reduce overhead. IBE is also flexible as it uses any unique string such as email or username as the public key which allows embedding additional information in the identity to dynamically control the validity of the key. And it is also scalable as the entire system uses a single master key pair maintained by the PKG which makes key generation and distribution more efficient for many users.

In the banking sector, IBE provides secure and scalable financial transactions where it can protect sensitive banking transactions by directly encrypting data with user identities (such as account numbers or emails) without the use of complex PKI, thus reducing the risk of MITM attacks. Additionally, the combination of IBE with digital ID authentication can enhance user authentication and data privacy by securely binding identity data to a cryptographic key.

For the Internet of Things (IoT) sector, IBE provides simplification of cryptographic key management in resource-

constrained devices by eliminating cumbersome PKI setup and it also supports scalable and flexible key distribution in dynamic IoT networks. Device ID with embedded identity also provides easy authentication and encryption. In terms of communication and storage, it supports secure cloud communication and storage suitable for IoT environments.

While for the healthcare sector, IBE allows secure exchange of confidential information associated with patient or provider identities without the need for complex PKIs and simplifies key management for multiple healthcare systems and practitioners. Besides, it also ensures secure cloud data transmission and medical record storage.

In conclusion, IBE provides more cost-effective security management compared to traditional PKI by reducing management overhead and making enterprise-level encryption scalable and affordable. IBE also provides flexible encryption that is directly linked to user identities and simplified key management. This is highly beneficial for sectors like banking, IoT and healthcare that require secure and scalable communications. However, the security risks associated with key escrow and reliance on a single trusted authority need to be addressed properly.

III. Research Methodology

The methods and strategies applied in this study are explained in this section. Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) protocol [20] is the methodology adopted for this work.

A. Search Strategy

The established digital library databases that have been identified to be used for obtaining related articles are Web of Science, IEEE Xplore, Scopus and Wiley. The publication papers are the recent papers, from 2020 to 2025. Keywords that were used in the searching process are "user authentication" or "user authentication model" or "Identity Based Encryption (IBE)" or "IBE".

These keywords were searched either in the title or abstract using Boolean operators like "AND" and "OR" together with parenthesis. The key string used in the searching process is: ("User Authentication" AND "IBE"), ("User Authentication Model" AND "IBE"), ("User Authentication" AND ("Identity-Based Encryption (IBE)" OR "Identity-Based Encryption") and ("User Authentication Model" AND ("Identity-Based Encryption (IBE)" OR "Identity-Based Encryption")).

In total, 414 papers were discovered from these four databases and after assessing the papers, 124 duplicates or unrelated papers were eliminated.

B. Inclusion and Exclusion Criteria for Selection

Details of the inclusion and exclusion criteria are described in Table IV.

TABLE IV. Inclusion and Exclusion Criteria

Inclusion Criteria	
IC1	Papers that were published between 2020 and 2025
IC2	Papers that are accessible and downloadable
IC3	Paper related on user authentication models using IBE scheme
IC4	Papers that provide design, scheme, or implementation of IBE in the user authentication model
IC5	Papers that are using English language
Exclusion Criteria	
EC1	Papers that are not related to the work and research question or objectives of this work
EC2	Papers that are not accessible as full text
EC3	Papers discussing user authentication method that are other than IBE scheme
EC4	Papers which studies do not include design, scheme, or implementation of IBE in the user authentication model
EC5	Papers using other than English language.

The selection and filtering process using the PRISMA methodology is illustrated in Fig. 2.

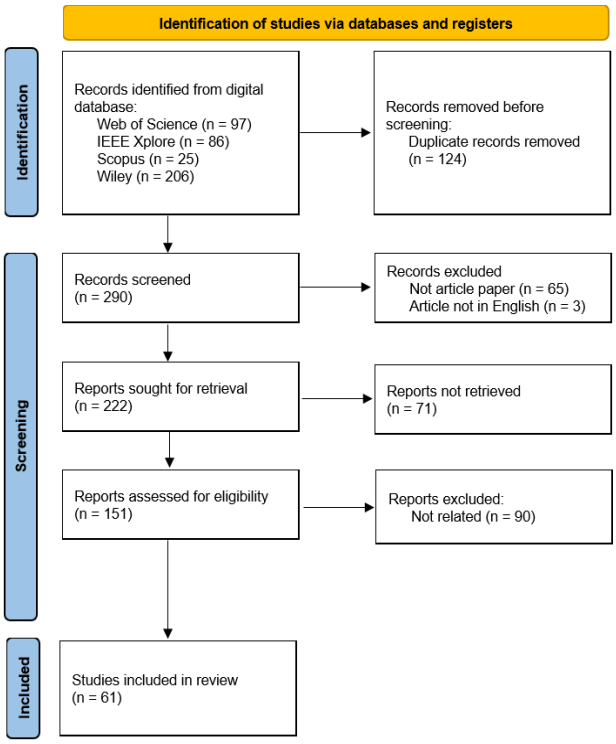

Fig. 2. PRISMA methodology flow diagram.

Based on the PRISMA statement, 61 papers have been identified and will be thoroughly reviewed and scrutinized in order to determine the current state of the user authentication method.

IV. Implementation of Identity-Based Encryption (IBE) in Various Fields

Based on the papers reviewed, various fields of studies have been identified. This section categorizes fields of study into three main fields: Security and Information Sharing, Internet of Things (IoT), and Network and Infrastructure.

Details of each field, which consist of the number of papers, equivalent representation in terms of percentage and presentation of an extensive overview of current state for every field identified, are shown in Fig. 3 and Table V.

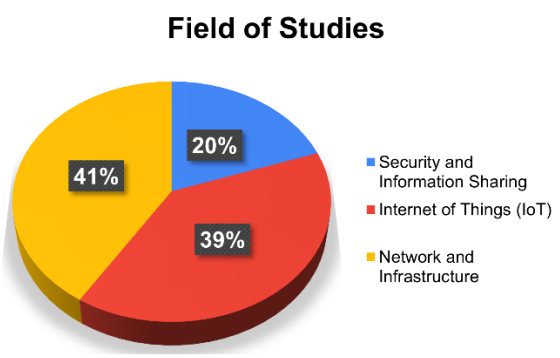

Fig. 3. Field of studies.

TABLE V. CATEGORIES OF FIELDS DISCOVERED IN THE PREVIEWED PAPERS.

Field of Studies	Papers
Security and Information Sharing	[6], [8], [11], [12], [13], [14], [16], [18], [19], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35]
Internet of Things (IoT)	[15], [36], [37], [38], [39], [40], [41], [42], [43]
Network and Infrastructure	[7], [9], [10], [17], [24], [44], [45], [46], [47], [48], [49], [50], [51], [52], [53], [54], [55], [56], [57], [58], [59], [60], [61], [62], [63]

A. Security and Information Sharing

Security is the most critical factor, especially in the field of information and technology. In line with security principles, confidentiality, integrity and availability, users' personal information must always be ensured secured at the most optimal level. Based on research papers that have been examined, 20% of them have highlighted that security issues have to be addressed accordingly in ensuring users' information and privacy are well preserved [8], [19], [18].

Likewise, a study by [27] has discussed challenges in ensuring outsourced data integrity, while [32] highlighted challenges related to outsourcing in cloud storage systems. A blockchain model for privacy-preserving smart contracts has also been proposed by [18] as a measure to increase the level of information security and user privacy.

In sectors related to security and information sharing, many enterprises have adopted IBE scheme to streamline corporate communications and secure email by using user identities such as email addresses directly as public keys, removing the need for revocation infrastructure, certificate authorities and certificates.

B. Internet of Things (IoT)

Currently, IoT has been widely used in many fields and industries. Thus, user authentication is vital in ensuring only authorized users can access facilities provided accordingly. 39% of the reviewed papers which are in IoT field highlight that having an efficient IBE scheme are crucial [15], [30], [38].

Similarly, [30] also highlighted the need to enhance user privacy in cryptographic schemes. While [39] have proposed solution to encounter issues related to data and privacy which was compromised in cloud storage environment. In addition, [41] has suggested that in order to handle identity revocation, it is crucial to provide data confidentiality and source authentication. Furthermore, [15] emphasized the importance of having secure communications in IoT applications through user authentication.

Implementation of IBE in IoT, such as Lightweight Authentication in IoT devices, is widely deployed in many sectors due to the reduced complexity of key distribution and management, as device identities (such as the serial number or device name) can directly serve as public keys. This will reduce the overhead in IoT contexts, which often have network and trust infrastructure limitations as well as restricted computational resources.

Additionally, the use of Hierarchical Identity-Based Encryption (HIBE) in IoT applications that have multiple levels of devices and access hierarchies (such as gateways, edge devices and sensors) is very useful due to the hierarchical key representation feature provided by HIBE. This hierarchical structure will also facilitate effective access control management in IoT ecosystems where devices may be organized under multiple administrative domains.

C. Network and Infrastructure

The highest fields from the reviewed papers are from the network and infrastructure field, which contributes 41%. According to [55], attacks such as session hijacking, traffic diversion, and eavesdropping during the initial handshake are possible. Therefore, security is essential for the successful implementation of MPTCP (Multi-Path TCP).

The Signal Protocol and similar cryptographic systems face several security challenges, including vulnerabilities to MITM attacks and users cannot fully trust service providers, as there are possibilities of malicious servers to distribute forged public keys [24].

Based on a study conducted by [50], secure data transfer is the challenges in fog computing and IoT ecosystems. Therefore, researchers propose IBE scheme called Hierarchical Identity-Based Architecture for Fog Computing (HIBAF) to enhance data security by providing performance enhancement in data processing and management compared to traditional cloud environments.

The difficulty of assuring data security, integrity and reliability in cloud storage systems have been examined by [58]. Likewise, [17] have conducted study related to delegation of update key generation to a cloud server by introducing the Delegated RIBE (DRIBE) concept.

Mobile Ad Hoc Networks (MANETs) are an example of a variant of IBE that has been prototyped in the networking and infrastructure-related sectors. By using device IDs such as phone numbers for encryption and authentication, they can enable effective, certificate-free secure communication without the need for a traditional PKI. In addition, IBE also has been utilized for network access control, simplifying user and device authentication without depending on certificate management systems by encoding identities in IBE private keys.

V. ISSUES AND CHALLENGES IN IBE

In accordance with the identified and evaluated papers, main issues that have been discovered related to IBE scheme in user

authentication model have been listed in this review. These issues are discovered and classified into two main categories, based on the problem statements and issues highlighted in the reviewed papers, as shown in Fig. 4 and Table VI.

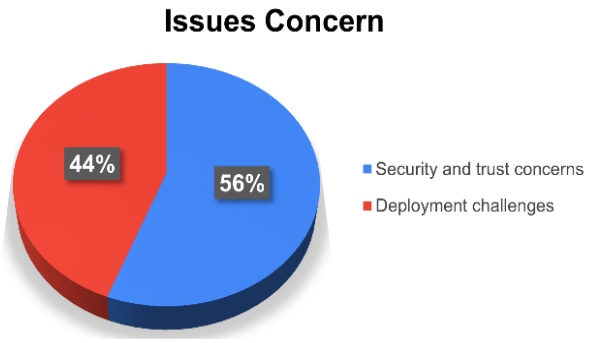

Fig. 4. Categories of issues of concern.

TABLE VI. ISSUES DISCUSSED IN THE PREVIEWED PAPERS

Issues	Papers
Security and trust concerns	[6], [9], [10], [11], [12], [14], [15], [16], [18], [22], [23], [24], [25], [26], [27], [30], [31], [33], [34], [38], [39], [41], [42], [43], [48], [49], [50], [51], [52], [53], [56], [61], [62]
Deployment challenges	[7], [8], [13], [15], [17], [19], [21], [24], [28], [29], [32], [35], [36], [37], [39], [40], [44], [45], [46], [47], [54], [55], [57], [58], [59], [60], [63]

A. Security and Trust Concerns

As shown in Fig. 4, the most critical and difficult issue to overcome is related to the level of users' personal information security with regard to verifying users' identities digitally and users' trust in the technology and online services offered. This is driven by various factors and is evident when the number of reported cybercrime cases is increasing despite the implementation of additional security features. This, in turn, pushes towards a higher level of improvement required in strengthening the level of security of users' personal information in order to increase and maintain the level of user trust.

Current password-based methods expose users to security risks thus encouraging a wider implementation of IBE in real-world contexts [22]. In IBE schemes, the issue of escrow [24], [9], [31], [11] and trust on third parties [51] is the primary and common issue. Thus, security and privacy concerns towards user's information need to be addressed [56] by enhancing security features like mutual authentication and key revocation [24].

Studies on security solutions to protect against various threats are highly needed in maintaining user's trust [52] and ensuring the confidentiality in communication amidst quantum threats [38]. Besides, [18] have identified that smart contract implementation faced challenges in preserving privacy. Other than that, most schemes only achieve selective security, not adaptive security [12], [31].

B. Deployment Challenges

The second issue of concern identified from the reviewed papers are the implementation challenges. Challenges related to the implementation of the IBE scheme in the real-world environment are the complexity of the model, interoperability across different platforms, practicality, cost, and computing time involved, level of effectiveness, reliability, flexibility, and the need for specialized cryptographic expertise.

Some of the IBE schemes are very complex and difficult to achieve tight security [21], [57], [63] and face complexity related to certificate [39], [32] and key [37] management. Additionally, [19] have highlighted the difficulties in ensuring interoperability among various platforms and the implications of privacy regulations, such as the right to be forgotten in a decentralized environment. And there are inefficiency issues related to keys, such as the update key sizes [17] and key regeneration for non-revoked users [13].

VI. LIMITATIONS

As indicated in the reviewed papers, limitations of the IBE scheme that have been discovered from the previous work are analyzed in this review. The limitations are categorized into three main categories, which are usability in real-world environments, vulnerabilities and the need for expertise. Details of all the categories are provided in Fig. 5 and Table VII.

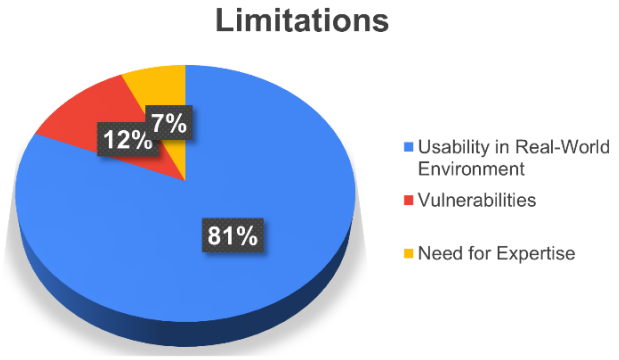

Fig. 5. Categories of limitations.

TABLE VII. LIMITATIONS IN THE PREVIEWED PAPERS

Issues	Papers
Usability in Real-World Environment	[6], [7], [8], [9], [10], [11], [12], [13], [15], [16], [17], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [36], [37], [39], [41], [42], [43], [45], [46], [47], [48], [49], [50], [51], [52], [54], [55], [56], [57], [58], [60], [61], [62], [63]
Vulnerabilities	[14], [22], [24], [35], [40], [44], [53]
Need for Expertise	[18], [19], [21], [59]

A. Usability in Real-World Environment

Proposals or ideas for a solution or a theoretically proposed model are very useful and helpful, by proving it through formal or theoretical methods will make it more meaningful and adaptable in the real-world environment. The key escrow issue would hinder the deployment of any IBE scheme since the Key Generation Center (KGC) have the ability to decrypt all ciphertext which would lead to potential security risks [23]. Thus, implementation of IBE in real-world environments are still limited [6] due to certain factors which need to be addressed before wider deployment is feasible.

B. Vulnerabilities

Overcoming possible threats and vulnerabilities with regard to crucial information, such as a user's digital identity and their personal information in online services are vital. Example of a situation, during user registration process, the Signal Protocol is vulnerable to Man-in-the-Middle (MITM) attacks due to malicious server actions [24]. Vulnerabilities to attacks, which might be due to the usage of low-entropy passwords, will become a challenge [53] even though the scheme used already deploys necessary security measures. And as discussed by [35], theoretical explanations of security might not completely encompass real-world vulnerabilities.

C. Need for Expertise

The emergence of new technology is very valuable in the development of today's technological world. But to adopt any technology, it requires more than just merely utilizing the technology. A comprehensive and detailed plan, together with relevant knowledge of the particular technology and requirements, is compulsory to drive the technology adoption and achieve the expected success. Therefore, expertise and skilled developers are required to ensure the successfulness for any solution's implementation.

In paper [18], it does recognize the need to have a developer with deep cryptography knowledge, especially in handling complexity in the blockchain environment. Similarly, [19] also raised about the difficulty of understanding and adopting underlying technologies such as blockchain and decentralized networks, as well as becoming one of the challenges to create a robust digital identity ecosystem.

VII. Future Perspectives and Enhancements

In advancing and securing the user authentication process by adopting relevant emerging technologies, more detailed research needs to be conducted. By exploring, identifying, analyzing, and choosing the most reliable and efficient technology would bring advantages to many fields and industries, especially those that require secure user authentication.

Since the authentication process is the most commonly used by people and organizations, it must be equipped with robust security measures. Therefore, any proposed model or solution must be tested in a real-world environment using relevant security tools and proved to be secure. This study would provide insights on possible and potential areas to be further examined by researchers. Future enhancements categories are described in Table VIII and Fig. 6.

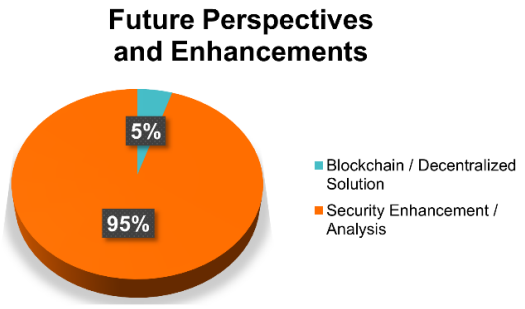

Fig. 6. Categories of future perspectives and enhancements.

TABLE VIII. Future Perspectives and Enhancements in the Previewed Papers.

Issues	Papers
Blockchain / Decentralized Solution	[19], [22], [61]
Security Enhancement / Analysis	[6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [21], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [46], [47], [48], [49], [50], [51], [52], [53], [54], [55], [56], [57], [58], [59], [60], [62], [63]

A. Blockchain / Decentralized Solution

Blockchain is one of the new technologies that has been explored by many industries. Many research related to user authentication also has considered and recognized the potential usage of blockchain technology by adopting it in their solution. According to [61], the studies have suggested future work on comprehensive rights divisions in blockchain-empowered metaverse applications, as existing editable blockchains cannot support user preferences on readability governance, which violates the GDPR rights to restrict processing.

Based on studies and solutions by [22], future works suggested are on decentralized storage in enhancing the solution's management beyond authentication. This will contribute in providing a more efficient and reliable authentication model in terms of performance, security, and ease of use.

B. Security Enhancement / Analysis

By deploying additional security features, it will not only be able to gain and maintain user trust towards the online services provided, but it will also help in establishing an organization's reputation. Many biological attributes have been explored and deployed as reliable and trustable security features that are hardly compromised. Similarly, a study by [50] has proposed a future plan in combining their proposed scheme with face or iris biometrics for enhanced protection. While [35] aimed to develop a biometric identity-based blind signature scheme.

VIII. Discussion

The security of information, especially personal information and the user's identity, must be protected and preserved from any cyber threat and ensure that it cannot be accessed, used, disclosed or modified without permission by unauthorized parties or cyber criminals who are increasingly worried by the public, especially users of digital services. The emergence of various digital applications which require user identity verification such as face recognition through the selfie process and identity card images as part of a verification and registration process to obtain digital services offered is one of the risks of personal information being exposed to cyber threats. This is due to the security level of the application is difficult to be guaranteed and proved as completely secure, and the location of the information's storage and who has access to the data are also unknown.

Various identity verification methods have been introduced and there are methods that can be combined with additional factors to further strengthen the level of security of user identity

information, such as security tokens, user biometric information, cryptographic or encryption methods, secure environment, and many others. However, the most secure and efficient identity verification model in terms of computing or execution duration, computational cost, and proven to be safe through security tests is difficult to be found [17], [15], [23].

In addition, for the issue of key regeneration for non-revoked users, which was found to be inefficient by [13], a method based on prime-order bilinear groups that includes server-assisted secure methods and selected ciphertexts could be used. While to protect data privacy in Internet of Things (IoT) applications, the Revocable IBE (RIBE) feature, which was proposed by [15], can be adopted as it was found to be effective.

As discussed by [18], although issues related to privacy in smart contracts could be overcome by deploying a new blockchain model to preserve the smart contract privacy as the protection mechanism, a security model for selected ciphertext attacks should be established, as well as security for various types of cryptographic assumptions should be explored.

By referring to study that have been done by [19], where numerous challenges were encountered related to digital identity management, further research to create a more robust digital identity ecosystem in order to achieve a more secure environment and ensure the seamless integration across different platforms is highly needed.

The main limitation of IBE is its reliance on PKGs, which are a single point of failure and a valuable target for attackers. This can be overcome by using Artificial Intelligence (AI) or Machine Learning (ML) to improve anomaly detection, as AI/ML can monitor PKG activity for unusual patterns and identify attempted compromises or unauthorized access attempts more quickly and effectively. Additionally, AI can analyze the global threat landscape and predict potential attack vectors targeting PKGs.

For the issue of the inefficiency of IBE for practical use due to bitwise message encryption, which leads to ciphertext expansion and high computational cost, especially for decryption, ML can be used to analyze the computational cost of IBE algorithms, identify bottlenecks, and suggest optimizations to speed up processes such as decryption without compromising security.

Thus, more detailed studies still need to be carried out as an effort to strengthen user identity verification methods that include efficient cryptography or encryption methods, secure authentication environment from any threat, interoperability across platform, as well as proof of performance and security levels that need to be obtained through security performance tests using security equipment and real-world environment scenarios in having a more appropriate and practical models that can be used in various fields.

IX. Conclusion

Based on the review and analysis from previous works that have been carried out by all the researchers in various topics that are related to user authentication using IBE scheme, numerous schemes and models can be adopted to ensure that the user identity verification process, especially user's information and privacy of data, is protected from any possible risks such as identity theft and cyber-attack like Man-in-the- Middle (MITM) attack. All the proposed solutions have its own advantages and disadvantages, either from the aspect of computing cost for the algorithm used or time taken to execute the algorithm, and the level of deployability in a real-world environment. This will depend on the needs and requirements, which may vary in different fields and industries. However, there are solutions that can be categorized as ideal and suitable to be a sample model in developing a more general model that can be deployed in various fields or industries.

In addition, as proposed and suggested by most of the researchers, integrating the existing IBE scheme with other relevant technologies can increase the level of security and overcome the inherent issues of privacy and trust faced in the IBE scheme. And there are many studies that have deployed new technologies such as blockchain in their solutions [18], [10], [33]. Thus, a general, lightweight, and practical user identity verification model using an IBE scheme that integrates with more secure technologies or environments such as blockchain or other emerging technologies, is expected to be able to overcome the limitations and challenges faced in existing IBE schemes and ensure wide range of implementation across industries, especially in public sectors.

In conclusion, this study aims to provide insights to address challenges faced in existing IBE schemes and proposed areas of study on potential solutions as suggested that may contribute to the development of user authentication models. As digital metaverse keeps evolving, all possible security risks must be taken into serious consideration, especially regarding privacy, accountability and data integrity in order to gain and increase user trust. Important factors such as performance, reliability, efficiency, flexibility and scalability also must be considered in the studies. This study also aims to contribute significant insights related to IBE schemes by analyzing challenges and opportunities and provide a comprehensive understanding of the current state and future directions in order to enhance the security level of user authentication in our daily needs and businesses as user digital identity are crucial in digital services.

Acknowledgment

The authors would like to express sincere gratitude to the Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, for the support in conducting this study. This study was supported by the Universiti Kebangsaan Malaysia (UKM) under the Research Grant Scheme under Grant FRGS/1/2025/ICT07/UKM/02/1.

References

[1] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: A survey," Cryptography, vol. 2, no. 1, pp. 1–31, Mar. 2018, doi: 10.3390/cryptography2010001.

[2] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," in LNCS, 1985, pp. 47–53. doi: 10.1007/3-540-39568-7_5.

[3] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586–615, Jan. 2003, doi: 10.1137/S0097539701398521.

[4] C. Cocks, "An Identity Based Encryption Scheme Based on Quadratic Residues," 2001, pp. 360–363. doi: 10.1007/3-540-45325-3_32.

[5] M. Kasahara, "Cryptosystems based on pairing," in The 2000 Symposium on Cryptography and Information Security, 2000, pp. 26–28.

[6] C. Adams, "Security Analysis of a Privacy-Preserving Identity-Based Encryption Architecture," Journal of Information Security, vol. 13, no. 04, pp. 323–336, 2022, doi: 10.4236/jis.2022.134018.

[7] T. L. Astrizi and R. Custódio, "Seamless Transition to Post-Quantum TLS 1.3: A Hybrid Approach Using Identity-Based Encryption," Sensors, vol. 24, no. 22, p. 7300, Nov. 2024, doi: 10.3390/s24227300.

[8] C. Adams, "Improving User Privacy in Identity-Based Encryption Environments," Cryptography, vol. 6, no. 4, 2022, doi: 10.3390/cryptography6040055.

[9] Y. Liang, G. Di Crescenzo, H. Wang, and Z. Patni, "Efficient Identity-Based Encryption with Minimal Server Trust," in 2024 43rd International Symposium on Reliable Distributed Systems (SRDS), IEEE, Sep. 2024, pp. 104–114. doi: 10.1109/SRDS64841.2024.00020.

[10] R. Saha et al., "A Blockchain Framework in Post-Quantum Decentralization," IEEE Trans Serv Comput, vol. 16, pp. 1–12, 2023, doi: 10.1109/TSC.2021.3116896.

[11] A. Karrothu and J. Norman, "A systematic analysis of Identity Based Encryption (IBE)," International Journal of Knowledge-Based and Intelligent Engineering Systems, vol. 25, no. 3, pp. 343–356, 2021, doi: 10.3233/KES-210078.

[12] K. Lee, "Revocable hierarchical identity-based encryption with adaptive security," Theor Comput Sci, vol. 880, pp. 37–68, Aug. 2021, doi: 10.1016/j.tcs.2021.05.034.

[13] K. Emura, J. H. Seo, and Y. Watanabe, "Efficient revocable identity-based encryption with short public parameters," Theor Comput Sci, vol. 863, pp. 127–155, Apr. 2021, doi: 10.1016/j.tcs.2021.02.024.

[14] W. Gao, L. Yang, D. Zhang, and X. Liu, "Quantum Identity-Based Encryption from the Learning with Errors Problem," Cryptography, vol. 6, no. 1, p. 9, Feb. 2022, doi: 10.3390/cryptography6010009.

[15] Y. Sun, P. Chatterjee, Y. Chen, and Y. Zhang, "Efficient Identity-Based Encryption with Revocation for Data Privacy in Internet of Things," IEEE Internet Things J, vol. 9, no. 4, pp. 2734–2743, Feb. 2022, doi: 10.1109/JIOT.2021.3109655.

[16] J. Kim, "Backward Compatible Identity-Based Encryption," Sensors, vol. 23, no. 9, p. 4181, Apr. 2023, doi: 10.3390/s23094181.

[17] K. Lee, "Delegate and Verify the Update Keys of Revocable Identity-Based Encryption," IEEE Access, pp. 1–1, 2023, doi: 10.1109/ACCESS.2023.3280253.

[18] H. Yin, Y. Zhu, G. Guo, and W. C.-C. Chu, "Privacy-Preserving Smart Contracts for Confidential Transactions Using Dual-Mode Broadcast Encryption," IEEE Trans Reliab, vol. 73, no. 2, pp. 1090–1103, Jun. 2024, doi: 10.1109/TR.2023.3328146.

[19] S. L. Nita and M. I. Mihailescu, "A Novel Authentication Scheme Based on Verifiable Credentials Using Digital Identity in the Context of Web 3.0," Electronics (Basel), vol. 13, no. 6, p. 1137, Mar. 2024, doi: 10.3390/electronics13061137.

[20] M. J. Page et al., "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," Syst Rev, vol. 10, no. 1, p. 89, Dec. 2021, doi: 10.1186/s13643-021-01626-4.

[21] R. Langrehr and J. Pan, "Tightly Secure Hierarchical Identity-Based Encryption," Journal of Cryptology, vol. 33, no. 4, pp. 1787–1821, Oct. 2020, doi: 10.1007/s00145-020-09356-x.

[22] P. Szalachowski, "Password-Authenticated Decentralized Identities," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 4801–4810, 2021, doi: 10.1109/TIFS.2021.3116429.

[23] 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, Jan. 2022, doi: 10.1016/j.tcs.2021.11.021.

[24] S. Liu, Y. Shao, H. Luo, and H. Di, "IBE-Signal: Reshaping Signal into a MITM-Attack-Resistant Protocol," Security and Communication Networks, vol. 2022, pp. 1–24, Jul. 2022, doi: 10.1155/2022/8653453.

[25] M. Clear and H. Tewari, "Anonymous Homomorphic IBE with Application to Anonymous Aggregation," Cryptography, vol. 7, no. 2, p. 22, Apr. 2023, doi: 10.3390/cryptography7020022.

[26] B. Xu et al., "T-FIM: Transparency in Federated Identity Management for Decentralized Trust and Forensics Investigation," Electronics (Basel), vol. 12, no. 17, p. 3591, Aug. 2023, doi: 10.3390/electronics12173591.

[27] J. Sun, G. Xu, T. Zhang, X. Yang, M. Alazab, and R. H. Deng, "Privacy-Aware and Security-Enhanced Efficient Matchmaking Encryption," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 4345–4360, 2023, doi: 10.1109/TIFS.2023.3294725.

[28] D. Hofheinz, J. Koch, and C. Striecks, "Identity-Based Encryption with (Almost) Tight Security in the Multi-instance, Multi-ciphertext Setting," Journal of Cryptology, vol. 37, no. 2, p. 12, Apr. 2024, doi: 10.1007/s00145-024-09496-4.

[29] B. Zuo, J. Li, Y. Zhang, and J. Shen, "Identity-Based Online/Offline Encryption Scheme from LWE," Information, vol. 15, no. 9, p. 539, Sep. 2024, doi: 10.3390/info15090539.

[30] S. Dong, Z. Zhao, B. Wang, W. Gao, and S. Zhang, "SM9 Identity-Based Encryption with Designated-Position Fuzzy Equality Test," Electronics (Basel), vol. 13, no. 7, p. 1256, Mar. 2024, doi: 10.3390/electronics13071256.

[31] K. Asano, K. Emura, and A. Takayasu, "More Efficient Adaptively Secure Lattice-Based IBE with Equality Test in the Standard Model," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E107.A, no. 3, Mar. 2024, doi: 10.1587/transfun.2023CIP0021.

[32] J. Du, G. Dong, J. Ning, Z. Xu, and R. Yang, "Identity-based controlled delegated outsourcing data integrity auditing scheme," Sci Rep, vol. 14, no. 1, p. 7582, Mar. 2024, doi: 10.1038/s41598-024-58325-y.

[33] D. Marchsreiter, "Towards quantum-safe blockchain: Exploration of PQC and public-key recovery on embedded systems," IET Blockchain, vol. 5, no. 1, Jan. 2025, doi: 10.1049/blc2.12094.

[34] H. Wang, K. Chen, Q. Xie, and Q. Meng, "Post-Quantum Secure Identity-Based Matchmaking Encryption," IEEE Trans Dependable Secure Comput, vol. 22, no. 1, pp. 833–844, Jan. 2025, doi: 10.1109/TDSC.2024.3418984.

[35] X. Shan, L. You, and G. Hu, "Two Efficient Constructions for Biometric-Based Signature in Identity-Based Setting Using Bilinear Pairings," IEEE Access, vol. 9, pp. 25973–25983, 2021, doi: 10.1109/ACCESS.2021.3057064.

[36] K. Emura, A. Takayasu, and Y. Watanabe, "Efficient identity-based encryption with Hierarchical key-insulation from HIBE," Des Codes Cryptogr, vol. 89, no. 10, pp. 2397–2431, Oct. 2021, doi: 10.1007/s10623-021-00926-z.

[37] D. Unal, A. Al-Ali, F. O. Catak, and M. Hammoudeh, "A secure and efficient Internet of Things cloud encryption scheme with forensics investigation compatibility based on identity-based encryption," Future Generation Computer Systems, vol. 125, pp. 433–445, Dec. 2021, doi: 10.1016/j.future.2021.06.050.

[38] D. Dharminder, A. K. Das, S. Saha, B. Bera, and A. V. Vasilakos, "Post-Quantum Secure Identity-Based Encryption Scheme using Random Integer Lattices for IoT-enabled AI Applications," Security and Communication Networks, vol. 2022, pp. 1–14, Jul. 2022, doi: 10.1155/2022/5498058.

[39] M. Zhao and Y. Ding, "Dual-Server Identity-Based Encryption with Authorized Equality Test for IoT Data in Clouds," Security and Communication Networks, vol. 2022, pp. 1–12, Oct. 2022, doi: 10.1155/2022/4905763.

[40] Y. Su, Y. Li, and Z. Cao, "Gait-Based Privacy Protection for Smart Wearable Devices," IEEE Internet Things J, vol. 11, no. 2, pp. 3497–3509, Jan. 2024, doi: 10.1109/JIOT.2023.3296650.

[41] X. Hu, L. Wang, L. Gu, and Y. Ning, "A Bilateral Access Control Data Sharing Scheme for Internet of Vehicles," IEEE Internet Things J, vol. 11, no. 22, pp. 36748–36762, Nov. 2024, doi: 10.1109/JIOT.2024.3420176.

[42] N. Gao et al., "Ciphertext Retrieval With Identity Bidirectional Authentication and Matrix Index in IoT," IEEE Internet Things J, vol. 11, no. 1, pp. 889–903, Jan. 2024, doi: 10.1109/JIOT.2023.3288131.

[43] H. Xiong et al., "Heterogeneous Signcryption with Equality Test for IIoT Environment," IEEE Internet Things J, vol. 8, no. 21, pp. 16142–16152, Nov. 2021, doi: 10.1109/JIOT.2020.3008955.

[44] Y. Zhang, Y. Liu, Y. Guo, S. Zheng, and L. Wang, "Adaptively Secure Efficient (H)IBE over Ideal Lattice with Short Parameters," Entropy, vol. 22, no. 11, p. 1247, Nov. 2020, doi: 10.3390/e22111247.

[45] T. A. Lone et al., "Securing communication by attribute-based authentication in HetNet used for medical applications," EURASIP J Wirel Commun Netw, vol. 2020, no. 1, p. 146, Dec. 2020, doi: 10.1186/s13638-020-01759-5.

[46] H. Ji, H. Zhang, L. Shao, D. He, and M. Luo, "An efficient attribute-based encryption scheme based on SM9 encryption algorithm for dispatching and control cloud," Conn Sci, vol. 33, no. 4, pp. 1094–1115, Oct. 2021, doi: 10.1080/09540091.2020.1858757.

[47] A. Wu, D. Feng, M. Zhang, A. Yang, and J. Chi, "Privacy-Preserving Bilateral Multi-Receiver Matching with Revocability for Mobile Social Networks," IEEE Trans Mob Comput, vol. 23, no. 12, pp. 11080–11090, Dec. 2024, doi: 10.1109/TMC.2024.3390036.

[48] S. Liu, L. Chen, G. Wu, H. Wang, and H. Yu, "Blockchain-Backed Searchable Proxy Signcryption for Cloud Personal Health Records," IEEE Trans Serv Comput, vol. 16, no. 5, pp. 3210–3223, Sep. 2023, doi: 10.1109/TSC.2023.3272770.

[49] W. Shen, J. Yu, M. Yang, and J. Hu, "Efficient Identity-Based Data Integrity Auditing with Key-Exposure Resistance for Cloud Storage," IEEE Trans Dependable Secure Comput, vol. 20, no. 6, pp. 4593–4606, Nov. 2023, doi: 10.1109/TDSC.2022.3228699.

[50] M. Whaiduzzaman et al., "HIBAF: A data security scheme for fog computing," Journal of High Speed Networks, vol. 27, no. 4, pp. 381–402, Nov. 2021, doi: 10.3233/JHS-210673.

[51] I. Gomaa, E. Abd-Elrahman, A. Hamdy, and E. M. Saad, "Automated Security Assessment for IDaaS Framework," Wirel Pers Commun, vol. 116, no. 4, pp. 3465–3490, Feb. 2021, doi: 10.1007/s11277-020-07860-8.

[52] C. Jiang, C. Huang, Q. Huang, and J. Shi, "A Multi-Source Big Data Security System of Power Monitoring Network Based on Adaptive Combined Public Key Algorithm," Symmetry (Basel), vol. 13, no. 9, p. 1718, Sep. 2021, doi: 10.3390/sym13091718.

[53] A. Karati, R. Amin, S. H. Islam, and K.-K. R. Choo, "Provably Secure and Lightweight Identity-Based Authenticated Data Sharing Protocol for Cyber-Physical Cloud Environment," IEEE Transactions on Cloud Computing, vol. 9, no. 1, pp. 318–330, Jan. 2021, doi: 10.1109/TCC.2018.2834405.

[54] A. Takayasu and Y. Watanabe, "Revocable identity-based encryption with bounded decryption key exposure resistance: Lattice-based construction and more," Theor Comput Sci, vol. 849, pp. 64–98, Jan. 2021, doi: 10.1016/j.tcs.2020.10.010.

[55] A. S. Almuflih, K. Popat, V. V. Kapdia, M. R. N. M. Qureshi, N. Almakayeel, and R. E. Al Mamlook, "Efficient Key Exchange Using Identity-Based Encryption in Multipath TCP Environment," Applied Sciences, vol. 12, no. 15, p. 7575, Jul. 2022, doi: 10.3390/app12157575.

[56] 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 Transactions on Intelligent Transportation Systems, vol. 23, no. 9, pp. 16161–16169, Sep. 2022, doi: 10.1109/TITS.2022.3148166.

[57] K. Emura and A. Takayasu, "A Generic Construction of CCA-Secure Identity-Based Encryption with Equality Test against Insider Attacks," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E106.A, no. 3, p. 2022CIP0012, Mar. 2023, doi: 10.1587/transfun.2022CIP0012.

[58] X. Zhang, C. Huang, D. Gu, J. Zhang, and H. Wang, "BIB-MKS: Post-Quantum Secure Biometric Identity-Based Multi-Keyword Search over Encrypted Data in Cloud Storage Systems," IEEE Trans Serv Comput, pp. 1–1, 2021, doi: 10.1109/TSC.2021.3112779.

[59] 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 Transactions on Intelligent Transportation Systems, pp. 1–9, 2021, doi: 10.1109/TITS.2021.3125402.

[60] R. Wang et al., "Securing Topology Control in SDWSNs Using Identity-Based Cryptography," J Sens, vol. 2023, no. 1, Jan. 2023, doi: 10.1155/2023/6187353.

[61] C. Zhang, M. Zhao, W. Zhang, Q. Fan, J. Ni, and L. Zhu, "Privacy-Preserving Identity-Based Data Rights Governance for Blockchain-Empowered Human-Centric Metaverse Communications," IEEE Journal on Selected Areas in Communications, vol. 42, no. 4, pp. 963–977, Apr. 2024, doi: 10.1109/JSAC.2023.3345392.

[62] H. Lian, B. Kang, and L. Yang, "Strongly Secure Identity-Based Authenticated Key Agreement Protocol with Identity Concealment for Secure Communication in 5G Network," IEEE Access, vol. 12, pp. 98611–98622, 2024, doi: 10.1109/ACCESS.2024.3428547.

[63] S. Yu, M. Shang, and F. Li, "A lattice-based efficient heterogeneous signcryption scheme for secure network communications," Journal of High Speed Networks, vol. 30, no. 1, pp. 19–27, Jan. 2024, doi: 10.3233/JHS-222020.