Computer Communications 181 (2022) 116–131

Contents lists available at ScienceDirect

Computer Communications

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

Certificateless signature schemes in Industrial Internet of Things: A comparative survey

Saddam Hussain [a], Syed Sajid Ullah [b], Ihsan Ali [c,*], Jiafeng Xie [b], Venkata N. Inukollu [d]

[a] School of Digital Science, Universiti Brunei Darussalam, Jln Tungku Link, Gadong, BE1410, Brunei Darussalam
[b] Department of Electrical & Computer Engineering, Villanova University, USA
[c] Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya, 50603, Kuala Lumpur, Malaysia
[d] Department of Computer Science Purdue University Fort Wayne, Fort Wayne, IN 46805, USA

ARTICLE INFO

Keywords:
Industrial Internet of Things
Signature
Certificateless signature
Wireless networks

ABSTRACT

Internet of Things (IoT), which is a growing domain, provides a universal connection to the Internet by spinning common objects to connected ones by changing the way people communicate and interact with the things around them. This type of setup paves the way for the creation of interconnected infrastructure to support innovative services that ensure improved efficiency and flexibility. Such benefits are attractive for user applications and industrial domain. The entry of the IoT domain into the industrial market, also termed as Industrial Internet of Things (IIoT), was recently observed. However, security threats are increasing daily with the prevalent use of IIoT technology. An efficient security solution that can help in the prevention of malicious attacks is researched despite the existence of multiple security solutions. The current study will help the research community to understand the security flaws and causes by classifying and comparing the different certificateless signature schemes of IIoT domain. This survey aims to provide a comparative analysis of the available solutions to improve security. The multi-criteria decision-making approach is utilized for the comparative analysis of the existing certificateless signature schemes by employing the EDAS technique to evaluate the previously suggested solution proposed for IIoT. The authors believe that this technique has never been previously used for any cryptographic solutions. In addition, the study addresses some of the public research issues for technologists, academia, and researchers to develop the security aspects of IIoT.

1. Introduction

The Internet of Things (IoT) is a self-configuring universal network architecture based on standard interoperable communication protocols that allows things to connect with one another and share information and make collaborative decisions [1]. To understand the dynamic information exchange, various sorts of items in the IoT with independent addresses are commonly connected through heterogeneous transmission networks. Industry 4.0, also known as Industrial IoT (IIoT), is a new study topic that has emerged as a result of IoT applications in the industrial sector [2–4]. Industry 4.0 has had a substantial positive impact on the adoption of IoT across all industries. As a result, smart startups can construct transportation, resource management, manufacturing, renewable energy resources, and smart cities using the IIoT. Digital/connected factories, automated production flow management, industrial security systems, industrial configuration alarms, management security, and worker health (status) monitoring have all gained unexpected attention in the field of smart manufacturing [5–7]. The IIoT system, like any other cyber–physical system, is made up of cyber and physical subsystems that help with data gathering, transmission, and analysis. According to the findings of the investigation, the system can increase monitoring, control, automation, and intelligent event response. Due to the daily increase in the number of devices connected to IIoT, an insecure environment for digital communication may emerge.

The fourth industrial revolution, which is the most devastating in the history of industrial automation, affects industries from healthcare to energy and transportation to manufacturing. The pace of change not only accelerates technological progress but also creates unprecedented opportunities for society through new dangers. Preliminary research results on Industry 4.0 suggest that IIoT devices may be similarly affected [8–10], drawing an equally blurred picture for the security of existing IIoT deployments. In addition, successful attacks on the availability or operational safety of industrial facilities are devastating. In the article [11], the authors address security/privacy issues in the context of the IIoT environment. They reported that the basic

[*] Corresponding author.
E-mail addresses: saddamicup1993@gmail.com (S. Hussain), sullah1@villanova.edu (S.S. Ullah), ihsanalichd@siswa.um.edu.my (I. Ali), jiafeng.xie@villanova.edu (J. Xie), inukollv@pfw.edu (V.N. Inukollu).

https://doi.org/10.1016/j.comcom.2021.10.010
Received 11 May 2021; Received in revised form 30 August 2021; Accepted 8 October 2021
Available online 20 October 2021

security requirements in the IIoT environment include confidentiality, integrity, protection against IoT, device tampering, and authentication of source/provider/sender. The public-key cryptography is generally considered an effective solution to these types of problems. However, key management is essential for resource-constrained devices in IIoT [12]. A certificateless public-key cryptography [13] and digital signature [14] provides an interesting solution for data integrity and authentication. The output of the digital signature gives the user data encryption using his/her signature key. The recipient can verify the digital signature using its affiliate public key. The correlation between private and public keys demonstrates the integrity and authenticity of data [15].

In conventional public-key cryptography, the verification of public-key certificates places an additional drain on certificate management. An IBC [16] suggests avoiding the additional burden where the public is generally calculated from the user IDs, while the corresponding private keys are generated from the Public Key Generator (PKG). However, the PKG knows the private keys of each user and can use these keys to create some fake signatures on important documents that are generally termed as Key Escrow (KE). In [17], Riyami and Peterson proposed the novel concept of certificateless public-key cryptography, which heals the problem of KE. In certificateless public-key cryptography, the PKG calculates a part of the private key known as the partial private key and sends it to the participants. The participants then add some additional information, such as secret values, to calculate its full private key.

An asymmetric technique based on public keys normally needs the authority for issuing certificates to the intended participant in the entire system. Bilinear Pairing, RSA, DSA, Elliptic Curve Cryptosystem (ECC), and El Gammal are generally found in this asymmetric technique [18–20]. In short, the advantage of the aforementioned techniques is their key management efficiency, scalability, and flexibility. However, these solutions are generally energy-consuming, which is unsuitable for resource-constrained devices. However, in many cases, ECC is considered efficient for ensuring security due to its 160-bit key size in contrast to RSA, Bilinear Pairing, and similar asymmetric techniques.

Motivated by the above-mentioned discussion, the suggested certificateless signature solutions presented in the domain of IIoT are analyzed and compared in this survey. The main contributions of this survey are listed below.

- An extensive survey of the existing certificateless signature solutions with their insecurities associated with the suggested solutions presented in the domain of IIoT is provided.
- The merits and demerits of the existing certificateless signature solutions presented in IIoT are discussed.
- A comparison of existing surveys is also provided to clarify the effectiveness of the current study.
- The Multi-Criteria Decision-Making (MCDM) approach is utilized for the comparative analysis of the existing certificateless signature schemes by employing the EDAS technique to evaluate the previously suggested solution proposed for IIoT. We strongly believe that the technique has never been previously used for any cryptographic solutions.
- Some of the public research issues have also been examined and explored for readers, researchers, and academia.

1.1. Overview of industrial internet of things

The Internet of Things [21] has had a significant impact on a variety of industries, particularly in industrial contexts. As a result, the IIoT [22,23] is frequently seen in the industrial settings [24]. IIoT is a new ecosystem that brings together intelligent and autonomous devices, enhanced forecast analytics, and robot–human collaboration to boost production, efficiency, and dependability. The IIoT introduces the world of smart, networked embedded technologies and devices that function as part of a larger, more complicated system. On the hand, IIoT connects billions of mobile devices, manufacturing machinery, industrial equipment, and a variety of other industrial component devices in a similar way to IoT. However, in such an environment, unprecedented industrial data is generated [25]. Fig. 1 depicts a typical three-level communication infrastructure (smart device, gateways, and cloud). During the industrial production process, the condition of deployed devices in the environment is monitored in the specified environment and data is collected. The data is subsequently sent to gateway devices, which transfer it to the cloud server. By allowing data-based services to overcome significant issues in data classification, processing, and storage, the cloud server has the potential to increase IIoT's environmental credibility. However, because cloud servers are controlled by private commercial groups, strategic information can be easily captured and disclosed. Moreover, the IIoT domain needs strong security measures due to wireless communication to ensure the validity of applications against cyber-attacks [26,27]. A cyber-attack can pose a serious risk of affecting human life or undermining resources depending on the strategic nature of the IIoT infrastructure. Therefore, authentication with data privacy is required to store data in the cloud [28]. The digital signature is considered a golden bullet to ensure strong security in the IIoT environment considering data authenticity. Thus, several signature solutions have been suggested for this purpose [29–34]. This survey analyzes and explores the introduced certificateless signature schemes to secure the IIoT domain.

1.2. Survey organization

Section 2 describes the related surveys in the domain of IIoT. Section 3 discusses the preliminaries and security model of certificateless signature schemes. Section 4 is about the taxonomy of the survey. Section 5 consists of the certificateless signature solutions in the domain of IIoT. Section 6 describes the comparative analysis of the suggested schemes considering communication overhead, computation time, security, and complexity assumptions. Section 7 comprises the comparative analysis based on the fuzzy logic method. Section 8 examines and explores some of the public research issues for readers, researchers, and academia. Section 9 concludes the survey. Moreover, Fig. 2 shows the organization of this survey, and the notations used throughout the survey are indicated in Table 1 below.

2. Related surveys

The related works is divided into two sections i.e., existing relevant reviews presented in the domain of IIoT and existing certificateless signature review as mentioned in Table 2 are studied and compared in this section.

(1) IIoT based Surveys

Xu et al. (2014) [3] studied some recent research work based on IoT from industrial perception. Moreover, they added some critical enabling technologies for major IoT applications inside industries. Additionally, the authors analyzed and discussed significant open research challenges and future trends associated with IoT. Unlike previous IoT survey papers, the theme of the current paper centered on IIoT application.

Perera et al. (2015) [35] present a comprehensive survey of IoT solutions in the emerging market. In their survey, the authors broadly discuss market solutions into five different categories, namely smart home, smart wearable, smart city, smart enterprise, and smart environment. Furthermore, they discuss and summarized each of the solutions with its functionality. In addition, their survey examines the contributions of the aforementioned solutions to improve the effectiveness and efficiency of consumer lifestyles.

Mumtaz et al. (2017) [36] discuss roadmaps to address connectivity issues in wireless IIoTs. They also present a detailed review of IIoT from the cyber–physical system perspective. Additionally, their article

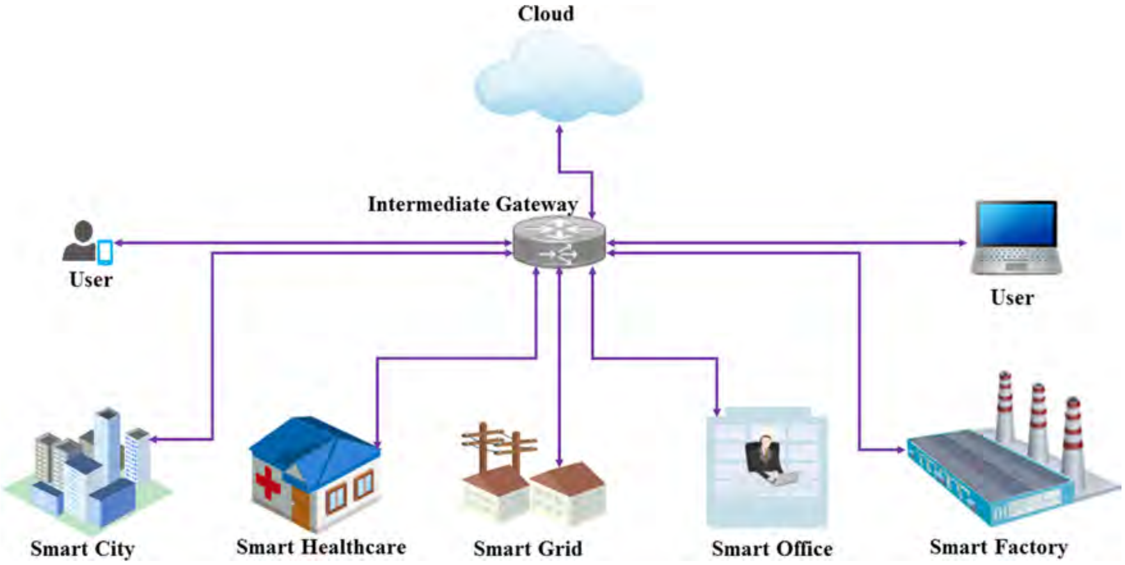


Fig. 1. Typical IIoT architecture with cloud.

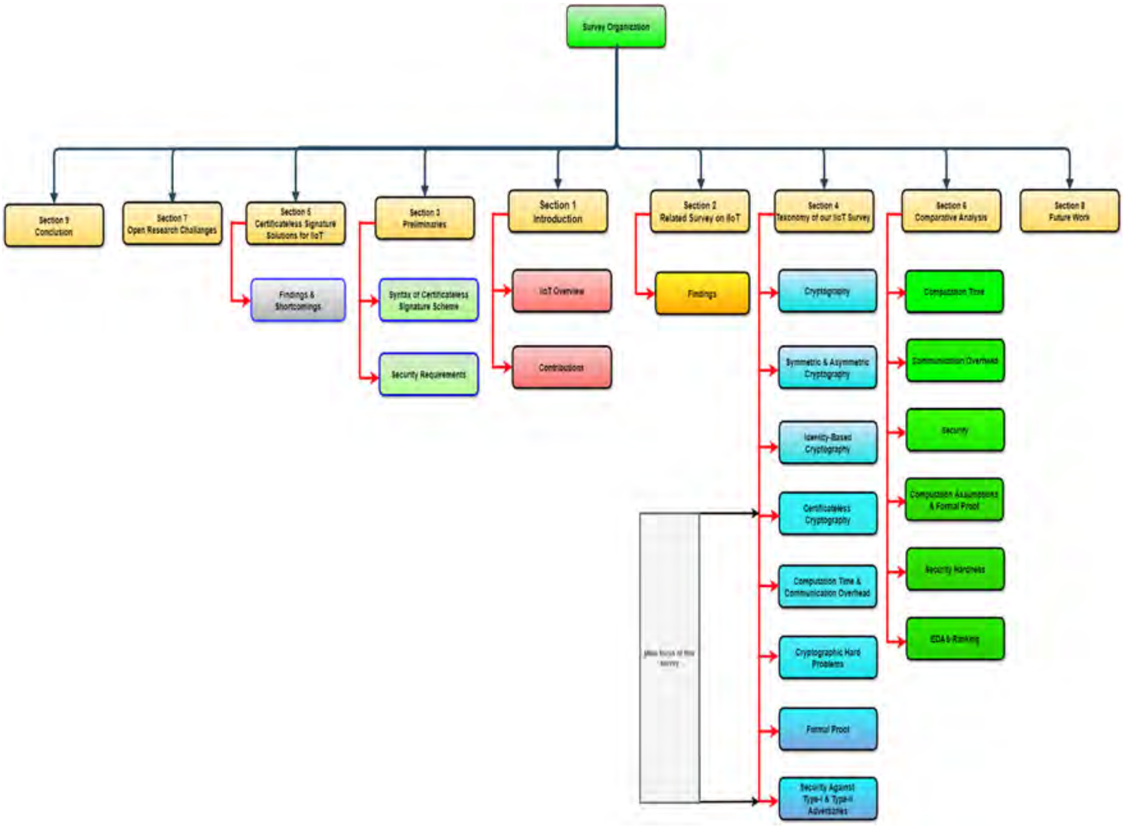

Survey Organization
Section 9 Conclusion
Section 7 Open Research Challanges
Section 5 Certificateless Signature Solutions for IIoT
Findings & Shortcomings
Section 3 Preliminaries
Syntax of Certificateless Signature Scheme
Security Requirements
Section 1 Introduction
IIoT Overview
Contributions
Section 2 Related Survey on IIoT
Findings
Section 4 Taxonomy of our IIoT Survey
Cryptography
Symmetric & Asymmetric Cryptography
Identity-Based Cryptography
Certificateless Cryptography
Computation Time & Communication Overhead
Cryptographic Hard Problems
Formal Proof
Security Against Type-I & Type-II Adversaries
Main focus of this survey
Section 6 Comparative Analysis
Computation Time
Communication Overhead
Security
Computation Assumptions & Formal Proof
Security Hardness
EDAS-Ranking
Section 8 Future Work

Fig. 2. Structure of the survey.

discussed future connectivity issues that must be examined during IIoT implementation.

Zhu et al. (2018) [37] studied trust-based communication for industrial IoT. They suggest the following three mechanisms for trust-based communication: mutual, independent, and collaborative sensor clouds. They also present some open research challenges related to sensor-cloud trust-based communication. Liao et al. (2018) [38] add some systematic reviews of the main contributions related to the Internet of IIoT domain. The authors illustrate their findings and insights after performing an analysis of the collected data. Furthermore, they summarize the strengths and weaknesses of the suggested literature. Sisinni et al. [10] present a preliminary study of the relationships between industry 4.0 and IIoT. Their survey aims to investigate the challenges associated with real-time performance and the need for energy efficiency, interoperability, security and privacy, and coexistence. Furthermore, they include some potential opportunities and challenges considering security and privacy, efficiency, and performance. Long et al. [39] discuss energy-aware routing in the IIoT Domain. They aim to minimize the energy consumption of complex, large-scale IIoT devices. The current article can overcome the shortcomings of the

Table 1
Notation guide.

S.N	Definition	Notation
1	Security Parameter	$\mathcal{N}$
2	System Parameters	$\mathcal{P}$
3	Secret Master Key	$\mathcal{R}$
4	User's Identity	UID
5	Partial Private Key	γ
6	Identity based Cryptography	IBC
7	User's Secret Value	S_V
8	Public Key Generator	PKG
9	User's Public Key	U_{PK}
10	Certificate based cryptography	CBC
11	User's Full Private Key	U_{PT}
12	Signature	δ
13	Type 1 Attacker	T_A
14	Type 2 Attacker	T_B
15	Private Key Generator	PKG
16	Elliptic Curve Cryptosystems	ECC
17	Key Escrow	KE
18	Random Oracle Model	ROM
19	Scalar Point Multiplication Of ECC	PM_{ECC}
20	Pairing-Based Point Multiplication	$Pairing_{PM}$
21	Exponentiation	e
22	Signature Generation	SignGen
23	Communication Cost	CommCost
24	Positive Distance	$\mathcal{P}_d$
25	Evaluation based on Distance from the Average Solution	EDAS
26	Negative Distance	$\mathcal{N}_d$
27	Assessment Scores	Δ

previous literature based on two crucial parameters: the remaining energy and transmission distance. Xu et al. [40] present a detailed review of IIoT, including IIoT applications, architecture, and characteristics. Their survey aims to identify crucial components of the IIoT systems and provide a comprehensive review of IIoT. Additionally, they address some major research challenges. Aazam et al. [24] present an architectural overview of Industry 4.0 and IIoT. They also discuss a potential middle, such as fog, to support local processing for industrial paradigms.

Furthermore, some major research challenges, including security and privacy, context- and semantic-aware service provisioning in IIoT, and energy consumption, are mentioned. The authors also add some future research directions for a wide range of application paradigms in IIoT.

Gumaei et al. [41] present a comprehensive survey of IoTs, technologies, and big data systems in the domain of industry 4.0. They discuss the integration of cloud-based IIoT and big data solutions in the survey. Furthermore, the authors deliberate the issues related to the use of the public cloud for IIoT applications. Boyes et al. [42] helps to develop the definition of IIoT and analyzed partial IoT taxonomies. Furthermore, they comprehensively explore the area of IIoT and its research gaps in technology, network discovery, and security.

Alcácer and Machado (2019) [43] discuss the key enabling technologies and the impact of cloud computing, big data, augmented reality, cybersecurity, and autonomous robots. They also present the research gap between major production systems and Industry 14.0.

Oztemel and Gursev (2020) [44] explore recent trends affecting industry framework and components. They also discuss the industry development life cycle, and projects, such as ENTOC, Parsi, FAI 4.0, INESA, ESIMA, and Meramo. In addition, they deliberate on smart factories and concluded with the challenges and scope of the study. Some real-time security issues can be emphasized for further research. Khan et al. [45] later provided a top-down overview of three important areas: IIoT framework and architecture, data management techniques, and communication protocols.

Jayalaxmi et al. [5] recently explore IIoT security issues, layer-based attacks, detection methods, security services and solutions, deep learning, machine learning, and other security techniques and solutions. Additionally, the authors discuss the attack and effect of security frameworks on security solutions and other techniques based on machine learning.

Finally, the authors believe that they have added an up-to-date review of the importance of certificateless signature schemes presented in the domain of IIoT. The authors of this paper have also analyzed and compared the existing literature of certificateless signature schemes utilizing the MCDM approach by employing the EDAS technique for the first time to a cryptographic scheme to evaluate the previously suggested solution proposed for IIoT. Furthermore, the authors have added a clear understanding of the definition of IIoT and highlighted the issues faced by the cryptographic certificateless signature schemes with some future insights.

(2) Certificateless Signature based Surveys

Housani et al. (2011) [46], study the initial certificateless cryptography scheme suggests by Riyami and Patterson [17]. The aim of the survey was centered on only one scheme.

Chen and Tso (2015) [47], study the security models of certificateless signature schemes. In the given survey the authors only consider two types of issues i.e., strong unforgeability and Public Key Replacement. The aim of the survey was limited to the aforementioned issues.

3. Preliminaries

3.1. Security requirement

The communication process in IIoT normally occurs through an open network. Therefore, the attacker has a full command for unauthorized access to modify the original message and generate the forged signature. The basic security requirements for certificateless signature schemes used in IIoT are mentioned in Fig. 3.

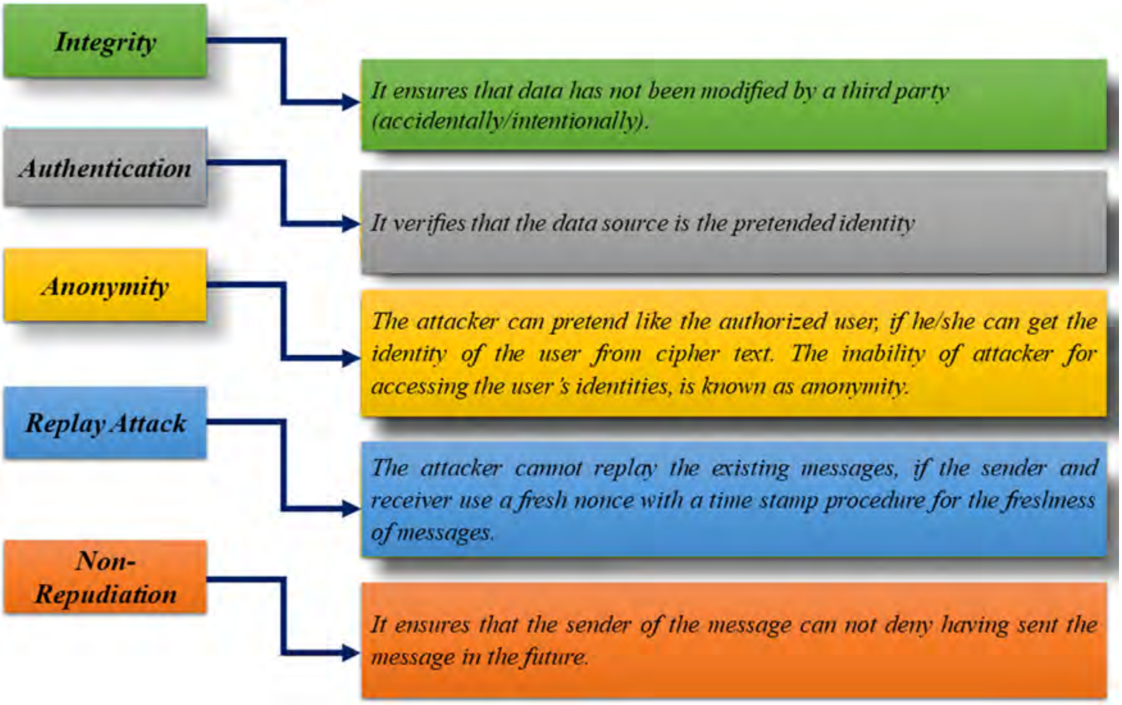
3.2. Generic syntax of certificateless signature scheme

This section discusses the formal concept of a certificateless signature methods. Seven polynomial-time algorithms define the certificateless signature s in general [49–53]. The generic model of certificateless signature is shown in Fig. 4.

1. Setup: This algorithm returns the master key ($\mathcal{R}$) and the system parameters ($\mathcal{P}$) by taking a security parameter ($\mathcal{N}$).
2. Partial Private Key Extraction: The given algorithm takes ($\mathcal{P}$), ($\mathcal{R}$), and the identity (UID) of participants as input and yields the partial private keys (γ) consistent to the participant.
3. Secret Value Setting: This algorithm returns the secret value (S_V) of participants by taking a security parameter ($\mathcal{N}$) and the identities of participants as input.
4. Public Key Setting: This algorithm proceeds the public key (U_{PK}) of the participant by taking the secret value (S_V) of the participant as input.
5. Private Key Setting: This algorithm returns the private key (U_{PT}) of participants by taking γ , U_{PK}, and his/her S_V as input.
6. Sign: Taking the system public parameter set ($\mathcal{P}$), message (M), and U_{PT} as input and returning the signature δ.
7. Verify: Taking M, , U_{PT}, and the signature σ as input and returning 0 or 1.

4. Taxonomy for the proposed survey

The suggested solutions for the security of IIoT are compared through different parameters. Fig. 5 represents the taxonomy for IIoT security.



It ensures that data has not been modified by a third party (accidentally/intentionally).

It verifies that the data source is the pretended identity

The attacker can pretend like the authorized user, if he/she can get the identity of the user from cipher text. The inability of attacker for accessing the user's identities, is known as anonymity.

The attacker cannot replay the existing messages, if the sender and receiver use a fresh nonce with a time stamp procedure for the freshness of messages.

It ensures that the sender of the message can not deny having sent the message in the future.

Fig. 3. Security Requirements.

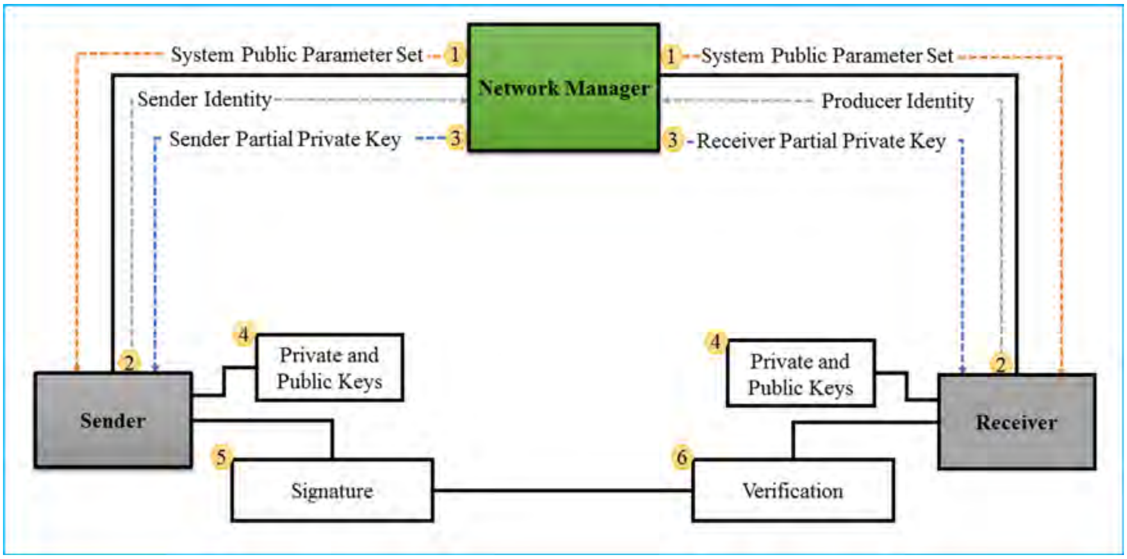


Fig. 4. Generic Illustration of the Certificateless Signature.

4.1. *Cryptography*

Cryptography is an art of secret writing that has been used since Roman times to hide important information/messages. One of the most widely used methods for keeping information is encryption/decryption, which is essentially one of the basic functions of cryptography. A plain text is converted to a non-readable form called ciphertext in encryption, while the ciphertext is converted to plain text in decryption. Both functions are used to protect the message against unauthorized users [54–56].

4.2. *Symmetric and asymmetric*

Cryptography is divided into two types: symmetric and asymmetric [48]. Asymmetric public cryptography, also known as public-key cryptography, uses public and private keys to secure information [57,58]. Symmetric key cryptography focuses on ensuring secure communication between the sender and receiver using a single secret key, whereas asymmetric public cryptography, also known as public-key cryptography, uses public and private keys to secure information. The private key is kept confidential, whereas the public key is widely known due to its open nature.

In symmetric and asymmetric cryptography, the key size is the most critical parameter for secure communication. Because symmetrical cryptography's main size is lower than asymmetric cryptography's, symmetrical cryptography is marginally more secure for sensitive data [59,60].

Table 2
Related surveys (IIoT and Certificateless Signature).

Reference No.	Year of survey	Findings
Xu et al. [3]	2014	Integrate social networking with IoT and the development of green IoT technology in the combination of artificial intelligence and cloud.
Perera et al. [35]	2015	Present a review of artificial intelligence in IoT from the monetization and commercialization perspectives.
Mumtaz et al. [36]	2017	Discuss roadmaps to address connectivity issues in wireless IIoTs.
Zhu et al. [37]	2018	Study trust-based research-related challenges in IIoTs.
Liao et al. [38]	2018	Add some systematic reviews of the main contributions related to the Internet of IIoT domain.
Sisinni et al. [10]	2018	Present a preliminary study of the relationships between industry 4.0 and IIoT and added some opportunities and challenges considering security and privacy, efficiency, and performance.
Long et al. [39]	2018	Discuss energy-aware routing in IIoT domain.
Xu et al. [40]	2018	Present a detailed review of IIoT from the perspective of cyber–physical systems.
Aazam et al. [24]	2018	Add application deployment scenarios in edge-enabled IIoT.
Gumaei et al. [41]	2018	Present a comprehensive survey of IoT, technologies, and big data systems in the domain of industry 4.0.
Boyes et al. [42]	2018	Comprehensively explore the area of IIoT and its research gaps in technology, network discovery, and security.
Alcácer and Machado [43]	2019	Present the research gap between major production systems and Industry 4.0.
Oztemel and Gursev [48]	2020	Discuss smart factory and concluded with the challenges and scope of the study; some real-time security issues can be emphasized for further research.
Khan et al. [45]	2020	Provide a top-down overview of three important areas, including IIoT frameworks and architecture, data management techniques, and communication protocols.
Jayalaxmi et al. [5]	2021	Discuss the attack and effect of security frameworks on security solutions and other techniques based on machine learning.
Housani et al. [46]	2011	Study the initial certificateless cryptography scheme suggests by Riyami and Patterson [17].
Chen and Tso [47]	2015	Study the security models of certificateless signature schemes by considering only two types of issues i.e., strong unforgeability and Public Key Replacement.
Proposed	2021	Comparative analysis of certificateless cryptographic techniques suggested for the domain of IIoT by employing the EDAS technique. Furthermore, this paper highlighted the security challenges and future work based on certificateless signature for IIoT.

4.3. Identity-based cryptography

The public key is commonly calculated from the user IDs, while the matching private keys are created from the PKG, according to identity-based cryptography [16]. The PKG, on the other hand, has access to each user's private keys and can use them to forge signatures on crucial papers known as KE.

4.4. Certificate-based cryptography (CBC)

Gentry introduces CBC, a feasible public-key cryptography primitive, in [61]. This primitive sits somewhere in the middle of IBC and standard public-key cryptography. In the CBC system, the user must first create public and private keys on their own. To apply for a certificate, the user submits his or her identifying information and public key to a trusted Certifier Authority (CA). Each CBC certificate is delivered to its owner and acts as a partial decryption or signature key, unlike typical public-key cryptography certificates.

4.5. Certificateless cryptography

The revolutionary notion of certificateless public-key cryptography proposed by Riyami and Peterson [17] eliminates the KE problem. In certificateless public-key cryptography, the PKG calculates and sends a portion of the private key known as the partial private key to the participants. After then, the participants contribute some extra information, such as a secret value, to calculate the whole private key.

4.6. Computation time and communication overhead

The complexity of the computation or simply the complexity of the algorithm is the number of required resources for its operation, with a particular focus on time and memory requirements. By contrast, a communicational overhead is the number of additional bits that a message will carry with itself.

4.7. Cryptographic hard problems

The security of a scheme is normally measured through the cryptographic hard problems used in a particular scheme, such as Bilinear Pairing and ECC. Therefore, the advantage of these mentioned techniques lies in their key management efficiency, scalability, and flexibility. However, in many cases, ECCs are considered remarkably efficient for ensuring security due to their 160-bit key size.

4.8. Formal proof (standard and random oracle model)

The standard model in cryptography is a computational model in which the advisory is limited only by time and power of computation.

Complexity assumptions underpin cryptographic techniques, implying that some tasks, such as factorization, cannot be solved in polynomial time. In the standard model, security techniques that can only be shown safe using complexity assumptions are safe. In a conventional model, security proof is notoriously difficult to produce. In many proofs, cryptographic primitives are thus replaced with idealized counterparts, such as the Random Oracle Model (ROM). The most typical technique, known as ROM, is to substitute a genuine random function for the cryptographic hash function.

4.9. $Type - I(T_A)$ And $Type - II(T_B)$ adversaries

The T_A adversary replaces the public key and acts as an outsider adversary. The adversary T_A, on the other hand, does not have access to the master key.

The T_B adversary entertain as malicious key generation center. The T_B adversary has access to the master key but is unable to replace the public keys [62].

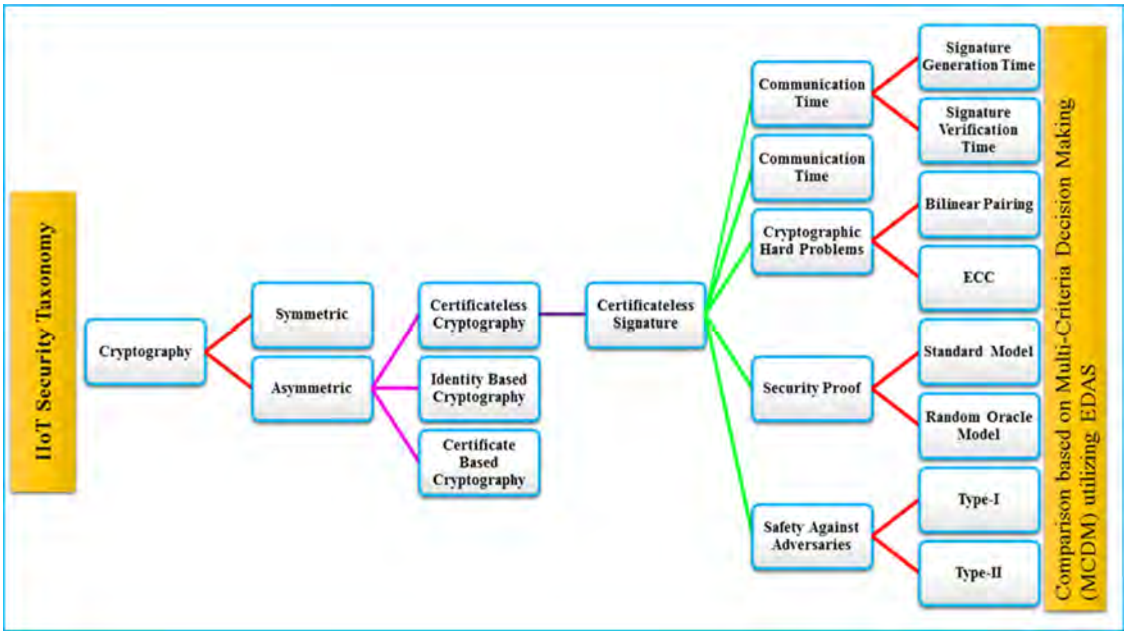

IIoT Security Taxonomy
Cryptography
Symmetric
Asymmetric
Certificateless Cryptography
Identity Based Cryptography
Certificate Based Cryptography
Certificateless Signature
Communication Time
Communication Time
Cryptographic Hard Problems
Security Proof
Safety Against Adversaries
Signature Generation Time
Signature Verification Time
Bilinear Pairing
ECC
Standard Model
Random Oracle Model
Type-I
Type-II
Comparison based on Multi-Criteria Decision Making (MCDM) utilizing EDAS

Fig. 5. IIoT Security Taxonomy.

5. Certificateless signature solutions for IIoT

Several certificateless signature solutions that discuss IIoT security have recently been published. However, none of the existing solutions have a compact security to protect IIoT communications. Different security threats are analyzed in this survey, and a classification of security requirements depending on the motives of the IIoT attack is provided. This classification aims to investigate the realization of a secure IIoT environment. Table 3 illustrates a comparative analysis of the cited literature.

To run the IIoT application, the digital signature approach must have two key features: low execution time and bandwidth utilization. The devices save energy due to the short execution time, while the bandwidth eliminates a critical requirement for wireless communications. It is critical to ensure a secure communication channel between IIoT devices and other systems. Therefore, Karati et al. [29] construct a lightweight certificateless signature scheme to ensure data authentication on IIoT systems. They prove the security of the propose scheme using the security hardness of extended bilinear Strong Diffie–Hellman and bilinear Strong Diffie–Hellman against T_A and T_B in the standard computational model. However, the scheme of Karati et al. [29] found that the solution is insecure by [30] and [31] for the claim properties. In addition, B. Zhang et al. [33] show that the security credentials of Karati et al. [29] are mathematically incorrect. Furthermore, the security of Karati et al. [29] depends on bilinear pairing, which is inappropriate for IIoT devices with limited resources due to the heavy cost of pairing operations.

In the same year, Zhang et al. [30] found that the recommended solution of Karati et al. [29] is insecure of T_A and T_B. However, the authors failed to provide a new scheme to secure IIoT infrastructure.

Y. Zhang et al. (2019) [31] attempt to provide a more efficient certificateless signature approach for data authenticity in IIoT infrastructure. The authors utilize ECC in the proposed approach for security hardness under the standard computational model. Furthermore, the given scheme reduces the cost consumption due to the use of a lightweight algorithm in the form of ECC. Yang et al. (2019) [32] found that the suggested solution of Y. Zhang et al. [31] is not secure against the T_A. However, the authors failed to provide a new scheme to secure IIoT infrastructure. Xiong et al. (2019) [33] later constructed a lightweight certificateless key-insulated scheme under hardness of ECC. The given scheme reduces the cost consumption due to the use of a lightweight algorithm in the form of ECC. In the same year, Rezaeibaghaet al. [34] improve the recommended solution of Karati et al. [29] and present a new concrete certificateless signature scheme under a standard computational model. They report that the designed scheme can resist T_A and T_B. However, K. Shim [63] later found that the scheme of Rezaeibaghaet al. [34] was insecure of T_A. Additionally, the security of Rezaeibaghaet al. [34] depends on bilinear pairing, which is inappropriate for IIoT devices with limited resources due to the heavy cost of pairing operations.

Ali et al. (2021) [64], presents hyperelliptic curve cryptosystem based solution for IIoT to minimize the cost consumption. The authors also presents a security validation proof under AVISPA. However, authors made a false claim that the design scheme is unforgeable against T_A and T_B adversaries. As the design scheme lacks a formal proof in either of ROM/Standard Model.

6. Comparative analysis

The suggested certificateless signature schemes proposed for the IIoT domain are compared in this section considering computation time, communication overhead, security, and cryptographic hard problems.

6.1. Computation time

Finding the computation time for the sender and receiver based on the key cryptographic operations utilized is necessary. Valuable mathematical operations, such as bilinear pairing ($B_{pairing}$), pairing-based point multiplication ($Pairing_{PM}$), scalar point multiplication of ECC (PM_{ECC}), are considered when computing a cryptographic signature algorithm [65]. Therefore, the current suggested studies [30–34] are compared in this section based on the signature generation and verification time. However, addition, division, and hashing, which require less time, are ignored [51,66,67]. Moreover, Table 4 provides a comparison in milliseconds (ms) using the above key cryptographic operations. The experiments performed in [68] and [69] are observed with the following system features. According to [68], single scalar point multiplication of elliptic curve (PM_{ECC}) and bilinear pairing ($B_{pairing}$) will respectively consume 6.38 ms and 20.01 ms, as shown in Table 5.

Table 3
Comparative analysis of the cited literature.

Reference No.	Year of publication	Findings	Limitation
Karati et al. [29]	2018	• First present certificateless signature scheme in the domain of IIoT	• Based on bilinear pairing • Insecure against T_A and T_B attacks • The scheme is mathematically incorrect
B. Zhang et al. [30]	2018	• Show insecurities of Karati et al. [29], T_A and T_B attacks.	• Did not present a solution to the claims
Y. Zhang et al. [31]	2019	• Enhance the security of Karati et al. [29] and construct a new solution utilizing ECC.	• Insecure against the T_A
Yang et al. [32]	2019	• Claim that the recommended solution of Y. Zhang et al. [31] is not secure against T_A	• Did not present a solution to the claims
Xiong et al. [33]	2019	• Present free-pairing key-insulated signature using ECC.	• Proved the security under ROM
Ali et al. [64]	2021	• Presents hyperelliptic curve cryptosystem based solution for IIoT to minimize the cost consumption.	• Unable to provide a formal proof in standard or ROM.

Table 4
Hardware and software specifications.

System	Specification
C Library	MIRACAL
Hardware processor	PIV 3 GHZ
RAM	512 MB
OS	Windows XP

Table 5
Cryptographic major operations time.

S/N	Operation	Computation time
1	Scalar point multiplication of elliptic curve (PM_{ECC})	0.83 ms
2	Bilinear pairing ($B_{pairing}$)	20.01 ms
3	Exponentiation (e)	11.20 ms
4	Pairing-based point multiplication ($Pairing_{PM}$)	6.38 ms

Note: Scalar point multiplication of elliptic curve (PM_{ECC}) means the point multiplication used in ECC based schemes [70,71] while pairing-based point multiplication ($Pairing_{PM}$) means the multiplication used in pairing-based cryptographic schemes [72–74].

Table 6
Signature generation time of the suggested schemes presented in the domain of IIoT.

Operations/Ref. No.	[29]	[31]	[33]	[34]
PM_{ECC}			$1PM_{ECC}$	
$B_{pairing}$				
Exponentiation (e)	2 e			1 e
$Pairing_{PM}$		1 $Pairing_{PM}$		
Signature generation time	22.4	6.38	0.83	11.20

Table 7
Signature verification time of the suggested schemes presented in the domain of IIoT.

Operations/Ref. No.	[29]	[31]	[33]	[34]
PM_{ECC}			$6PM_{ECC}$	
$B_{pairing}$	$1B_{pairing}$	$1B_{pairing}$		$2B_{pairing}$
Exponentiation (e)	2 e			1 e
$Pairing_{PM}$		1 $Pairing_{PM}$		
Signature verification time	42.41	26.39	4.98	51.22

Table 8
Total computation cost of signature generation and signature verification phase.

Operations/Ref. No.	[29]	[31]	[33]	[34]
PM_{ECC}			7 PM_{ECC}	
$B_{pairing}$	$1B_{pairing}$	$1B_{pairing}$		$2B_{pairing}$
Exponentiation (e)	4 e			2 e
$Pairing_{PM}$		2 $Pairing_{PM}$		
Total computation time in ms	64.81	32.77	5.81	62.42

(1). Signature Generation Phase

In the scheme of Karati et al. [29], the sender of the message first executes the signature generation algorithm, which takes 2 e mathematical operations. The scheme of Y. Zhang et al. [31] takes 1$Pairing_{PM}$ operation in the signature generation phase. The schemes of Xiong et al. [33] and Rezaeibagha et al. [34] respectively take $1PM_{ECC}$ and 1 e costly mathematical operation in the signature generation phase. However, the schemes of B. Zhang et al. [30] and Yang et al. [32] are ignored from the comparative analysis in the case of the signature generation phase because both given schemes are based on cryptanalysis and do not present a new scheme. Moreover, Table 6 and Fig. 6 show the comparative analysis considering major cryptographic operations used in signature generation time of the suggested schemes proposed to secure the communication of IIoT.

(2). Signature Verification Phase

In the scheme of Karati et al. [29], the receiver of the message executes the signature verification algorithm, which takes 2 e and $1B_{pairing}$ mathematical operations. The schemes of Y. Zhang et al. [31] and Xiong et al. [33] respectively take 1 $Pairing_{PM}$ and $1B_{pairing}$ operations and $6PM_{ECC}$ costly mathematical operation in the signature verification phase. Meanwhile, the scheme of Rezaeibagha et al. [34] takes 1 e and $2B_{pairing}$ operations in the signature verification phase. However, the schemes of B. Zhang et al. [30] and Yang et al. [32] are ignored from the comparative analysis in the case of the signature verification phase because both given schemes are based on cryptanalysis and do not present a new scheme while Ali et al. [64], did not present a formal proof. Moreover, Table 7 and Fig. 7 present the comparative analysis considering major cryptographic operations used in signature verification time of the suggested schemes proposed to secure the communication of IIoT.

(3). Total Computation Time of Signature Generation and Verification

In the scheme of Karati et al. [29], the total computation time of signature verification and signature verification becomes 4 e + $1B_{pairing}$. The scheme of Y. Zhang et al. [31] takes $1B_{pairing}$+2 $Pairing_{PM}$ costly operations in the signature generation and signature verification phase. The schemes of Xiong et al. [33] and Rezaeibagha et al. [34] respectively take 7 PM_{ECC} costly mathematical operation and 2 e and $2B_{pairing}$ operations in the signature generation and signature verification phase. Moreover, Table 8 and Fig. 8. Present the comparative analysis considering major cryptographic operations used in the signature verification and signature generation phase of the suggested schemes.

Summary

Most of the existing certificateless signature schemes suggested for IIoT infrastructure utilized bilinear pairings. Though the schemes are proven secure in the standard computational model, the use of bilinear pairing increases the computational complexity of the suggested solutions. On the other hand, the scheme of Xiong et al. [33], were constructed on ECC under ROM. Unfortunately, ROM is considered as a theoretical model where the hash function is modeled as a random oracle and is controlled by a simulator of the security approach [75–77]. Hence, there is a need for a secure ECC-based cryptographic

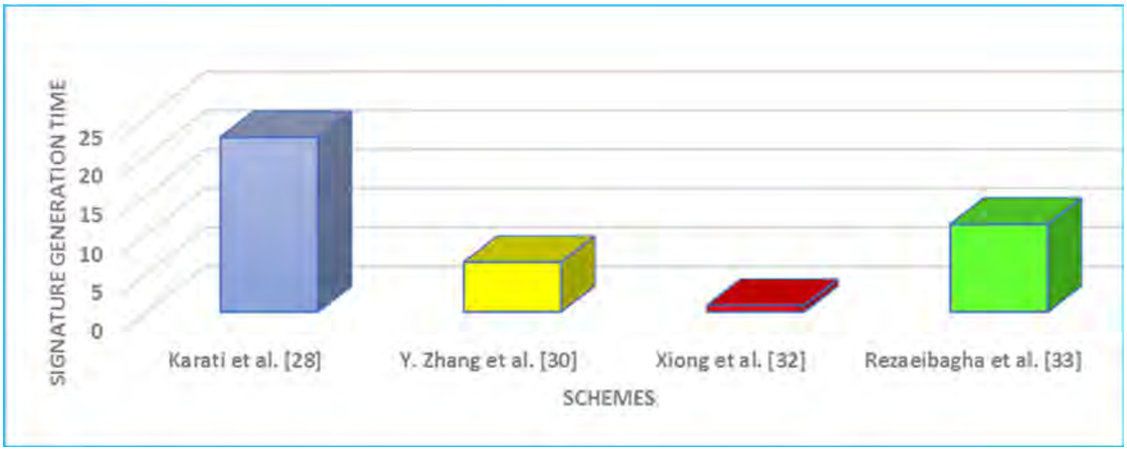


Fig. 6. Signature generation time of the suggested schemes presented in the domain of IIoT.

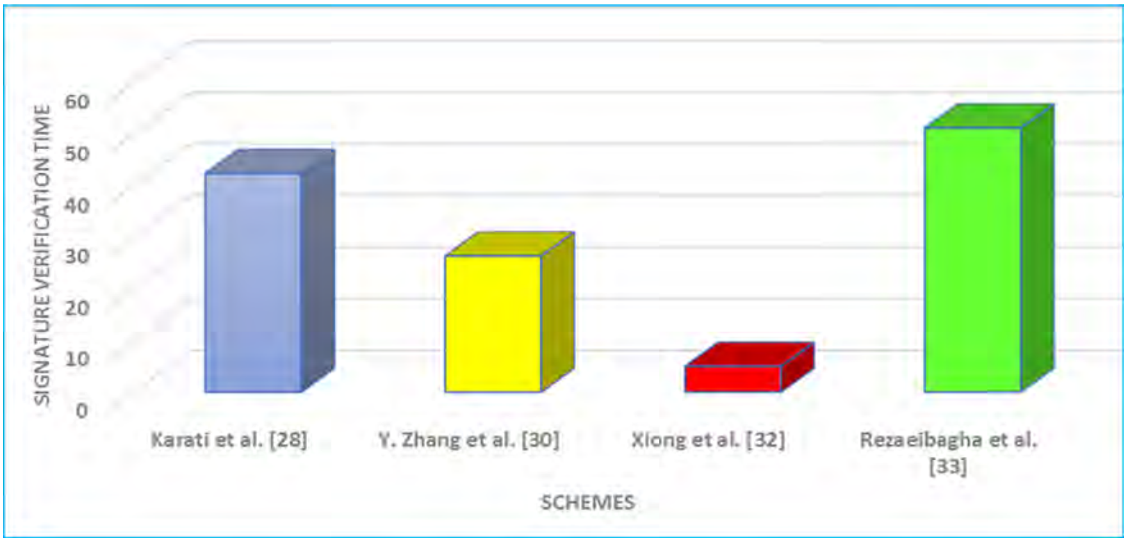


Fig. 7. Signature verification time of the suggested schemes presented in the domain of IIoT.

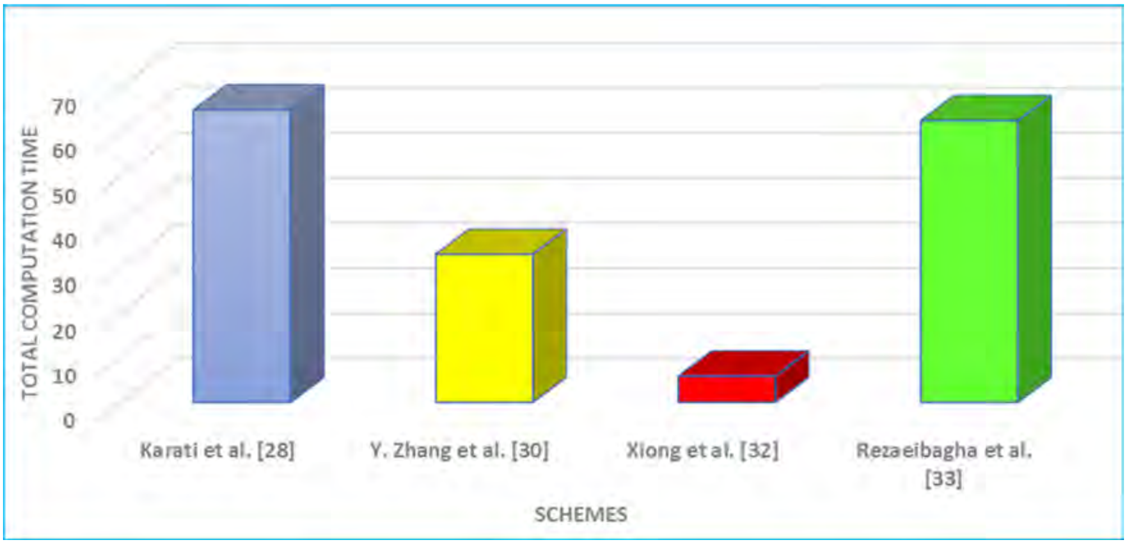


Fig. 8. Total computation cost of signature generation and verification phase.

Table 9
Communication overhead analysis of the suggested schemes presented for the domain of IIoT.

Schemes	Signature length	Total cost in bits
Karati et al. [29]	$2\,|\mathcal{G}|$	2048
Y. Zhang et al. [31]	$2\,|\mathcal{G}|$	2048
Xiong et al. [33]	$3\,|\mathcal{Q}|$	480
Rezaeibagha et al. [34]	$2\,|\mathcal{G}|$	2048

Table 10
Classification based on cryptographic algorithm.

Algorithm	Schemes
Bilinear pairing cryptosystem	Karati et al. [29], Y. Zhang et al. [31] and Rezaeibagha et al. [34]
Elliptic curve cryptosystem	Xiong et al. [33]

Table 11
Classification based on security against T_A and T_B adversaries.

Schemes	Security against T_A	Security against T_B
Karati et al. [29]	NO	NO
Y. Zhang et al. [31]	NO	NO
Xiong et al. [33]	YES	YES
Rezaeibagha et al. [34]	NO	YES

scheme under a standard computational model which is able to fulfill the security requirement of IIoT.

6.2. Communication overhead

The previously suggested certificateless signature schemes in the IIoT domain will be compared in this section considering communication overhead. Some variables, such as $|\mathcal{G}| = 1024$ bits for Bilinear Pairing and $|\mathcal{Q}| = 160$ bits for ECC cryptosystem, are assumed for the comparative analysis [51,65,69].

The theoretical calculation revealed that the communication overhead for the schemes of Karati et al. [29], Y. Zhang et al. [31], Xiong et al. [33], and Rezaeibagha et al. [34] is $2\,|\mathcal{G}|$, $2\,|\mathcal{G}|$, $3\,|\mathcal{Q}|$, and $2\,|\mathcal{G}|$, respectively. Moreover, Table 9 and Fig. 9 represent the comparative analysis considering the major communication overhead used in the suggested schemes while securing the communication of IIoT.

Summary

The existing certificateless signature schemes utilized Bilinear Pairing for security efficiency. However, Bilinear Pairing significantly increases the communicational complexity of the suggested solutions. On the other hand, the scheme of Xiong et al. [33], are constructed on ECC utilizing 160-bits. Hence, an ECC-based cryptographic scheme can better suit IIoT due to its minimal use of communicational resources.

6.3. Comparison considering cryptographic hard problems

The existing suggested solutions presented for IIoT are classified in this section based on hard problems as shown in Table 10. The schemes of Karati et al. [29], Y. Zhang et al. [31], and Rezaeibagha et al. [34] are constructed on bilinear pairing, while the scheme of Xiong et al. [33] is constructed on ECC utilizing 160 bits.

6.4. Comparison based on T_A and T_B adversaries

The existing suggested solutions presented for IIoT based on security against T_A and T_B adversaries are classified in this section as shown in Table 11. The schemes of Karati et al. [29], Y. Zhang et al. [31], and Rezaeibagha et al. [34] are insecure of T_A and T_B adversaries, while the scheme of Xiong et al. [33] is considered secure against T_A and T_B adversaries under ROM.

Table 12
Classification based on formal proof and complexity assumptions.

Schemes	Formal proof	Complexity assumptions
Karati et al. [29]	Standard model	$q-$EBSDH and $q-$BSDH
Y. Zhang et al. [31]	Standard model	$(q_s+1)-$SDH
Xiong et al. [33]	ROM	DL
Rezaeibagha et al. [34]	Standard model	$q-$BSDH

6.5. Comparison based on formal proof and complexity assumptions

The existing suggested solutions presented for IIoT on the basis of security formal proof and complexity assumptions are classified in this section as shown in Table 12. The scheme of Karati et al. [29] is constructed based on $q-EBSDH\&q-BSDH$ under the standard model. Meanwhile, the scheme of Y. Zhang et al. [31] is based on $\left(q_s+1\right)-SDH$ under standard model assumptions. Similarly, the scheme of Rezaeibagha et al. [34] is constructed based on $q-BSDH$ under the standard model, while the scheme of Xiong et al. [33] is based on DL assumptions under ROM.

6.6. Findings

The theoretical analysis shows the computational cost complexity of the bilinear operations of bilinear pairing and modular exponentiation is considerably higher than the scalar multiplication of the elliptical curve. Therefore, the scheme of Xiong et al. [33] has better performance than that of Karati et al. [29], Y. Zhang et al. [31], and Rezaeibagha et al. [34]. Moreover, the schemes of Karati et al. [29], Y. Zhang et al. [31], and Rezaeibagha et al. [34] are constructed on a standard model but insecure against T_A and T_B adversaries.

6.7. Open challenges

The number of IIoT devices and the amount of data are growing. This increase addresses several security issues to ensure the evaluation of a secure IIoT infrastructure. Section 4 reveals that several explicit solutions have been suggested to improve IIoT security. However, developing a lightweight certificateless signature security solution suitable for resource-constrained devices is still a challenge.

6.8. Ranking based on performance evaluation using EDAS

EDAS is a method used as an average solution for evaluating alternatives. The method was first presented by Ghorabaee et al. [78]. In EDAS, two activities, which are defined as Positive Distance from Average and Negative Distance from Average solution, are measured for the evaluation. The EDAS is an MCDM that calculates the distance of every alternative solution from the average solution and then using that particular information to select the best alternative [79].

The existing literature of certificateless signature schemes utilizing the MCDM approach has also been analyzed and compared by employing the EDAS technique for the first time to a cryptographic scheme to evaluate the previously suggested solution proposed by the IIoT [80] and [81]. Comparing the performance of different schemes with excellent results [82] and [83] is an effective method. The performance metrics of Signature Generation (SignGen), Signature Verification (SigVeri), Communication Cost (CommCost), Security, Formal verification tool, and security hardness have been selected as shown in Table 12.

The fuzzy-logic Evaluation Based on Distance from the Average Solution (EDAS)evaluation [84–86]. Table 12 demonstrate the comparative analysis of the different identified performance matrices. Additionally, the cross −EDAS method in this appraisal is utilized to pick the most effective values of the six different approaches on the basis of the selected parameters. On the other hand, the assessment scores (Δ)

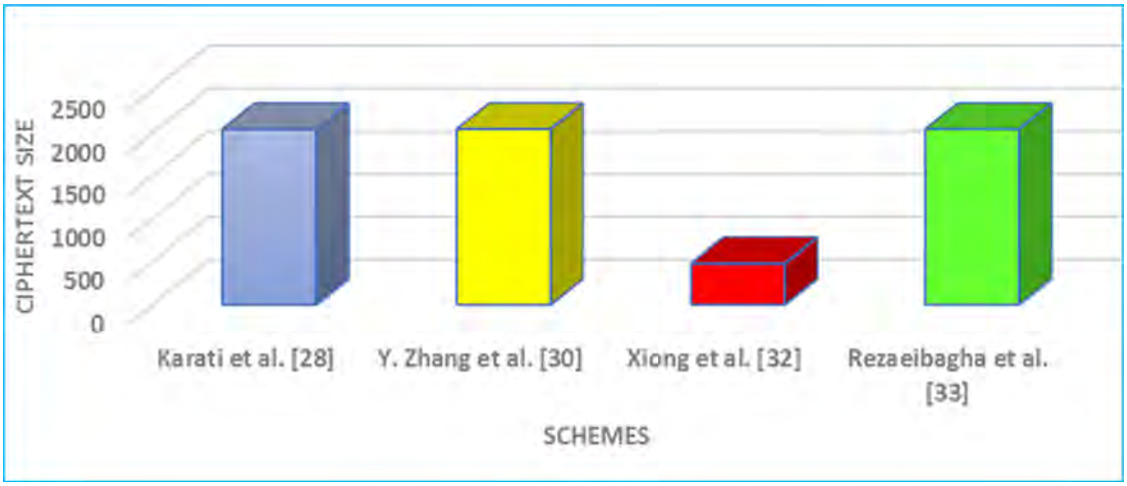


Fig. 9. Communication overhead analysis of the suggested certificateless signature schemes presented by IIoT.

are used to calculate the ranking of the existing techniques. Table 13 considers the performance matrices of the suggested schemes.

The weightage assigned to SignGen is "0.125", weightage assign to SigVeri is "0.125", weightage assign to CommCost is "0.25", weightage assign to Security is "0.2", weightage assign to Security hardness is "0.15" and for Formal Proof is "0.15".

Step One:

The solution of the average value ($\boldsymbol{\pi}$) of the selected matrices is calculated.

$$(\phi) = \left[\boldsymbol{\pi}_b\right]_{1\times\beta}, \tag{1}$$

While

$$= \frac{\sum_{i=1}^{y} X_{ab}}{y}. \tag{2}$$

The aforementioned step states the performance of the selected matrices as the criteria of suggested solutions. Moreover, the aggregate calculation of Eqs. (1) and (2) can be attained as an $\boldsymbol{\pi}$ for each calculated value on each selected matrix, as given in Table 14.

Step Two

In step two of the EDAS-based on Positive Distance from Average (P_{dav}), Equations (3), (4), and (5).

$$P_{dav} = \left[\left(P_{dav}\right)_{ab}\right]_{\beta\times\beta}. \tag{3}$$

If the state bth is favorable, than

$$\left(P_{dav}\right)_{ab} = \frac{\mathcal{MAX}\left(0, \left(Ave_b - X_{ab}\right)\right)}{Ave_b} \tag{4}$$

And for less favorable, it becomes;

$$\left(P_{dav}\right)_{ab} = \frac{\mathcal{MAX}\left(0, \left(X_{ab} - Ave_b\right)\right)}{Ave_b}, \tag{5}$$

where P_{dav} represents the Negative Distance of bth rated algorithm from the given average value on the ath rating performance matrices. The outputted result is shown in Table 15.

Step Three:

The Negative Distance from Average (N_{dav}) is calculated in this step using Equations (6), (7), and (8).

$$\left(N_{dav}\right) = \left[\left(N_{dav}\right)_{ab}\right]_{\beta\times\beta}. \tag{6}$$

If the bth criterion is more favorable than

$$\left(N_{dav}\right)_{ab} = \frac{\mathcal{MAX}\left(0, \left(Ave_b - X_{ab}\right)\right)}{Ave_b} \tag{7}$$

And if less desirable, then the given above equations become

$$\left(N_{dav}\right)_{ab} = \frac{\mathcal{MAX}\left(0, \left(X_{ab} - Ave_b\right)\right)}{Ave_b}, \tag{8}$$

where $\left(N_{dav}\right)_{ab}$ represents the Negative Distance of bth rated algorithm from the given average value of the ath rating performance matrices. The outputted result is shown in Table 16.

Step Four:

The weighted sum of the Positive Distance ($\mathcal{P}_d$) for the rated algorithm is calculated at this stage as illustrated in Table 17.

$$\left(WS_{\mathcal{P}_d}\right)_a = \sum_{b=1}^{y} \lambda_b \left(\mathcal{P}_d\right)_{ab}. \tag{9}$$

Step Five:

The weighted sum of the Negative Distance ($\mathcal{N}_d$) for the rated algorithms is calculated in this stage by means of the following formula, the outcomes are shown in Table 18.

$$\left(WS_{\mathcal{N}_d}\right)_a = \sum_{b=1}^{y} \lambda_b \left(\mathcal{N}_d\right)_{ab} \tag{10}$$

Step Six:

The calculated scores based on the $\left(WS_{\mathcal{P}_d}\right)_a$ & $\left(WS_{\mathcal{N}_d}\right)_a$, which are based on the rated technique, are respectively given in the subsequent Eqs. (11) and (12).

$$\mathcal{N}\left(WS_{\mathcal{P}_d}\right)_a = \frac{\left(WS_{\mathcal{P}_d}\right)_a}{\mathcal{MAX}_a\left(\left(WS_{\mathcal{P}_d}\right)_a\right)}, \tag{11}$$

$$\mathcal{N}\left(WS_{\mathcal{N}_d}\right)_a = 1 - \frac{\left(WS_{\mathcal{N}_d}\right)_a}{\mathcal{MAX}_a\left(\left(WS_{\mathcal{N}_d}\right)_a\right)}. \tag{12}$$

Step Seven:

The score values based on $\left(WS_{\mathcal{P}_d}\right)_a$ & $\mathcal{N}\left(WS_{\mathcal{N}_d}\right)_a$, which are based on the evaluation scores (ψ) for the rated schemes are evaluated in this section.

$$\Delta = \frac{1}{2}\left(\mathcal{N}\left(WS_{\mathcal{P}_d}\right)_a - \mathcal{N}\left(WS_{\mathcal{N}_d}\right)_a\right), \quad \text{where } 0 \le \Delta \ge 1.$$

The final output of Δ is determined using the aggregate values of both $\mathcal{N}WS_{\mathcal{P}_d}$ & $\mathcal{N}WS_{\mathcal{N}_d}$.

Step Eight:

The sequence of the aforementioned activities considers the extent of Δ and generate the ranking of given schemes. The obtained results certify that best solution has a higher evaluation scores than that of the other solutions. Consequently, the scheme of Xiong et al. [33] has the highest evaluation score (Δ) as shown in Table 18. Therefore, the last calculated rank result is shown in Table 19.

The final output of the EDAS ranking indicates that the solution suggested by Xiong et al. [33] outperforms the suggested certificateless signature schemes proposed in the domain of IIoT. Moreover, the output table lists the suggested certificateless signature schemes based on the selected matrices. The comparative analysis based on fuzzy logic revealed that the scheme of Xiong et al. [33] is on top based on the selected matrices, while that of Y. Zhang et al. [31] and Rezaeibagha et al. [34] ranked second and third, respectively. Meanwhile, the scheme of Karati et al. [29] ranked fourth according to the selected matrix.

Findings

The EDAS technique has been applied to evaluate the suggested certificateless signature schemes presented for IIoT domain in order to find the idlest solution among the suggested. For this purpose, we choose the performance metrics of Signature Generation (SignGen), Signature Verification (SigVeri), Communication Cost (CommCost), Security, Formal verification tool, and security hardness, respectively. The analysis indicates that the solution suggested by Xiong et al. [33] outperforms the suggested certificateless signature schemes proposed in the domain of IIoT.

Open Challenges

The scheme suggested by Xiong et al. [33] outperforms the remaining solutions proposed for IIoT domain. However, this scheme needs some improvement in terms of cost consumption as well as security. As the scheme of Xiong et al. [33] is proven secure under ROM. So, there is a need for a secure ECC-based secure scheme under the standard computation model.

7. Challenges and open research issues

This paper investigated the suggested literature on the security of IIoT discussed in the previous sections. The results reveal that the security issues in IIoT must be addressed to realize its complete implementation. This survey highlighted the issues and findings of the suggested certificateless signature schemes proposed for the IIoT domain. A concrete certificateless signature scheme may be proposed for IIoT due to security vulnerabilities and lack of authentication scheme in the IIoT environment. All certificateless signature solutions suggested for securing the IIoT domain are examined, analyzed, and discussed in this survey. However, IIoT applications can be secured by adopting a universally concrete IIoT security scheme and considering the IIoT security solutions suggested in this survey. The authors believe that none of the certificateless signature schemes is recommended for effectively securing IIoT infrastructure work considering security and cost-efficiency. Section 4 presents a comparative analysis of the security solutions (certificateless signature schemes) presented in the domain of IIoT based on the selected criterion. From a high-level synthetic picture, IIoT still faces some open issues that must be considered. Some open research challenges that need serious investigation are presented as follows.

7.1. Key distribution problem

Notably, the cryptographic solutions presented in the literature for securing the IIoT are efficient in all aspects and do not satisfy the security necessities. Thus, the solutions based on certificateless signature schemes adopted for industrial IoT generally suffer from partial private key distribution problems in new certificateless signature schemes.

7.2. Insecurities against T_A and T_B adversaries

IIoT must withstand the possible security threats in its domain. However, the comprehensive analysis showed that the suggested solutions are subject to Public-Key-Replacement-Attack and Known-Message-Attack. Therefore, a new solution must consider these threats while designing a cryptographic certificateless signature scheme for IIoT.

7.3. Scheme for big data analytics

The IIoT is commonly utilized for data-related applications in which devices generate large amounts of data. The created data is saved on a cloud server, where the machine learning algorithm performs data preparation, extraction, and analysis. The algorithm's average processing time ranges from days to months [87]. Furthermore, important concerns with this method include privacy leaks, access control mechanisms, and so on.

7.4. Computation and communication cost complexity

Most of the devices utilized in IIoT domain are resource-constrained. These devices have limitations in terms of processing power and storage capacity. The certificateless signature solutions adopted for IIoT are time-consuming, as shown in Table 9. The existing solutions are based on classical asymmetric approaches, such as ECC and bilinear pairing. According to [25,30], bilinear pairing and ECC are unsuitable for resource-constrained devices due to their high energy consumption. A new solution based on certificateless signature should be adopted to tradeoff between energy consumption and security level of the certificateless signature solution. The solution should ensure an adequate level of security with the expense of minimal energy consumption for the resource-constrained devices of IIoT.

7.5. Framework for dynamic security

Heterogeneous devices, spanning from low-power gadgets to high-power servers, are connected in the IIoT domain. As a result, a universal solution may not be applicable to all IIoT systems. Besides, security solution should also take the nature of a lightweight in terms of powers with an additional support for the end users basic security requirements. Thus, developing a flexible and dynamic certificateless signature security framework for IIoT domain is an interesting research topic.

8. Future work

The authors believe that the future IIoT must efficiently handle and secure data based on earlier surveys on the IIoT and the suggested solutions based on certificateless signature. The main future research works after analyzing the existing literature regarding certificateless signature schemes in IIoT are summarized below.

- The suggested solutions are subject to Public-Key-Replacement-Attack and Known-Message-Attack. However, an efficient certificateless signature scheme for IIoT is necessary considering the existing security flaws in the suggested certificateless signature solutions proposed for IIoT environment.
- Most of the author's utilize pairing-based cryptography, which is subject to heavy pairing operations, thus making it inefficient, especially in the deployment of IIoT. Hence, the construction of an efficient certificateless signature scheme is an open problem.
- The security proof for the recommended solutions is examined, and a new scheme is proposed to demonstrate the security of the IIoT scheme not only in the ROM but also in the standard model. Existing security models are explored, and the adversarial attack capability is observed.

Table 13
Performance metrics of suggested schemes.

Selected matrices						
Ref. No	SignGen (ms)	SigVeri (ms)	CommCost (bits)	Security (Yes/NO)	Formal proof (ROM = 0, SM = 1)	Security hardness (BP = 0, ECC = 1)
Karati et al. [29]	22.4	42.41	2048	0	1	0
Y. Zhang et al. [31]	6.38	26.39	2048	0	1	0
Xiong et al. [33]	0.83	4.98	480	1	0	1
Rezaeibagha et al. [34]	11.2	51.22	2048	0	1	0

Table 14
Cross efficient values.

Selected matrices						
Ref. No	SignGen (ms)	SigVeri(ms)	CommCost (bits)	Security (Yes/NO)	Formal proof (ROM = 0, SM = 1)	Security hardness (BP = 0, ECC = 1)
Karati et al. [29]	22.4	42.41	2048	0	1	0
Y. Zhang et al. [31]	6.38	26.39	2048	0	1	0
Xiong et al. [33]	0.83	4.98	480	1	0	1
Rezaeibagha et al. [34]	11.2	51.22	2048	0	1	0
Average	10.2025	31.25	1656	0.25	0.75	0.25

Table 15
Analysis results of average P_{dav}.

Selected matrices						
Schemes	SignGen (ms)	SigVeri(ms)	CommCost (bits)	Security (Yes/NO)	Formal proof (ROM = 0, SM = 1)	Security hardness (BP = 0, ECC = 1)
Karati et al. [29]	0	0	0	0	0.333333333	1
Y. Zhang et al. [31]	0.374663073	0.15552	0	0	0.333333333	1
Xiong et al. [33]	0.91864739	0.84064	0.710144928	3	0	0
Rezaeibagha et al. [34]	0	0	0	0	0.333333333	1

Table 16
Analysis results of average N_{dav}.

Selected matrices						
Schemes	SignGen (ms)	SigVeri(ms)	CommCost (bits)	Security (Yes/NO)	Formal proof (ROM = 0, SM = 1)	Security hardness (BP = 0, ECC = 1)
Karati et al. [29]	1.195540309	0.35712	0.236714976	1	0	0
Y. Zhang et al. [31]	0	0	0.236714976	1	0	0
Xiong et al. [33]	0	0	0	0	1	3
Rezaeibagha et al. [34]	0.097770154	0.63904	0.236714976	1	0	0

Table 17
Comparative analysis results of the $(WS_{\mathcal{P}_d})_a$.

Selected matrices							
Schemes	SignGen (ms)	SigVeri(ms)	CommCost (bits)	Security (Yes/NO)	Formal proof (ROM = 0, SM = 1)	Security hardness (BP = 0, ECC = 1)	$(WS_{\mathcal{P}_d})_a$
Karati et al. [29]	0	0	0	0	0.05	0.15	0.2
Y. Zhang et al. [31]	0.046832884	0.01944	0	0	0.05	0.15	0.266272884
Xiong et al. [33]	0.114830924	0.10508	0.177536232	0.6	0	0	0.997447156
Rezaeibagha et al. [34]	0	0	0	0	0.05	0.15	0.2

Table 18
Analysis results of the aggregate $(WS_{\mathcal{N}_d})_a$.

Selected matrices							
Schemes	SignGen (ms)	SigVeri(ms)	CommCost (bits)	Security (Yes/NO)	Formal proof (ROM = 0, SM = 1)	Security hardness (BP = 0, ECC = 1)	$(WS_{\mathcal{N}_d})_a$
Karati et al. [29]	0.149442539	0.04464	0.059178744	0.2	0	0	0.453261283
Y. Zhang et al. [31]	0	0	0.059178744	0.2	0	0	0.259178744
Xiong et al. [33]	0	0	0	0	0.15	0.45	0.6
Rezaeibagha et al. [34]	0.012221269	0.07988	0.059178744	0.2	0	0	0.351280013

- The recommended solutions are discussed and improved. Some shortcomings are found in the recommended solutions; therefore, these solutions should be discussed, studied, and improved.
- The certificateless cryptography suffers from the distribution of partial keys i.e., the delivery of partial keys requires a secure channel between KGC and the participating users [88,89]. Therefore, a novel certificateless signature approach, which does not require any secure channel for the distribution of partial private keys among the entities, need to be constructed.
- A new approach based on Hyperelliptic Curve Cryptosystem(HCC) need to be constructed with the assumption of Hyperelliptic Curve Discrete Logarithm Problem (HCDLP). The HDLP must be considered for constructing a secure certificateless signature scheme for IIoT due to its small key size and compact security.

9. Conclusion

Security threats are increasing daily with the prevalent use of IIoT technology. Researching an efficient security solution that can

Table 19
Performance analysis of the suggested schemes.

Schemes	$\left(WS_{\mathcal{P}_d}\right)_a$	$\left(WS_{\mathcal{N}_d}\right)_a$	$\mathcal{N}\left(WS_{\mathcal{P}_d}\right)_a$	$\mathcal{N}\left(WS_{\mathcal{N}_d}\right)_a$	Δ	Rank
Karati et al. [29]	0.2	0.453261283	0.200511876	0.244564529	0.222538202	4
Y. Zhang et al. [31]	0.266272884	0.259178744	0.266954377	0.568035427	0.417494902	2
Xiong et al. [33]	0.997447156	0.6	1	0	0.5	1
Rezaeibagha et al. [34]	0.2	0.351280013	0.200511876	0.414533311	0.307522593	3

help prevent malicious attacks is necessary despite the existence of multiple security solutions. The current study will help the research community understand the security flaws and causes by classifying and comparing the different certificateless signature schemes of the IIoT domain. This survey aims to investigate the security issues faced by the IIoT paradigm and provide a comparative analysis of the available solutions to improve security. The MCDM approach is used for the comparative analysis of the existing certificateless signature schemes by employing the EDAS technique to evaluate the previously suggested solution proposed for IIoT. The authors believe that the proposed technique has never been previously used for any cryptographic solutions. Finally, the study also addresses some of the public research issues for technologists, academia, and researchers to develop the security aspects of IIoT.

CRediT authorship contribution statement

Saddam Hussain: Conceptualization, Project administration, Validation, Writing, Methodology, Data curation, Formal analysis, Writing – review & editing. **Syed Sajid Ullah:** Data curation, Visualization, Writing, Writing – review & editing. **Ihsan Ali:** Writing, Formal analysis, Visualization, Writing – review & editing, Validation. **Jiafeng Xie:** Writing – review & editing, Supervision. **Venkata N. Inukollu:** Data curation, Methodology, Writing – review & editing, Validation.

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.

Acknowledgments

This research work was supported by the Faculty of Computer Science and Information Technology, University of Malaya, under Postgraduate Research Grant PG035-2016A.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of things: A survey on enabling technologies, protocols, and applications, IEEE Commun. Surv. Tutor. 17 (4) (2015) 2347–2376.

[2] T. Qiu, J. Chi, X. Zhou, Z. Ning, M. Atiquzzaman, D.O. Wu, Edge computing in industrial internet of things: Architecture, advances and challenges, IEEE Commun. Surv. Tutor. 22 (4) (2020) 2462–2488.

[3] L.D. Xu, W. He, S. Li, Internet of things in industries: A survey, IEEE Trans. Ind. Inform. 10 (4) (2014) 2233–2243.

[4] M. Wollschlaeger, T. Sauter, J. Jasperneite, The future of industrial comm.: Automation networks in the era of the IoT and industry 4.0, IEEE Ind. Elec. Mag. 11 (1) (2017) 17–27.

[5] P. Jayalaxmi, R. Saha, G. Kumar, N. Kumar, T.H. Kim, A taxonomy of security issues in industrial internet-of-things: Scoping review for existing solutions, future implications, and research challenges, IEEE Access 9 (2021) 25344–25359.

[6] G. George, S.M. Thampi, A graph-based security framework for securing industrial IoT networks from vulnerability exploitations, IEEE Access 6 (2018) 43586–43601.

[7] A.-R. Sadeghi, C. Wachsmann, M. Waidner, Security and privacy challenges in industrial Internet of Things, in: Proc. 52nd Annu. Design Autom. Conf. San Francisco, CA, USA, Jun. 2015, 1–6.

[8] J. Wurm, K. Hoang, O. Arias, et al., Security analysis on consumer and industrial iot devices, in: ASP-DAC, 2016, pp. 519–524.

[9] Sadeghi, C. Wachsmann, M. Waidner, Security and privacy challenges in IIoT, in: ACM/EDAC/IEEE DAC, 2015.

[10] E. Sisinni, A. Saifullah, S. Han, et al., Industrial internet of things: Challenges, opportunities, and directions, IEEE Trans. Ind. Inf. 14 (11) (2018) 4724–4734.

[11] W. Atamli, A. Martin, Threat-based security analysis for the internet of things, in: International Workshop on Secure Internet of Things (SIoT), IEEE, 2014, p. 3543.

[12] G.K. Verma, B.B. Singh, N. Kumar, V. Chamola, CB-CAS: Certificate-based efficient signature scheme with compact aggregation for industrial Internet of Things environment, IEEE Internet Things J. 7 (4) (2019) 2563–2572.

[13] M.E. Hellman, An overview of public key cryptography, IEEE Commun. Mag. 40 (5) (2002) 42–49.

[14] A. Roy, S. Karforma, A survey on digital signatures and its applications, J. Comput. Inform. Technol. 3 (1) (2012) 45–69.

[15] W. Diffie, M. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory 22 (6) (1976) 644–654.

[16] A. Shamir, Identity-based cryptosystems and signature schemes, in: Workshop on the Theory and Application of Cryptographic Techniques, Springer, Berlin, Heidelberg, 1984, pp. 47–53.

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

[18] Nils Gura, Arun Patel, Arvinderpal Wander, Hans Eberle, Sheueling Chang Shantz, Comparing elliptic curve cryptography and RSA on 8-bit CPUs, in: International Workshop on Cryptographic Hardware and Embedded Systems, Springer, Berlin, Heidelberg, 2004, pp. 119–132.

[19] C. Tamizhselvan, V. Vijayalakshmi, An energy efficient secure distributed naming service for IoT, Int. J. Adv. Stud. Sci. Res. (2019) 3.

[20] V. Naresh, R. Sivaranjani, N.V.E.S Murthy, Provable secure lightweight hyper elliptic curve-based communication system for wireless sensor networks, Int. J. Commun. Syst. 31 (2018) e3763.

[21] Hermann Kopetz, Internet of things, in: Real-Time Systems, Springer, Boston, MA, 2011, pp. 307–323.

[22] Dimitrios Serpanos, Marilyn Wolf, Industrial internet of things, in: Internet-of-Things (IoT) Systems, Springer, Cham, 2018, pp. 37–54.

[23] J. Tervonen, V. Isoherranen, M. Heikkilä, A review of the cognitive capabilities and data analysis issues of the future industrial internet-of-things, in: 2015 6th IEEE International Conference on Cognitive Infocommunications (CogInfoCom), IEEE, 2015, pp. 127–132.

[24] Mohammad Aazam, Sherali Zeadally, Khaled A. Harras, Deploying fog computing in industrial internet of things and industry 4.0, IEEE Trans. Ind. Inf. 14 (10) (2018) 4674–4682.

[25] M. Guizani, The industrial internet of things, IEEE Netw. 33 (5) (2019) 4, http://dx.doi.org/10.1109/MNET.2019.8863716.

[26] X. Yu, H. Guo, A Survey on IIoT Security, in: IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS), Singapore, 2019, (2019) pp. 1–5.

[27] K. Seyhan, T.N. Nguyen, S. Akleylek, K. Cengiz, S.H. Islam, Bi-GISIS KE: Modified key exchange protocol with reusable keys for IoT security, J. Inform. Secur. Appl. 58 (2021) 102788.

[28] T.N. Nguyen, B.H. Liu, N.P. Nguyen, J.T. Chou, Cyber security of smart grid: Attacks and defenses, in: ICC 2020-2020 IEEE International Conference on Communications (ICC), IEEE, 2020, pp. 1–6.

[29] Arijit Karati, S.K. Hafizul Islam, Marimuthu Karuppiah, Provably secure and lightweight certificateless signature scheme for IIoT environments, IEEE Trans. Ind. Inf. 14 (8) (2018) 3701–3711.

[30] B. Zhang, T. Zhu, C. Hu, C. Zhao, Cryptanalysis of a lightweight certificateless signature scheme for IIOT environments, IEEE Access 6 (2018) 73885–73894.

[31] Y. Zhang, R.H. Deng, D. Zheng, J. Li, P. Wu, Cao, J efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial, IoT IEEE Trans. Indust. Inform. 15 (9) (2019) 5099–5108.

[32] W. Yang, S. Wang, X. Huang, Y. Mu, On the security of an efficient and robust certificateless signature scheme for iiot environments, IEEE Access 7 (2019) 91074–91079.

[33] H. Xiong, Q. Mei, Y. Zhao, Efficient and provably secure certificateless parallel key-insulated signature without pairing for IIoT environments, IEEE Syst. J. (2019).

[34] F. Rezaeibagha, Y. Mu, X. Huang, W. Yang, K. Huang, Fully secure lightweight certificateless signature scheme for IIoT, IEEE Access 7 (2019) 144433–144443.

[35] C. Perera, C.H. Liu, S. Jayawardena, The emerging internet of things marketplace from an industrial perspective: a survey, IEEE Trans. Emerg. Top. Comput. 3 (4) (2015) 585–598.

[36] S. Mumtaz, A. Alsohaily, Z. Pang, A. Rayes, K.F. Tsang, J. Rodriguez, Massive internet of things for industrial applications: addressing wireless IIoT connectivity challenges and ecosystem fragmentation, IEEE Ind. Electron. Mag. 11 (1) (2017) 28–33.

[37] C. Zhu, J.J.P.C Rodrigues, V.C.M. Leung, L. Shu, L.T. Yang, Trust-based communication for the industrial internet of things, IEEE Commun. Mag. 56 (2) (2018) 16–22.

[38] Y. Liao, E. de Freitas Rocha Loures, F. Deschamps, Industrial internet of things: a systematic literature review and insights, IEEE Internet Things J. 5 (6) (2018) 4515–4525.

[39] N.B. Long, H. Tran-Dang, D. Kim, Energy-aware real-time routing for large-scale industrial internet of things, IEEE Internet Things J. 5 (3) (2018) 2190–2199, http://dx.doi.org/10.1109/JIOT.2018.2827050.

[40] H. Xu, W. Yu, D. Griffith, N. Golmie, A survey on industrial internet of things: a cyber–physical systems perspective, IEEE Access 6 (2018) 78238–78259, http://dx.doi.org/10.1109/ACCESS.2018.2884906.

[41] K. Al-Gumaei, K. Schuba, A. Friesen, S. Heymann, C. Pieper, F. Pethig, et al., A survey of internet of things and big data integrated solutions for industrie 4.0, in: 2018 & Nbsp; IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA), 1, IEEE, 2018, pp. 1417–1424.

[42] H. Boyes, B. Hallaq, J. Cunningham, T. Watson, The industrial internet of things (IIoT): An analysis framework, Comput. Ind. 101 (2018) 1–12.

[43] V. Alcácer, V. Cruz-Machado, Scanning the industry 4.0: A literature review on technologies for manufacturing systems, Eng. Sci. Technol. Int. J. 22 (3) (2019) 899–919.

[44] E. Oztemel, S. Gursev, Literature review of industry 4.0 and related technologies, J. Intell. Manuf. 31 (1) (2020) 127–182, http://dx.doi.org/10.1007/s10845-018-1433-8.

[45] Wazir Zada Khan, M.H. Rehman, Hussein Mohammed Zangoti, Muhammad Khalil Afzal, Nasrullah Armi, Khaled Salah, Industrial internet of things: Recent advances, enabling technologies and open challenges, Comput. Electr. Eng. 81 (2020) 106522.

[46] H. Al Housani, Joonsang Baek, Chan Yeob Yeun, Survey on certificateless public key cryptography, in: 2011 International Conference for Internet Technology and Secured Transactions, 2011, pp. 53–58.

[47] Y.C. Chen, R. Tso, A survey on security of certificateless signature schemes, IETE Tech. Rev. 33 (2) (2016) 115–121.

[48] M. Mikhail, Y. Abouelseoud, G. Elkobrosy, Extension and application of El-Gamal Encryption Scheme, 2014.

[49] X. Huang, W. Susilo, Y. Mu, F. Zhang, On the security of certificateless signature schemes from asiacrypt 2003, in: CANS 2005, LNCS, vol. 3810, SpringerVerlag, 2005, pp. 13–25.

[50] K.Y. Choi, J.H. Park, J.Y. Hwang, D.H. Lee, Efficient certificateless signature schemes, in: International Conference on Applied Cryptography and Network Security, Springer, Berlin, Heidelberg, 2007, pp. 443–458.

[51] S. Hussain, S.S. Ullah, A. Gumaei, M. Al-Rakhami, I. Ahmad, S.M. Arif, A novel efficient certificateless signature scheme for the prevention of content poisoning attack in named data networking-based internet of things, IEEE Access 9 (2021) 40198–40215.

[52] S. Al-Riyami, K. Paterson, Certificateless public key cryptography, in: Asiacrypt 2003, LNCS, vol. 2894, Springer-Verlag, 2003, pp. 452–473.

[53] Z. Zhang, D.S. Wong, J. Xu, D. Feng, Certificateless public-key signature: security model and efficient construction, in: International Conference on Applied Cryptography and Network Security, Springer, Berlin, Heidelberg, 2006, pp. 293–308.

[54] Jitendra Singh Chauhan, S.K. Sharma, A comparative study of cryptographic algorithms, Int. J. Innov. Res. (2015) 24–28.

[55] A. Al Hasib, A.A.M.M Haque, A comparative study of the performance and security issues of AES and RSA cryptography, in: Proc. - 3rd Int. Conf. Converg. Hybrid Inf. Technol. ICCIT 2008, 2, (2001) (2008) pp. 505–510.

[56] C. Narasimham, J. Pradhan, Evaluation of performance characteristics of cryptosystem using text files., J. Theor. Appl. Inf. Technol. 4 (1) (2008).

[57] A. Naureen, A. Akram, T. Maqsood, R. Riaz, K.H. Kim, H.F. Ahmed, Performance and security assessment of a PKC based key management scheme for hierarchical sensor networks, IEEE Veh. Technol. Conf. (2008) 163–167.

[58] S. Farah, M.Y. Javed, A. Shamim, T. Nawaz, An experimental study on performance evaluation of asymmetric encryption algorithms, Recent Advaces Inf. Sci. 8 (2012) 121–124.

[59] R. Tripathi, S. Agrawal, Comparative study of symmetric and asymmetric cryptography techniques, Int. J. Adv. Found. Res. Comput. 1 (6) (2014) 68–76.

[60] B. Padmavathi, S.R. Kumari, A survey on performance analysis of DES, AES and RSA algorithm along with LSB substitution technique, Int. J. Sci. Res. 2 (4) (2013) 170–174.

[61] C. Gentry, Certificate-based encryption and the certificate revocation problem, in: International Conference on the Theory and Applications of Cryptographic Techniques, Springer, Berlin, Heidelberg, 2003, pp. 272–293.

[62] Y.C. Chen, R. Tso, W. Susilo, X. Huang, G. Horng, Certificateless signatures: Structural extensions of security models and new provably secure schemes, IACR Cryptol. EPrint Arch. 2013 (193) (2013).

[63] Kyung-Ah Shim, Security vulnerabilities of four signature schemes from NTRU lattices and pairings, IEEE Access (2020).

[64] A. Muhammad, N.U. Amin, I. Ullah, A. Alsanad, S. Hussain, S. Al-Hadhrami, M.I. Uddin, H. Khattak, M.A. Khan, An efficient scheme for industrial internet of things using certificateless signature, Math. Probl. Eng. (2021) (2021).

[65] S.S. Ullah, et al., A lightweight identity-based signature scheme for mitigation of content poisoning attack in named data networking with internet of things, IEEE Access 8 (2020) 98910–98928, http://dx.doi.org/10.1109/ACCESS.2020.2995080.

[66] E. Ahene, Z. Qin, A.K. Adusei, F. Li, Efficient signcryption with proxy re-encryption and its application in smart grid, IEEE Internet Things J. 6 (6) (2019) 9722–9737.

[67] E. Ahene, J. Dai, H. Feng, F. Li, A certificateless signcryption with proxy re-encryption for practical access control in cloud-based reliable smart grid, Telecommun. Syst. 70 (4) (2019) 491–510.

[68] X. Cao, W. Kou, X. Du, A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges, Inform. Sci. 180 (15) (2010) 28952903.

[69] Abdul Waheed, Arif Iqbal Umar, Mahdi Zareei, Nizamud Din, Noor Ul Amin, Jawaid Iqbal, Yousaf Saeed, Ehab Mahmoud Mohamed, Cryptanalysis and improvement of a proxy signcryption scheme in the standard computational model, IEEE Access 8 (2020) 131188–131201.

[70] Jianying Qiu, Kai Fan, Kuan Zhang, Qiang Pan, Hui Li, Yintang Yang, An efficient multi-message and multi-receiver signcryption scheme for heterogeneous smart mobile IoT, IEEE Access 7 (2019) 180205-180217.

[71] Cong Peng, Jianhua Chen, Mohammad S. Obaidat, Pandi Vijayakumar, Debiao He, Efficient and provably secure multireceiver signcryption scheme for multicast communication in edge computing, IEEE Internet Things J. 7 (7) (2019) 6056–6068.

[72] I. Ullah, N.U. Amin, M. Naeem, H. Khattak, S.J. Khattak, H. Ali, A novel provable secured signcryption scheme????: A hyper-elliptic curve-based approach, Mathematics 7 (8) (2019) 686.

[73] I. Ullah, A. Alomari, N. Ul Amin, M.A. Khan, H. Khattak, An energy efficient and formally secured certificate-based signcryption for Wireless Body Area networks with the internet of things, Electronics 8 (10) (2019) 1171.

[74] M.A. Khan, I.M. Qureshi, I. Ullah, S. Khan, F. Khanzada, F. Noor, An efficient and provably secure certificateless blind signature scheme for flying ad-hoc network based on multi-access edge computing, Electronics 9 (1) (2020) 30.

[75] Arijit Karati, G.P. Biswas, Provably secure and authenticated data sharing protocol for IoT-based crowdsensing network, Trans. Emerg. Telecommun. Technol. 30 (4) (2019) e3315.

[76] Arijit Karati, Chun-I. Fan, Ruei-Hau Hsu, Provably secure and generalized signcryption with public verifiability for secure data transmission between resource-constrained IoT devices, IEEE Internet Things J. 6 (6) (2019) 10431–10440.

[77] Arijit Karati, S.K. Hafizul Islam, Marimuthu Karuppiah, Provably secure and lightweight certificateless signature scheme for IIoT environments, IEEE Trans. Ind. Inf. 14 (8) (2018) 3701–3711.

[78] M. Keshavarz Ghorabaee, E.K. Zavadskas, L. Olfat, Z. Turskis, Multi-criteria inventory classification using a new method of evaluation based on distance from average solution (EDAS), Informatica 26 (3) (2015) 435–451.

[79] K. Keshavarz Ghorabaee, E.K. Zavadskas, M. Amiri, Z. Turskis, Extended EDAS method for fuzzy multi-criteria decision-making: an application to supplier selection, Int. J. Comput. Commun. Control 11 (3) (2016) 358–371.

[80] Lotfi A. Zadeh, A fuzzy logic, Computer 21 (4) (1988) 83–93.

[81] K. Tanaka, An introduction to fuzzy logic for practical applications, 1997.

[82] N.A. Malik, M. Rai, Enhanced secure and efficient key management algorithm and fuzzy with trust management for MANETs, in: Proc. Int. Conf. Innov. Comput. Commun. (ICICC), 2020.

[83] G. Mehmood, M.Z. Khan, A. Waheed, M. Zareei, E.M. Mohamed, A trust-based energy-efficient and reliable communication scheme (trust-based ERCS) for remote patient monitoring in wireless body area networks, IEEE Access 8 (2020) 131397–131413.

[84] D. Zindani, S.R. Maity, S. Bhowmik, Fuzzy-EDAS (evaluation based on distance from average solution) for material selection problems, in: Advances in Computational Methods in Manufacturing, Springer, Singapore, 2019, pp. 755–771.

[85] Morteza Yazdani, Ali Ebadi Torkayesh, Ernesto D.R. Santibanez-Gonzalez, Sina Khanmohammadi Otaghsara, Evaluation of renewable energy resources using integrated Shannon entropy–EDAS model, Sustain. Oper. Comput. (2020).

[86] C.H. Nguyen, T.L. Pham, T.N. Nguyen, C.H. Ho, T.A. Nguyen, The linguistic summarization and the interpretability, scalability of fuzzy representations of multilevel semantic structures of word-domains, Microprocess. Microsyst. 81 (2021) 103641.

[87] S.K. Dwivedi, P. Roy, C. Karda, S. Agrawal, R. Amin, Blockchain-based internet of things and industrial IoT: A comprehensive survey, Secur. Commun. Netw. (2021) 21, http://dx.doi.org/10.1155/2021/7142048, Article ID 7142048.

[88] Y. Lu, J. Li, Provably secure certificate-based signcryption scheme without pairings, KSII Trans. Internet Inf. Syst. 8 (7) (2014) 2554–2571.

[89] Y. Lu, J. Li, A pairing-free certificate-based proxy re-encryption scheme for secure data sharing in public clouds, Futur. Gener. Comput. Syst. 62 (2016) 140–147.