International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys.13, No.1 (Apr-23)

http://dx.doi.org/10.12785/ijcds/130178

A Comprehensive Analysis of Signature Schemes: Towards Pairing and Non-pairing, Taxonomy and Future Scopes

Pairing & Non-pairing Security

Rajkumar Gaur[1] **and Shiva Prakash**[2]

[1]*Department of ITCA, MMMUT, Gorakhpur, India*
[2]*Department of ITCA, MMMUT, Gorakhpur, India*

Received 25 Jun. 2022, Revised 22 Dec. 2022, Accepted 6 Feb. 2023, Published 16 Apr. 2023

Abstract: The notion of a ”Signature scheme” carries possibilities to solve the message and key security problems. A signature scheme aims to secure the channels, IoT nodes, and Blockchain to use public resources and provide high-quality services. The Information and communication system acquires a prominent role in IoT and Blockchain applications. These signature schemes provide trust-free transparency, pseudo-anonymity, equality, motorization, decentralization, and protection. The article contributes a pervasive analysis of the literature pairing, and the non-pairing scheme provides high Security, cost-effectiveness, high service, and several keys for lightweight components. Our proposed approach analyzes the security schemes and differentiates the different security levels. The schemes introduced research contribution and research motivation. Finally, the article presents a well-organized fundamental for future work, segregation analysis of security models and schemes. This article benefits the new researcher with detailed information about signatures and critical security analysis.

Keywords: Sign, pairing, non-pairing, schemes, cryptosystem, digital signature

1. INTRODUCTION

In the digital system, device-to-device interaction and data transfer from different applications. The communication system used various techniques to reduce costs, time, resources, and human work. However, many intelligent computing systems share information; some information is more critical, and some are sensitive, like government organizations, Banking systems, and defense. So, to secure the data, the cryptography base security methodology is used to prevent the attack and connect the information shared devices. The primary security services are Identity, Authentication, and non-repudiation. The pairing and non-pairing base techniques of the cryptosystem provide Security in IoT and Blockchain applications. This paper discusses the various pairing, non-pairing-based signature schemes, and multi-signature schemes. Some security schemes are based on ECC, called the lightweight protocol [1], [2], [3], [4]. These security protocols address the multiple issues of IoT and Blockchain. The IoT and Blockchain applications have a massive amount of information to deploy in edge devices for data processing. Electronic devices require data processing techniques in a large-scale and efficient way. The pairing-based security techniques slow in computation than the non-pairing-based techniques, but the security level is very high. The security mechanism of application devices requires Authentication and Identity to prevent attacks. The other issues are resource constraints, and interoperability [5], [6], [7]. The limited resources of IoT and Blockchain devices have fewer process computations. These fundamental issues as data transformation and architecture. The emerging paradigm of security systems requires the secure architecture of IoT and Blockchain applications. These are based on cloud, Fog, and Edge computing. This computing platform provides fast data access, less response time, and efficiency for data execution [5]. For the above issues and challenges, the proposed techniques for analyzing the articles are based on the security algorithms and verification techniques to verify the various schemes[8], [9]. This paper provides a comprehensive study of Identity-based signature schemes and presents the techniques to analyze systems with future work. The taxonomy of signature schemes used in IoT-assisted cloud environments is devised from different perspectives: device interoperability, secure network, syntactical methods for IoT and Blockchain, semantic systems, and platform interoperability. Furthermore, based on the provided taxonomy, review the primary ID-Based scheme security techniques and solutions to address different attacks. The survey ends by providing some open research

E-mail address: rajkumargaur@gmail.com, spitca@mmmut.ac.in

challenges. This review enables domain professionals and experts to identify the different approaches for enhancing IoT security to increase the number of IoT Nodes protections [10], [11], [12], [8], [9].
Next, specify the main contributions of a paper based on the proposed design for signature analysis. Some proposals aim for throughput refinement, runtime signature reduction, or signature verification reduction. Another aim is to reduce different domains or memory usage—some attempt to enhance security or reduce the amount of data communicated. By identifying a "main" objective, do not say that a work manages the different goals but take additional steps to enhance a distinctive characteristic.

- **Security:** To select a high-level security setting and then domain from it to construct the lightweight solution. Mitigating an extensive range of attacks and enhancing the security features of the system furthermore fall in this classification. Some of the reanalyzed works measure the security of their proposals based on the number of attacks resisted. Other procedures may consider connecting this with the key size used in applications.

- **Performance:** To reduce the signature generation and verification process or the computation of the schemes. This usually contains faster algorithms, a reduced number of procedures, and a reduced number of degrees, among different schemes. This feature is commonly associated with metrics such as key setup, key generation, sign generation, and verification in runtime applications. The implementation medium specifies essential attributes, such as sign generation and verification, which affects the systems in runtime applications. A more technologically autonomous measure is signature length, which is the necessary number of computations to perform a task. The signature performance, however, depends on the execution approach for the algorithm.

- **Hardware resources:** In the case of hardware, to decrease the memory appearance of a software performance or segment estimate. This category typically includes the use of smaller fields, a reduction in the range of operations, and circuit design optimization for hardware implementations.

Our Contribution The following are the paper's significant contributions based on the primary observations:

- The existing approach addresses the corresponding articles with flaws in the suggested Authentication.

- The multiple security preservation models were examined, including various device attacks, anonymity, certificate-based Authentication, Mutual Authentication, and eavesdropping.

- Next, categorize privacy-preserving and security models for IoT-assisted cloud environments into different categories: Node Authentication, conditional, user's Identity, and location-based privacy.

- And highlight the future research challenges, discussion of the scheme, and likely future research trends in Security and privacy for IoT-assisted cloud-based applications.

The rest of the paper coordinates as succeeds in Section 2 as Background of signatures schemes. Section 3, related work of the various encryption schemes based on different methods and signatures discussed in Section 4, analyzes signatures on other cryptology-based systems and processes. Section 5, key management, uses fundamental aggregations to make one key, and Section describes multiple threshold schemes for security increase. Section 6 consists of a mixed bilinear pairing scheme, threshold signature scheme, and mixed cryptography technique. Section 7, related research methods, compares the protocol descriptions, assumptions, and efficiency and concludes in Section 8.

2. BACKGROUND

This section briefly explains basic signature scheme types and some cryptography operations used in IoT environments.

A. ID-Based Encryption

In simpler terms, encryption uses readable data and modifies it to perform unusual data. Encryption difficulties accept a cryptographic technique, so some rules of analytical value that both the correspondent and the beneficiary of an encrypted message agree on some conditions to convert to the original data [13].

B. ID-Based Decryption

Decryption is a systematic technique that extracts and converts the cipher data into an easily understandable system or human-readable form. Decryption automatically through the system. Therefore, it may be achieved with codes or identification values [23].

C. ID-Based Signature

A signature is a mark that identifies a performer for authentic documents or programs. In cryptography systems, signatures of various types, such as:

1) Blind Signature: A blind signature is a sign that the singer does not recognize or acquire the message. Then the signature message is unblinded, and this time the news is publicly checked by public key with the original message. The blind signature used a public-key encryption scheme [8], [12], [14]. A blind Signature Scheme approved by someone to receive notifications signed by other parties without inadequate notice concerning the information on a different personality. The ID-Based Blind signature schemes realize a significant use agreement in applications where sender privacy is essential. This

type of scheme is helpful for the secrecy needed, for example, election systems (e-Vote), Digital cash schemes (e-Cash), e-Hospital, etc.

2) Short Signature: In cases where time and communication are limited, these signatures require a limited period. For Example, fewer signatures are necessary if a person requests that the signature be entered manually [15].
3) Aggregate Signature: Let U_i be the collection of users, and n is considered U_i = 1,2,..... n. for every user i, the U_i has two keys as public and secret, the key pair as $(PubK_i; SerK_i)$. Let i^{th} users sign a message (mi) and produce sign σ_i. An aggregation algorithm as public and output is compressed small signature σ with inputs of σ_1, σ_2, ...σ_n: This scheme of n signatures aggregated through anyone. Therefore, an aggregate verifies algorithm takes values as $(PubK_1), (PubK_2), ...(PubK_n)$, messages as $m_1, m_2.....m_n$; and Sign σ as input determines the aggregate sign (σ) are authentic. Therefore, the aggregate schemes utilized in BGP to reduce the number of signs for separate information [9], [12], [15], [16], [17].
4) Proxy Signature: This signature scheme allows inventive signers to commit their signing ability to another party called the proxy signer. This sign is beneficial in various applications. It is useful when the initial signer cannot sign the document(s) [18]. These signatures have many practical applications, particularly in distributed, collective object, and mobile interactions.
5) Group Signature: In this signature scheme, different users sign a part of the information on the portion of the group. In this scheme, several verifiers know a message signed by a group member, not a particular signer in the scenario. These signature schemes applications in distinct areas like e-cash, e-voting, bidding, etc.
6) Multi-signature: This scheme enables the small subgroup of users to simultaneously sign a message such that a confirmation to participate each member in signing a subset. The multi-signature system aims to prove each member can sign messages in a subgroup, and the subgroup size is arbitrary. The verifier denies the signature because it does not satisfy the conditions. This signature applies to efficiently attest the same message's signature under various public keys [17], [18], [19].
7) Threshold Signature: In this signature scheme, various parties, with a determined number of signers, encrypt the message with a public key and an identical secret key specified by parties. Then (t; n) as the threshold sign, the sequence of members with the minor number t from an aggregate of n members requires generating a signature, and t shows the threshold number.

D. Bilinear pairings

This scheme is the pairing between many groups or a minimum of two groups with prime order. This signature scheme constructs from the Tate pairing especially selected by elliptic curves [8], [16].

E. Key Agreement

When two or more participants want to share a message securely, the key agreement conditions require this situation. The various parties share a secret key to communicate with each other in the system. This first exchange of the encryption key is called the key exchange. In this situation, the parties securely share a piece of information with everyone. An opponent does not possess admittance to the secret key capable of decrypting the data.

F. Multifarious Schemes

1) The Signcryption: This technique processes a method that implements confidential and authentic transmission of communication between two multitudes. This approach is more helpful to an encryption scheme's sinister organization through a sign method. This scheme merges the function of signing and encryption techniques. The signcryption scheme's strategy is to achieve deciphering and logical round in signature to accept cryptography properties.
2) Identification: This scheme is another model cryptography mechanism where the prover P correlates with the verifier V to assure its integrity. The prover P identifies a certain content agreeing with the public and that a specific range authorizes to establish V of his innocence.

   Discussing schemes and attacks by various papers and distinct cryptosystem primitives contains merely those methods that include assurance evidence of the current adversarial models. The bilinear pairing-based procedure is a unique accumulation of surviving literature on pairing-based cryptosystems. The scheme does not explore a mathematical method for estimating pairing algorithms.

3. Related Work

Shamir presented the first ID-Based scheme in 1984; the central concept of this scheme is critical key management, except for certificate-based shared keys. These public aims to set the process and design the first ID Based scheme [1, 2]. The article follows the ID-Based scheme survey [7] from 2000 to 2003 and 2007 to 2011 [1]. In this Design, the user identity technique uses a public entrance and is concerned with the private key. The certificate authenticity does not extract the public key in the ID-based cryptosystem. In this concept, users create public access without the involvement of a certificate authority (CA). As a result, an ID-based system avoids the use of certificates. However, Id-based systems have more issues [2], [20]. Authors and researchers offer a variety of solutions for ID-based encryption systems. The scheme [21] presented the Weil pairing and the bilinear

pairing proposed by Sakai et al. [3] as the first practical and completely ID-based system as a pairing base. Another technique and the altered assumption are Ref [10], as Gap Diffie Hellman group [4]. Chaum [11] proposed the blind signature in 1982, and Rivest et al. [12] 2001 proposed the ring-based signature system. The scheme [10], [11] created the group signature method and the ring and blind signatures presented by Chaum and Van Heijst [13], while Zhang and Kim only dealt with key management difficulties in 1991. Popescu introduced the group signature based on the Identity and raised and constructed a bilinear pairing over the elliptic curve in 2002 [21], [22]. The threshold signature scheme was prepared by Desmedt [22]. In this scheme, if any group member cannot join, the group condition is fixed to the number of members. Beak and Zheng [23] introduced the concept and designed an identity-based threshold signature without a distributed public key generator [24]. In a different situation, the additional key present in the security system, another type of signature as a proxy base signature scheme introduced the Mambo et al. [23] in 1996, at the same scheme introduced by Zhang and Kim in 2003 [2], [23]. Therefore, the signature schemes require public confirmation of their efficacy signature scheme. Therefore, this technique is known as an undeniable signature. The other types of signature schemes were introduced by Chaum, and Antwerpen [25] in 1990. After that, Han et al. [2] proposed this type of signature scheme. In other scenarios, the validity of the signature, then the preferred strong verify the signature, is formalized and secured. Several researchers proposed a signature (IN-SDVS) ID-based robust designated verification signature scheme in 2004 [26]. The secure ID-based signature partially blind scheme design by Chow et al. [12] in 2005 resolved the Diffie-Hellman compute hardness problem. The ID-based signature scheme has occurred strongly in the last many years. In 2007, Huet et al.; presented the partially Blind Signature scheme, but this scheme suffered an acute forgery attack. Various identities-based digital signatures and multi-signature schemes proposed by various researchers and authors offer the most acceptable methods. This paper has shown many public-private keys to respect signature schemes and many forms of attacks as proof of security systems. It explores signature-based schemes and how to protect messages and related keys such as the public or secret key. The ID-Based signature schemes survey covers from 2001 to 2020 maximum schemes and tries to determine different research issues and challenges. Therefore, explore the Blockchain Bitcoin security based on Identity-based methods from Mihir Bellare et al. in 2005 with Yunlei Zhao et al. in 2020. The essential varieties of encryption schemes are based on BLS and Schnorr signature schemes. These signature schemes provide Security for keys and messages with less computation cost and less memory and discuss the various attack techniques and their pros/cons. The other discussion respects schemes, key size, Security, protection of messages, and forgery attacks for their proof. Finally, try to determine our contribution to the research purpose and its challenges, applications, security

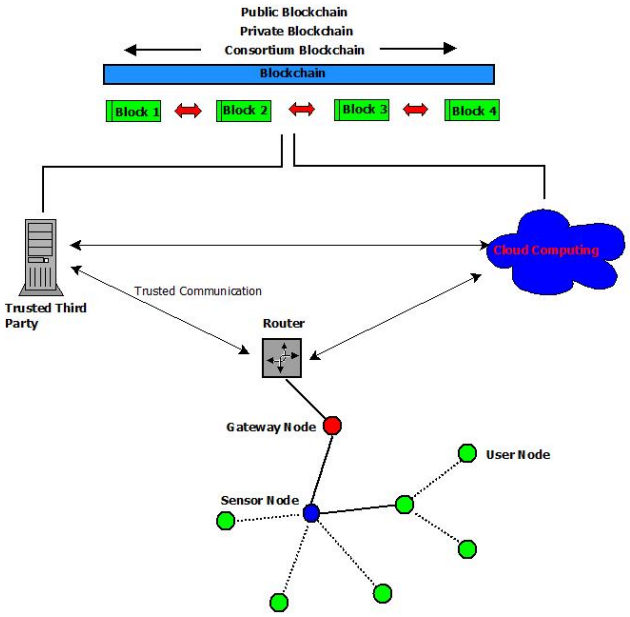

Figure 1. VHDL Synthesis Process

terms, and taxonomy of signatures schemes. After that, some basic cryptography primitives, encryption, decryption, signature, key management, and protocols are designed for identification and verification, signcryption, threshold sign scheme, key exchange, and hash functioning. The basic rules and security reviews of various identity-based signature schemes ensure their corresponding development from the beginning. Its benefits scholars and invigorate work in related domains with flow references. Therefore, this article uses some terms to continue to center on the essential terminologies for IoT and Blockchain, as shown in Figure 1. In Figure 1, the IoT application and Blockchain are connected insecurely by cloud computing and a trusted third party. There are three types: private, public, and consortium Blockchain. The block is connected in all Blockchain, and data transfer is rule-based. IoT network nodes are related to transmission one-to-one and too many. Thus, Security is required with various schemes and techniques to secure IoT and Blockchain with multiple methods such as ID-based, pairing, non-pairing, and based on DSA and multi signatures [27], [28].

A. *Signature Schemes*

This subsection concerns the various sign schemes. The schemes are based on pairing and non-pairing techniques. Signatures are belongings of human life, and it defines the responsible or authenticity of a person or document verifiable by third parties. The signature schemes are based on the analysis of signature assumptions, efficiency, possible attacks, and techniques discussed as follows: Signature schemes are the procedure of signing messages with algorithms with different keys as public and private keys. These types of methods are known as signature schemes [25]. This signature base on five tuples as $P_{mes}, A_{fps}, S_{fpk}, K_{ks}, V_{ver}$

- P_{mes} set of all possible finite message.
- A_{fps} set of all possible finite signature
- k_{ks} set of all possible key
- ∀ k some signature algorithms $SIG_{k_{ks}}$ send for verification V_{ver_r} in V_{ver}
  such that $SIG_{k_{ks}} : P_{mes} \rightarrow A_{fps}$
  $V_{ver_r} : P_{mes} \times A_{fps} \rightarrow \{true, false\}$
  $V_{ver_r}(x, y) = true$ iff $y = SIG_{k_{ks}}(x)$
- a pair of $(x, y) \in P_{mes} \times A_{fps}$ is called a signed message.

The various security requirements are violated because of the diverse attacks targeting IoT-assisted cloud environments, as depicted in Figure 2.

B. Extract of the literature

The existing works of the publications are committed to preserving the following shortcomings.

- Most of the existing works are either significant in exploitation or questioning, but not during the technique of allocating resources to secure systems in IoT.
- Most existing approaches fail to balance local and global Security during the nodes allocation approach of communication systems.
- The soundness and accuracy concerned during the procedure of node distribution in the existing secure schemes still maintain space for refinement.

4. ANALYSIS OF SECURITY SCHEMES

This section discusses the various security schemes and Encryption/decryption techniques for data. Encryption is a technique to encode messages or sensible data. So only certified parties can access it. Encryption does not prevent or stop any information from the attacks. Various encryption methods, analysis techniques, assumptions, efficiency, and aggression are used.
Scheme: ID-Based Authenticated Encryption with ID Confidentiality.
Security Analysis: The modern IBHigncryption method functions in bilinear symmetric Type 1 pairings scheme BFIBE [8], and the IBHigncryption method bilinear asymmetric Type 2 pairings in IEEE P1363.3 standard [16], which is shortly compiled in Table I
Strongness:

- When generating and saving parameters, the system decreases computational and space complexity.
- The attack vector (to recover the master secret key) decreased for maximum system utilization.
- Identity-based cryptosystems reduce deployment and adaptability and reduce the adaptability to handle identity-based cryptosystems when the IBHigncryption method deploys and the original public key is unchanged [15].

Explanation:
The authors introduced the primary identity-based signcryption (IBHigncryption) in 2020. The various exciting characteristics of IBHigncryption, among others, are its integrity and effectiveness. The high-level IBHigncryption method is helpful in the entire CCA-secure ID-Based encryption scheme [3] while concurrently proposing individual Authentication and self-hiding. Compared with the ID-Based signcryption process that appropriates the IEEE P1363.3 standard, the IBHigncryption method is essential and comfortable for meaningful performance improvement. Moreover, the IBHigncryption appreciates progressive identity privacy, receiver deniability, and protection. The presented IBHigncryption is a simplistic structure with fewer public parameters and does not contain the standard original shared key [15]. The scheme comparison with other schemes with different parameters is shown in Table I. Where indicates X as "unapplicable," "-" no exponentiation operation, "ME" as modular exponentiation, "PA" as a pairing, Hsf as a straightforward hashing, Hbg as a hashing on the bilinear group, "MA" as modular addition, "MM" as modular multiplication in G1 or G2 (resp., GT), "MI" as a modular inversion, and isomorphism. The especially partial IBHigncryption in-service stages prominently deliver the original public key, which provides various benefits.

Scheme: Efficient ID-Based Signature Scheme with Bilinear Map
*Security Analysis:*The author, R, Sahu et al. 2011 gave the schemes of ID-Based sign scheme based on the BP. This idea preserves the existential fraud on adaptively chosen messages and presents an ID attack under the ROM with com-DH assumption.
Strongness: The new method is manageable and computationally more helpful than other enduring schemes. Moreover, since the sections built for the proposed ID-based signature, the Boneh–Lynn–Shacham short signature, this scheme is more profitable and suitable for connections of signatures above small bandwidth channels [1], [30], [31].
Explanation: This scheme incorporates another scheme's computational performance with other ID-based signature techniques and proves that the method is comparably more valuable, as shown in Table II [36, 37]. In this table, various parameters are used: eb = number of bilinear maps, Hf = number of hash functions, Ep = number of exponentiations, and SM = number of scalar multiplications in G1.

Scheme: New Multi-SS and a General Forking Lemma
Security Analysis: Mihir Bellaire et al., in 2005 and 2006, analyzed the multi-Signature scheme. The comparability of MSDL and MS-DDH schemes' effectiveness toward the various IDB schemes against the IBMS-GR method.

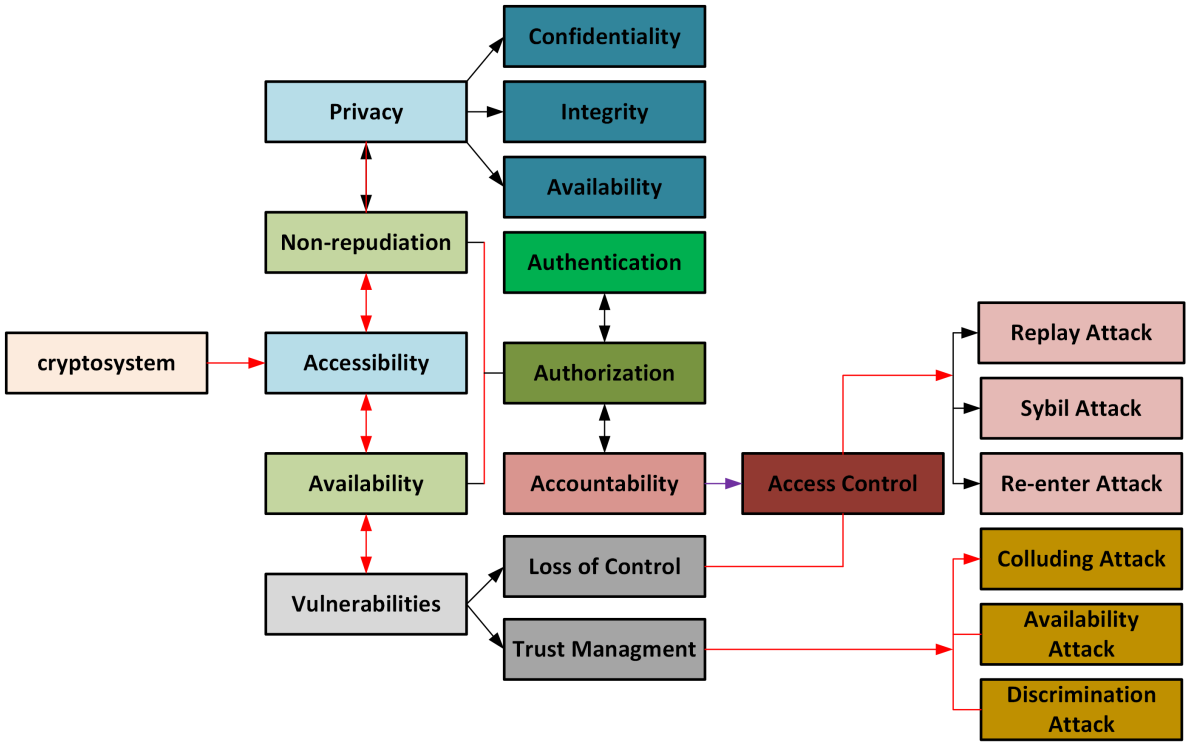

Figure 2. Security essentials services and various threats

Individual scenarios define the computation detriment of each signer sign and the computation cost of attestation of a multi-sign. The signature size is a system's appropriate signer's public key size. The system parameter sizes are inferior to all witnesses, key setup, attest Security, and each part of size in bits. The exp indicates the exponent form of the sign [36]. *Strongness:* The work is based on the DL approach over EC group 160-bits for RSA-based scheme, and work considers as modulo N and exponent e for sizes 1024 and 160 bits separately in Table III. *Explanation:* The same paper was solved in the practical form in 2006 by Mihir Bellare et al., as in [42], [43]. The other idea is a novel approach that approves protection in the truthfully public fundamental Design, and the applications require nothing more than every signer's public key. Moreover, critical generalization is essential direction performers are not at the expense of competence or promise. This scheme approach recognizes the signing period, verification period, and signature size to declare secure in the ROM under a usual hypothesis. The protection is based on the performance of a common Forking Lemmas.

scheme: A Multi-ps scheme with various proxy groups
Security Analysis: The author proposed the MPMS scheme in 2017 with multiple proxy groups. Besides, this scheme confirms the definitive proxy signature and a group of defined verifiers' accesses.
Strongness: It generates a safety model to prove that the novel one secure base on the CDH assumption. The new one is offered tight protection and better computational ability.
Explanation: Therefore, it is a significant problem that all original signers can choose their proxy group, which is dissimilar from others. However, some schemes analyze the property of this scheme and protect it [44].

Scheme: ID-Based Multi-PSscheme in SM
*Security Analysis:*The IBMPS structure based on the n + 1 signers (where n is no of the proxy participate signers) presents a specific security model for IBMPS. This scheme structure performs an ID-based multiproxy sign method in the approved model [45].
Strongness: The proposed method is securely related to other ID-based multi-proxy sign schemes. Therefore, the IBMPS scheme proves too safe in the SM. Since the suggested system is not efficient enough, the IBMPS still requires enhancing more.
Explanation: Ke GU Et Al. introduced a scheme in 2017 based on various ID-based multi-proxy sign methods [46]. However, the other techniques are based on ROM construction. Although, the existing security model for the ID-based multi-proxy sign is not entirely suitable for execution. Table IV comparisons of the schemes, key length, signature size, and delegation size (by [45], [46], [47]). In Table 4, the key length, model, and assumptions analyze three types of schemes with the author's system.
Table IV relates to [45], [46] based on ID cryptography and

TABLE I. Comparison of various schemes with key setup, key generation, and its assumptions.

		[3]	[15]	[29]
Parameter		(q, G1, GT, e, n, g, Ppub, h1, h2, h3, h4)	(q, G1, G2, GT, g1, g2, g, Qpub, e, ψ, h1, h2, h3)	(q, G1, GT, e, g, h)
Efficiency	Setup	1 E + 1 P + 1 ψ	1 E	-
	KeyGen	1 E + 1 INV + 1 H1 + 1 A	1 E + 1 H2	1 E + 1 H2
	Sender	4 E +2 ψ + 3 H1 + 1 M +1 A	2 E + 1 P + 1 H2 + 3 H1	2 E + 1 P + 2 H2 + 1 Enc
	Receiver	2 E + 2 P + 3 H1 + 1 MT +1 M+ 1 A	1 E + 1 P + 3 H1	1 E + 1 P + 1 H2 + 1 Dec
Space of Message		$\{0,1\}^*$	$\{0,1\}^1$	$\{0,1\}^1$
Privacy-ID		-	×	✓
x-security		-	×	✓
Receiver Deniability		-	×	✓
Assumption		BDH	q-BDHIP	Gap-SBDH
Model		ROM	ROM	ROM
Assumption		unforgeable	unforgeable	cold-boot attack

TABLE II. IDBS Scheme from Bilinear Maps signing phase as well as verification phase

Scheme	Signing-phase				Verify-Phase				Model
	eb	Hf	Ep	SM	eb	Hf	Ep	SM	
[30]	0	1	1	2	2	2	1	0	ROM
[32]	0	2	0	4	3	2	2	0	SM
[33]	1	1	1	2	2	1	1	0	ROM
[34]	0	1	0	3	2	1	0	1	SM
[35]	0	1	0	1	2	1	0	1	ROM

no need for vital public certificates. Therefore, this scheme has more advantages in simplifying essential supervision. Thus, this scheme creates a conventional model [52].
Where $|Z_q|$ show is the element in $Z_q|G_1|$ and shows the length of the component in G1. Therefore, the identification scheme is private, and the system [46] is in the usual Design, and the other two identity-based systems in the ROM [45].

Scheme: New Provably Secure ID-Based Multi-PSS
Security Analysis: The first scheme is based on the ROM, with the new Security, the system based on the CDH assumptions, and the following scheme description and protection model of an ID-Based Multiproxy signature design as identity-based Multiproxy signature scheme with the com-DHA's hardness [46].
Strongness: This scheme confirms the confidence in the ROM. Furthermore, correlated via previous ID-based Multiproxy sign schemes based on BP, the existing approach is provably protective and more productive [50].
Explanation: Qunshan Chen, 2019 formalizes a security model for the ID-Based Multiproxy sign and ID-Based Multiproxy sign system using BP. In Table V, Msc is the point scalar multiplication in G1, Ex is the exponentiation operation in G2, and Po is the [50] pairing method and ignores other actions hashing in all systems [45], [47], [51], [27], [28]. The method's explanation is more effective than the scheme in [51], which is undoubtedly secure. Moreover, this scheme is reliable under the co-DHA. Although the Design in [27] is more valuable than the proposed scheme, there is no actual security credential in the system, and the methods in need provable Security as well, as the technique is not secure in [45]. Hence, this ID-based multi-proxy sign scheme uses bilinear pairings that establish safety in the ROM [18].

Scheme: Okamoto beats schnorr, on the provable security of multi-signatures
Security Analysis: The M. Drijvers et al. experiment and explain the second generator in DG-CoSi hardly concerns the scalable associates with CoSi, which allows 8191 signers to collaborate a message in under 1.5 seconds and makes a convenient and provable safe preference for outsized deployments. The related first CoSi scheme and this new scheme yield a 32% improvement in CPU time and no recorded modification in sign latency. It also presents that DG-CoSi is approximately just as scalable as CoSi, a viable alternative for large-scale decentralized systems [44].
Strongness: The shared key, sign, and the aggregate shared key, where several "proof-of-possession" of the protected key is assumed to be part of the shared key.
Explanation: Table VI presents the effectiveness of the signature-based fundamental verifying model. In table form, the two to five-column computational performance of the algorithms counts the size of exponentiation pairings, where "G" indicates the exponentiation in the group G, and Gn

TABLE III. Multi Signature scheme and Security Model

Scheme	Sign	Verify	Keys	Assumption
[37]	1 exp	1 exp	Dedicated key-reg	DL
[38]	1 exp	2 exp	KOSK-model	co-CDH
[39]	3 exp	2 exp	KOSK-model	co-CDH
MS-DL-sch	1 exp	1 exp	Plain-pk-model	DL
MS-DDH-sch	1 exp	1 exp	Plain-pk-model	DDH
[40]	2 exp	3 exp	ID-based	co-CDH
IBMS-GQ [41]	1exp	1 exp	ID-based	RSA

TABLE IV. Various signature schemes with key size

Scheme	Pri_k length	Pub_k length	length of del	length of sig_n	Model	Asmpt
[45]	$\mid G_1 \mid$	–	$2.\mid G_1 \mid + \mid w \mid$	$3\mid G_1 \mid + \mid w \mid$	RM	CDH
[46]	$2.\mid Z_q \mid$	$2.\mid G_1 \mid$	$2.\mid G_1 \mid + \mid w \mid$	$3.\mid G_1 \mid + \mid w \mid$	SM	CR Hash and CDH
[48]	$\mid Z_q \mid$	–	$2.\mid Z_q \mid + \mid w \mid$	$3.\mid Z_q \mid + \mid w \mid$	RM	RSA
[49]	$2.\mid G_1 \mid$	–	$3.\mid G_1 \mid + \mid w \mid$	$(n + 4).\mid G_1 \mid + w \mid$	SM	CDH

TABLE V. COMPARISON OF VARIOUS SCHEME MODELS AND SIGNATURE VERIFICATION

Schemes	Del-gen	Multip-sign	Multip-verify	Provable security	Model
[27]	1Msc +1Po+3Ex	2Msc +1Po+3Ex	1Po+2Ex	NA	ROM
[28]	2M sc+3Po+2Ex	4Msc +4Po+3Ex	3Po+3Ex	NA	SM
[45]	2Msc+3Po	3Msc +5P0+1Ex	3Msc+4Po	NA	ROM
[47]	3Msc +5Po+1Ex	5Msc +3Po+1Ex	nMmc +3Po+1Ex	NA	SM
[50]	2Msc+3Po	4Msc+3Po	3Msc+3Po	YES	ROM
[51]	2Msc+3Po	3Msc +5Po+1Ex	3Msc +4Po	YES	ROM

TABLE VI. Comparison Of the Various Multi-Signature Schemes, Signature Size, Assumption, And Models.

Schemes	K_{Vf}	K_{Ag}	R_{nd}	Sign Size	Model and Asmpt
[28]	-	-	2	Zq3	DL, ROM
[31]	1G2	-	2	Zq2	N/A
[32]	1G2	-	2	G2×Zq4	DL, ROM
[37]	2P	-	1	G1	co-CDH,ROM
[43]	1G3	-	2	Zq3	DL, ROM
[48]	-	-	3	G × Zq	DL, ROM
[51]	2P	-	1	G1×G2	co-CDH
[52]		1Gn	22	Zq2	N/A

expresses n various exponentiations in the group G, where n is the number of signers, and "P" expresses a pairing operation. Column four presents the communication rotation, and column two shows the volume of every signer's shared key, the signature, and the aggregate shared key, wherever several "proof-of-possession" of the secure key is assumed to be part of the shared key. Column number six presents the hypothesis above, which some designs prove to protect under ROM [41], [51].

Scheme: Compact Multi-Signatures For Small Blockchain
Dan Boneh formulated a scheme that reduces the Bitcoin Blockchain's size and value in many other environments using multi signatures. All formulations maintain the signature handshake and aggregation of the public keys [7], [17], [31], [43].
Security Analysis: To verify that in many schemes, someone signs formal messages m, the verifier requires a small multi-signature, an innovative aggregate of public keys, and m message.
Strongness: The original method originates from BLS and Schnorr signatures. The straightforward general key standard implies that users do not expect to prove their secret key's knowledge or property.
Explanation: Formulate the initial dumpy accountable subgroup multi-signature (ASM) technique. An ASM technique allows any subset S a set of n members, to sign a message m so that a helpful sign identifies which subset generates the scheme [8].

Scheme: Simple Schnorr Multi-Sign With Bitcoin Applications
Security Analysis: The specific multi-signature systems contribute an advance over the current possible approach. The couple features improve the potential influence: The availability of significant aggregation eliminates verifiers' essential to observe all associated keys, enhancing network ranges, privacy, and verification value. Security follows the traditional shared fundamental model that supports multi-sign beyond numerous performances of information, where different witnesses cannot perform improvement [28], [31], [33]. These consider improving the number of events in which multi-sign is valuable.

Strongness: The new scheme improves enforcement and user secrecy in Bitcoin. The association between Discrete Logarithmic based multi-sign methods protected the traditional shared key model using a group G of order p and hash functions with l -bit outputs.
Explanation: The author introduced a new Schnorr-based multisignature scheme. It holds two respects: the first is practical and straightforward, the method has an equal key and signs intensity, as usual, Schnorr sign, and the second is to provide a key aggregate. That implies that the collective designation verifies precisely as a classical Schnorr sign involves a single" aggregated" shared key that computes the signer's shared key. The first multisignature scheme design protects the DL hypothesis in the plain public-key standard, providing essential aggregation to be most helpful.

Scheme: On the Protection Of Two Round Multi Sign
Security Analysis: The CoSi scheme does not prove secure, and then the author finds out certain defects in reissuing the security proof with some determining the different results and actual specifications of the scheme [6,18]. After that, examine the practical sub-exponential attacks in methods and add some evidence of vulnerability. The process mBCJ variant of BCJ after a two-round specification performance proves secure under the DL assumption in the ROM [19].
Strongness: This research demonstrates that mBCJ complex effects are more scalable than CoSi, provide signers to collaborate a message sign in about two seconds, and make a reasonable and specific reliable choice for large-scale deployment. In the performance of the multi-signatures, the key is the attestation pattern. For completeness, the first part of the scheme identifies a two-round multi-signature without matching and introduces a three-round system, a non-interactive pairing-based approach. The computation performance count by pairing-based proves and multi-exponentiation [6].
Explanation: This scheme collects signers to sign a message collaboratively and create a single signature, and verifiers verify each specific signer signs in the message. The signature scheme improves the two-round Schnorr-based multi-sign with high efficiency and decentralized and covers thousands of co-signers. The two-round multi-sign method without pairing serves security issues. First, they confirm that none of the schemes establishes Security completely different from directly known techniques. If the DLP is hard, then the algebraic change is not exited, proving any of the methods under the DLP.

5. Analysis Of Various Key Agreement Protocols and Threshold Scheme

This section discusses the key agreement protocols used in IoT and Blockchain applications. The key agreement applies to key exchanges in which two or more parties must perform a message securely and share a resultant key value. An alternative to key agreement is the use of information sharing. Key exchange contracts typically use cryptography to fulfill Security. Therefore, the threshold base signature methods achieve different fundamental agreement techniques to achieve these features. The threshold signature is a digital signature where signers authorize groups such that only particular group subsets present a signature on the part of the group. The threshold scheme is the combination of subsets approved to produce a signature. Therefore, the various schemes discuss as follows:

Scheme: An Efficient Proxy Sign Scheme Based On RSA
In this scheme, the author performs a proxy sign scheme based on the RSA for (EPSSB), and the singer signs the message on behalf of the original signer [53]. This scheme is an effective medium for choosing their signing ability to the opposite party. This scheme does not recognize a proxy repudiation tool, but it is more effective than the current RSA-based schemes, i.e., Lee et al. and Shao's scheme. This scheme performs a proxy signature in specific security conditions.
Strongness: It does not need any proxy key to deliver the secure channel, whereas a secure channel is necessary for the present scheme [28], [47], [51].

Scheme: An Efficient Multivariate Threshold RSS
The scheme uses the previous Petzoldt and Zhang-Zhao. It appropriates the unique connecting etiquette by Monteiro et al. to introduce a further effective threshold RSS. The proposed signature scheme was more profitable than before regarding communication detriments and sign range. The scheme's signature length is faster than Petzoldt and Zhang-Zhao individually.
Strongness: Future works will invent some additional sign schemes, including Monteiro et al.'s multiple attributes-based identification scheme [4]. Another desired outcome estimates the existing scheme's confidence in the quantum in ROM.

Scheme: An Efficient Threshold Ring Sign Technique This approach allows every grouping of t objects to automatically select temporary n-t objects to produce a carefully validated t out of n signatures on the part of the entire set of n things. At the same time, the primary signers continued anonymously based on the ring signature scheme in 2007.
Strongness: These schemes create an Identity-based threshold ring signing scheme. This scheme is incredibly stable under the conventional model, and its security implementation is extremely valuable. The ring signature scheme is a common challenge as the signature consists of some values from group elements.
This signature size is linearly comparable to the ring size and every user's key probe of the ring signature proposed by various authors in TCC 2006. Furthermore, this scheme is crucial to represent the identical group. This scheme has limitations, and several open problems [3], [4], [22].

6. Analysis Of Miscellaneous Security Schemes

This section discusses various sign schemes which are used in cryptosystems to secure the various IoT and Blockchain applications:

Scheme: Secured and Efficient Method For Delegation Of

Signing Rights
The author proposed a technique that protects the data from various attacks when transmitting messages in a channel. The proxy sign allows a signer to sign a message on behalf of other users, a proxy sign. In the multiproxy sign, the signer signs a message on behalf of a group member's signature, and each member is authorized to participate in the original transmission signer.
Strongness and Explanation: This scheme is practical and secure for ID-based MPS and the hardness of com-DHA as the bilinear map. The method [24] verifies the Security against adaptive chosen message and adaptive chosen ID attacks in the ROM under the com-DHA, shown in Table VII.

Scheme: Conditional Privacy-Preserving Authentication (IBSCPPA) Scheme
An ID-Based sign scheme without BP is valuable and efficient for vehicle-to-vehicle information transmission in the VANET system. The approach is capable ID-Based signatures with a provisional privacy-preserving authentication system. It is based on the ECC universal restricted hash function for a vehicle-to-vehicle communication system [10], [18], [44]. This Design presents the group signature attestation process, which authorizes specific vehicles to verify many messages simultaneously. The author presents the Security verified for this scheme in the ROM. The execution evaluation proves that the procedure, which is numerous and practical in computational cost, concerns relevant tasks.
Strongness and Explanation: This scheme utilizes standard restricted hash functions, preferably of M2P. The purpose of hash is to reduce the computational capacity of a verified vehicle throughout the Authentication of a message. The execution evaluation decides that the presented scheme's computational cost and batch signature attestation are lower than existing signature schemes [55].

7. Research Methods

This section of the review highlights the security knowledge gaps which need to be addressed to construct a trustworthy, acceptable, and responsible IoT and Blockchain platform based on the above literature. Despite their massive potential and various applications, developers and designers have yet to develop technical solutions for cloud systems. However, as Cloud computing or other related technologies (although data centers) resemble the working mechanism of traditional computing, they can provide a greater understanding of the relevant concerns and solutions.

From Figure 3, the information is selected from different publishers; first, the user chooses the topics for selection from web-based, and the system verifies with various methods and steps. The related queries are generated from the question definitions module, and the conceptual module generates the users' primary information. The user expands the selected topics, and the user verifies the description of the data. The users send it to the subsequent modules if the information is valid. The data were chosen from design methods based on the selections. After that, the best selects the results of searching pieces of information.

From Figure 4, using different resources, choose the various types of papers and classify them as International conferences, international journals, Surveys, and workshops/symposiums. Most articles were selected from international conferences because the other conference provided various new ideas on Security and applications. The Journal offers authentic research related to the area. The survey paper describes all views from date to date and authentications.

A. Requirement of Security system

This subsection discusses the security scheme's essential security features, such as confidentiality, integrity, execution, Authentication, and scalability used in cloud networks.

1) **Scalable key interchange:** The security framework provides a straightforward automatic connected security key control process for the cloud network provider and avoids the group's key dispatch. The user's key management delivers new keys required to encrypt the messages in real time in an application.
2) **Authentication:** This prevents unauthorized users from accessing the information they have not registered in the network. In reserve, a non-member entity does not complete a notification for which access contends. If many users report a common issue, The user cannot authenticate the actual users.
3) **Confidentiality and integrity:** It requires that messages are transmitted from the source node to the destination node via model to protect against malicious nodes or attackers for data re-transformation. These include authorized source nodes and destination nodes for secure routing probity. The security framework is protected against Denial of Service attacks, flood attacks, and particular or random attacks.
4) **Performance:** The security techniques reduce performance overhead such as storing information and sharing information to the Cloud-based network.

From the Table, VIII and IX find the various challenges. These challenges follow as [4], [27], [35], [40], [53]:

- **Challenge 1:**
  Including data and security measurements reduces the computational resources available for traditional cloud operations. Furthermore, the ciphertext can take more additional disc memory than the original text concerning the functional mechanisms of the application and database layers.

- **Challenge 2:**
  Preventing attacks is either too costly for experimental execution, or the explanation protects against a distinct kind of attack. Analysis indicates the attack's

TABLE VII. Comparison Of the Efficiency Of Different Schemes

Scheme	B_p	H_f	E_p	SM_m	OT			
					p_{kg}	m_{pv}	m_{psg}	Over all
[28]	3	2	2	2	95.96	73.78	124.65	294.29
[40]	1	0	0	3	45.56	75.92	75.02	196.50
[47]	3	0	1	6	103.71	78.19	84.57	266.44
[51]	3	1	0	2	85.34	99.01	121.34	305.65
[54]	2	2	0	5	71.98	65.6	78.36	215.95

Notes: Bp: No of Bilinear pairings Hf: Hash function Map Point Ep: Modular exponentiation SMm: Scalar Multiplication OT: Consequent Operation Time.

TABLE VIII. IoT Challenges And Security Challenges Width Various Schemes

S. No.	IoT Challenges	Security Challenges	Schemes
1	Losing physical control	Identification of Nodes	[7,22,25,26,36,38]
2	Multi-tenancy	Access Control multiple users	[10,20,22,19,30]
3	Privacy breach	Trust management	[8,9,10,34,52]
4	Location Privacy Preservation	Authentication and Identification	[12,13,21,45,52]
5	Detection of Rogue cloud Nodes and IoT Devices	Integrity and Non-repudiation	[10,22,25,28,29]
6	Privacy Exposure in Data Combination	Authorization and confidentiality	[10,25,30,35,40,45]
7	Transient storage	Secure data sharing	[12,15,18,20,52]
		Data Integrity and identification	[20,24,25,30,36]
		Data detection	[12,20,32,52]
8	Data Dissemination	Secure data distribution	[20,23,36,40]
		Sensitive data searching	[25,26,36,52]
		Data aggregation and privacy preservation	[2,12,23,25,56]
		Secure data transmission	[23,25,26,28,29]
9	Decentralized Computation	Secure Big data Computation	[25,35,45,56]
		Secure Data processing	[1,3,4,7,8,9,25]
		Data Verification and Data integrity	[1,5,6,7,8,10,36]
10	Real Time Services	Access control	[12,25,34,36,53]
		Trust management of KGC	[7,9,12,24]
		IDS and IPS	[23,25,26,29]
		Secure Lightweight protocol	[7,25,26,36]
		Node Identity and Authentication	[1,20,36,39,40,42]
		Attack prevention	[15,25,36,56]
11	Social and Environmental Impact	cybersecurity management	[23,25,36,39,42,53]
12	Concerns on AI and Autonomous Systems	Cybersecurity management	[12,14,18,19,36,53]

interferences with the multiple types of nodes and eliminates the required hardware and software.

- **Challenge 3:**
A Cloud network generally relates to several thin devices. These devices' data is affected through a single device for a short time, but when streaming numerous appliances is linked, the general information becomes highly difficult to manage. Therefore, filtering each network packet would provoke the condition to enhance technique and recollection capacity.

- **Challenge 4:**
Increasing the node's network complexity produces malware attacks because of the opportunity for vulnerabilities and the device's significant protection challenges every time threats detect. So, the cloud-based system furthermore needs a lightweight, network-based detection and cross-storage service for threats.

- **Challenge 5:**
The extensive cloud network's devices hold WS and IoT devices. Because of the large number of capable wireless devices and their availability, It is challenging to verify the protection of a cloud network. If the wireless network is not encrypted and linked, attackers have much capacity to intercept important data in conversation.

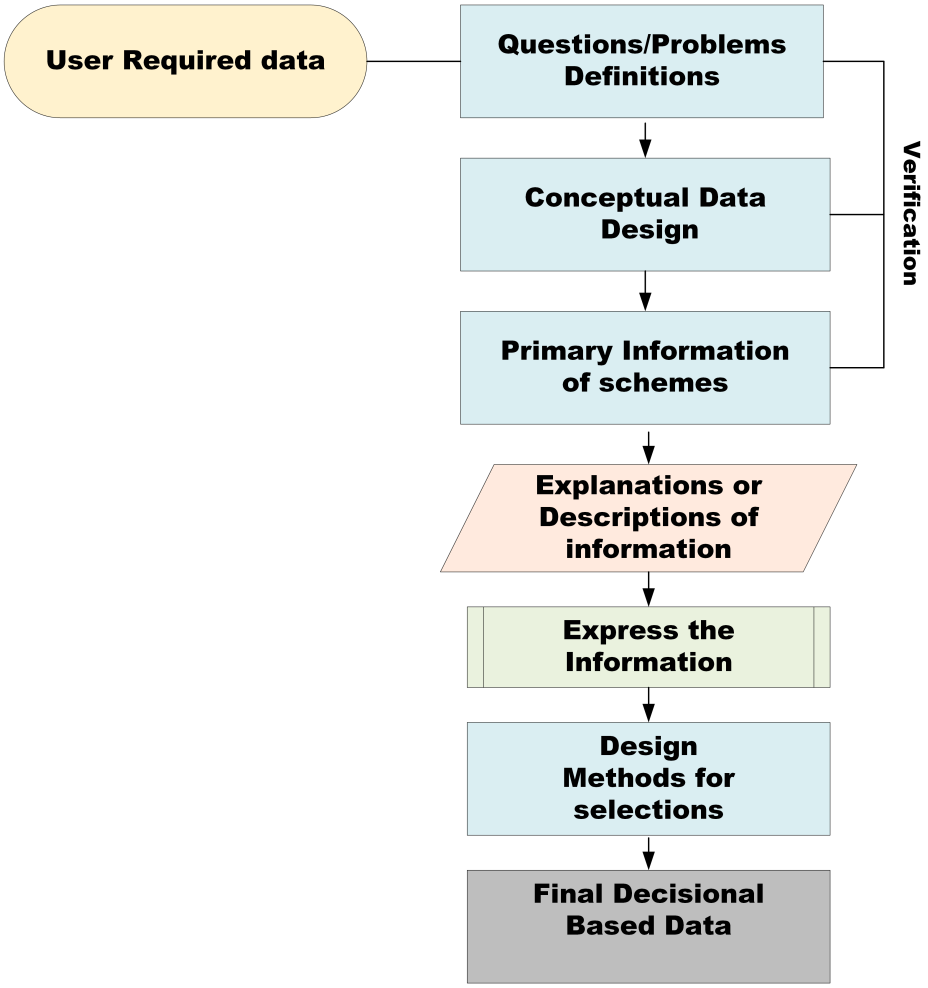

Figure 3. Proposed Techniques for data Selection from database

TABLE IX. Different Security services of the Security Schemes.

Security Solution	*Schemes*								
	[7]	[9]	[12]	[15]	[17]	[23]	[24]	[25]	[28]
Preventing Attacks	✓	×	×	✓	×	✓	✓	×	✓
Network Identification	✓	✓	✓	×	×	×	✓	✓	×
Malware Protection	✓	×	✓	✓	✓	✓	✓	×	✓
Wireless communication security	✓	✓	✓	✓	×	×	✓	✓	×
Secure Vehicular Network	×	×	✓	×	×	×	×	×	×
Authentication	✓	✓	✓	×	✓	×	×	✓	✓
Linkability	✓	✓	✓	✓	×	✓	✓	✓	✓
Unforgeability	×	×	×	✓	×	×	✓	×	✓
Traceability	×	✓	×	✓	×	✓	×	✓	✓
Identification	✓	×	×	×	✓	✓	×	×	×
Non-repudiation	✓	✓	×	✓	×	✓	✓	×	✓

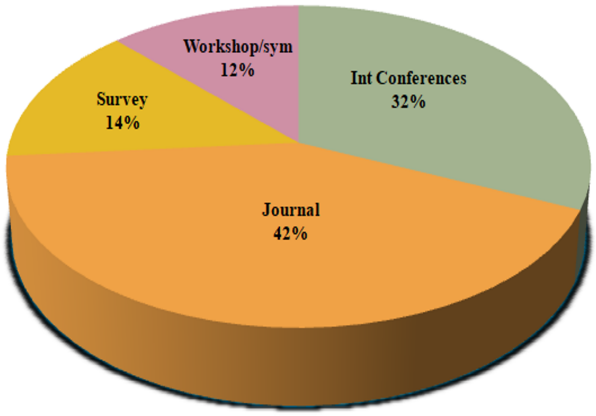

Figure 4. Classification of the research papers used in articles. [2], [3], [4]

- **Challenge 6:**
  A cloud network is volatile as the connection with the end-user is specified for a short time, so it is challenging to verify identities. The number of links to large data sets is increasing significantly. Even a robust cyber security system will be rendered ineffective.

- **Challenge 7:**
  When a cloud node begins to transmit various data and resources to the network, the cloud services like performance, scalability, data security, user identity, and monitoring, the potential appearance of insider threats becomes challenging to manage in a cloud network for IoT applications and Blockchain.

- **Challenge 8:** With an insufficient protection system, the execution can have numerous implementation problems of a security system. So, it became essential to determine conformity with the requirements carefully. What security services to combine with the capacity to require nodes and choose the secure execution models?

- **Challenge 9:**
  Verify the security system by challenging it to ensure Security for the entire system structure—one of the most critical issues in the preservation of complex systems. It is difficult for designers to determine a secure scheme that addresses all high-level security threats.

- **Challenge 10:**
  Security limitations should be required based on the semantic factors of IoT and Blockchain applications, not their schemes, models, techniques, and secure development procedures. In these phases, recognize threats and attacker goals—furthermore, conceptual protection justifications are required to prevent these goals without assuming performance attributes.

- **Challenge 11:**
  The Interoperability between IoT platforms should not imply significant modifications in the participants' systems, and the solution should not be dependent on their systems.

B. Comparison of Protocol Encryption/Decryption, Assumption, Security, and Efficiency

The subsection examines the different ID-based schemes, signature attacks, etc. After that concerns other protocol methods description, setup, extracting the public or secret key, encryption/decryption methods, and its assumption as follows:

ID-Based Encryption Scheme Without ROM [24]

- **Protocol Representation:**
  - Setup Phase: Let assumed identity-based (ID) public key elements of $\mathbb{Z}_q^*$ and message elements of G_2.
    Choose random elements $m, n \in \mathbb{Z}_q^*$ and set $\mathbb{U} = mP, \mathbb{V} = nP$. So, (m,n) key and $(\mathbb{U}, \mathbb{V})$ are set of parameters.
  - Extract Phase: The key $ID \in \mathbb{Z}_q^*$, pick random $r \in \mathbb{Z}_q^*$ and compute value $\mathbb{K} = \frac{1}{ID+m+yn} P \in G_1$ and result value as private key $S_{ID} = (r, \mathbb{K})$.
  - Encrypt Phase: The encryption of messages $\mathbb{M} \in G_1$ as public key $ID \in \mathbb{Z}_q^*$, choose a randomly $s \in \mathbb{Z}_q^*$ and result value as the ciphertext as
    $$C = \left\langle s(ID)P + s\mathbb{U}, s\mathbb{V}, e(P,P)^s M \right\rangle.$$
  - Decrypt Phase: For decryption of a Cipher value $C = \langle X, Y, Z \rangle$. use the secret key $S_{ID} = (r, \mathbb{K})$, and result value is $Z/e(X + rY, \mathbb{K})$

- **Assumption Phase:** q-Decisional Bilinear Diffie-Hellman Inversion(q-DBDHI) assumption is hard.

- **Security Phase:**To protect from facing the selective ID-based adaptive chosen ciphertext attack without ROM under the q-DBDHI problem.

- **Efficiency Phase:**
  - Setup: Two non-zero multiplication.
  - Extract: One inversion in $\mathbb{Z}_q^*$; one scalar multiplication in G_1
  - Encrypt: Four non-zero multiplication in G_1
  - Decrypt: One non-zero multiplication in G_1: one addition in G_1, and one inverse in G_2.

Table X analyzes the various terms of various papers that show as a reference and each paper protocol description with the help of different techniques such as setup, extract, encrypt, and decrypt. Other parts of the paper explain which assumptions use and related security. The security

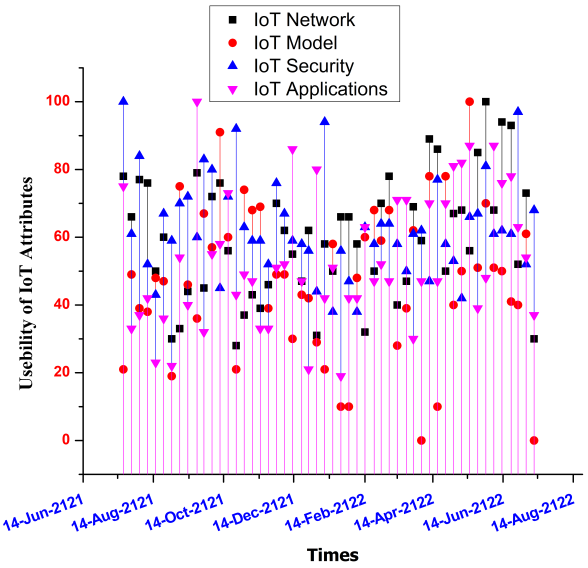

Figure 5. Internet of Things network, Model, Security, and its applications [51]

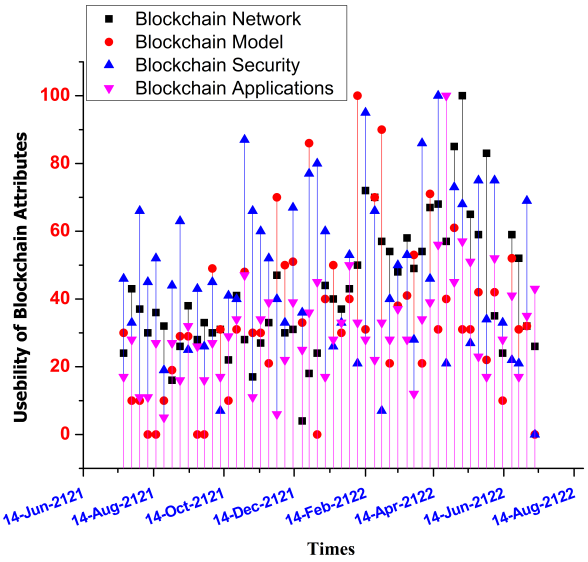

Figure 6. Blockchain Network architecture, Model, Security, and its applications [51]

explanations are based on various cryptography methods. The successive terms explain efficiency in different phases: setup, extract, encrypt, and decrypt. The table uses the x-mark, which denotes the techniques does not confirm use as related paper, and the tick-marks show the various techniques used with related paper, which explains the above details [39].

1) **IoT Current Trends and Applications:** In the IoT network, the current applications and their security schemes protect the pieces of information. Communicating with the node required the encryption/decryption scheme to preserve the messages. The network performance also depends on the IoT model and its application in different techniques [34], [39], [51], [27], shown in Figure 5. In Figure 5, the Black point shows the IoT network used with IoT models present in red colors and the operation used of Security in blue colors in different IoT applications in purple colors.
2) **Blockchain current Trends and Applications:** In Figure 6, the Blockchain comprises the network model for various applications with security features. The security features protect the data in communication with various ID-based schemes and cryptosystems [39], [28]. In Figure 6, the black points show the Blockchain network used with Blockchain models present in red colors and the operation used of Security as blue colors in different IoT applications purple colors.

C. *Abbreviations and Acronyms*

Abbreviation	Definition
DLP	Discrete Logarithm Problem
FP	Factoring Problem
BLP	Bilinear pairing
ROM	Random Oracle Model
Sign	Signature
Com-DHA	Computational Diffie-Hellman Assumptions
ID-Based	Identity based
Multi	Multi-signature scheme
IBMPS	Identity Based Multi Proxy Signature
RSS	Ring Signature Scheme
ECC	Elliptic curve cryptography
IoT	Internet of Things
CA	Certificate Authority
Pub	Public key
KGC	Key Generation center

8. Conclusions and Future Work

This article analyzes the Identity-Based bilinear pairing and non-pairing schemes with various security algorithms based on cryptosystems of different applications as research challenges, techniques, services, and opportunities. Security is categorized based on application models, methods, and process levels. Some security schemes are the standard for secure Blockchain and other applications. Our analysis also explores and increases the security aspects to address the others based on insights from the analysis of research techniques and promising research directions for different security applications. The analysis reflects meaningful conceptual and specialized approaches at this crossroads of impressive improvement. It expects that our

TABLE X. Various scheme and its Efficiency, protocol description and security

Ref	Protocol Description				Assump	Security	Efficiency			
	Setup	Extract	Encry	Decry			Setup	Extract	Encry	Decry
[5]	✓	✓	✓	✓	NA	SM	✓	✓	✓	✓
[7]	✓	✓	✓	✓	DLP ,BL	NA	✓	✓	✓	✓
[8]	✓	✓	✓	✓	NA	NA	✓	✓	✓	✓
[9]	✓	✓	✓	✓	NA	SM	✓	✓	✓	✓
[11]	×	✓	✓	✓	GDH	Under ROM	×	✓	×	✓
[13]	×	✓	✓	✓	GDH	SM	✓	✓	✓	×
[18]	✓	✓	✓	✓	NA	NA	✓	✓	✓	✓
[22]	✓	✓	✓	✓	NA	SM	✓	×	✓	✓
[25]	✓	✓	✓	✓	DBDH	NA	✓	✓	×	✓
[28]	✓	✓	✓	✓	DLP ,BL	NA	✓	✓	✓	✓
[29]	×	×	✓	✓	DLP ,BL	NA	✓	✓	✓	✓
[30]	✓	✓	✓	✓	GDH	SM	✓	✓	×	✓
[31]	✓	×	✓	✓	FD,DLP	SM	×	✓	✓	✓
[32]	✓	✓	✓	✓	DLP ,BL	SM	×	✓	×	✓
[34]	✓	✓	✓	✓	DLP ,BL	NA	✓	✓	✓	×
[35]	✓	✓	✓	✓	DLP ,BL	NA	✓	✓	✓	✓
[43]	✓	×	✓	✓	DLP ,BL	SM	×	✓	✓	✓
[44]	✓	✓	✓	✓	FD,DLP	u-ROM	✓	✓	✓	✓
[49]	✓	✓	✓	✓	GDH	NA	×	✓	✓	✓
[50]	✓	✓	✓	✓	FD,DLP	NA	×	✓	✓	✓
[52]	✓	✓	✓	✓	FP	SM	×	✓	✓	✓
[56]	✓	✓	✓	✓	BDH	under ROM	✓	✓	✓	✓
[57]	✓	✓	✓	✓	DLP ,BL	NA	✓	✓	×	✓

measure puts a clear framework for building protection and innovative service in research and building schemes. This article categorized the existing proposals according to their security handling techniques as pairing and non-pairing schemes, and attributes-based security schemes based on different models such as ROM, SM, etc., for open standards. Each security scheme type has various standards. The most effective technique has been shown in this article on scheme analysis. It is unbelievable to analyze related IoT applications and platforms. Most of the scheme's challenges and setup model have been summarized in (Tables 8,9 and 10) with future scope. It outlines how most proposals support algorithm classes and the semantic cryptography algorithm's support for scheme setup.

References

[1] D. Chaum, "Blind signatures for untraceable payments," in *Advances in cryptology*. Springer, 1983, pp. 199–203.

[2] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *International conference on the theory and application of cryptology and information security*. Springer, 2001, pp. 552–565.

[3] Y. Zhou, N. Li, Y. Tian, D. An, and L. Wang, "Public key encryption with keyword search in cloud: a survey," *Entropy*, vol. 22, no. 4, p. 421, 2020.

[4] H. Guo and L. Deng, "An identity based proxy signcryption scheme without pairings." *Int. J. Netw. Secur.*, vol. 22, no. 4, pp. 561–568, 2020.

[5] R. Barua, R. Dutta, and P. Sarkar, "Extending joux's protocol to multi party key agreement," in *International Conference on Cryptology in India*. Springer, 2003, pp. 205–217.

[6] S. Han, W. K. Yeung, and J. Wang, "Identity-based confirmer signatures from pairings over elliptic curves," in *Proceedings of the 4th ACM conference on Electronic commerce*, 2003, pp. 262–263.

[7] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *SIAM journal on computing*, vol. 32, no. 3, pp. 586–615, 2003.

[8] K. Gu, W. Zhang, S.-J. Lim, P. K. Sharma, Z. Al-Makhadmeh, and A. Tolba, "Reusable mesh signature scheme for protecting identity privacy of iot devices," *Sensors*, vol. 20, no. 3, p. 758, 2020.

[9] S. Micali, K. Ohta, and L. Reyzin, "Accountable-subgroup multisignatures," in *Proceedings of the 8th ACM Conference on Computer and Communications Security*, 2001, pp. 245–254.

[10] D. Boneh and X. Boyen, "Efficient selective-id secure identity-based encryption without random oracles," in *International conference on the theory and applications of cryptographic techniques*. Springer, 2004, pp. 223–238.

[11] G. Swapna, P. Gopal, T. Gowri, and P. V. Reddy, "An efficient id-based proxy signcryption scheme," *International Journal of Information and Network Security*, vol. 1, no. 3, p. 200, 2012.

[12] N.-W. Lo and J.-L. Tsai, "A provably secure proxy signcryption scheme using bilinear pairings," *Journal of Applied Mathematics*, vol. 2014, 2014.

[13] J. Han, X. QiuLiang, and C. Guohua, "Efficient id-based threshold ring signature scheme," in *2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, vol. 2. IEEE, 2008, pp. 437–442.

[14] S. H. Islam and M. S. Obaidat, "Design of provably secure and efficient certificateless blind signature scheme using bilinear pairing," *Security and Communication Networks*, vol. 8, no. 18, pp. 4319–4332, 2015.

[15] K. Gu, Y. Wang, and S. Wen, "Traceable threshold proxy signature." *Journal of Information Science & Engineering*, vol. 33, no. 1, 2017.

[16] A. Boldyreva, "Threshold signatures, multisignatures and blind signatures based on the gap-diffie-hellman-group signature scheme," in *International Workshop on Public Key Cryptography*. Springer, 2003, pp. 31–46.

[17] D. Boneh, M. Drijvers, and G. Neven, "Compact multi-signatures for smaller blockchains," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2018, pp. 435–464.

[18] M. Drijvers, K. Edalatnejad, B. Ford, and G. Neven, "Okamoto beats schnorr: On the provable security of multi-signatures." *IACR Cryptol. ePrint Arch.*, vol. 2018, p. 417, 2018.

[19] M. Drijvers, K. Edalatnejad, B. Ford, E. Kiltz, J. Loss, G. Neven, and I. Stepanovs, "On the security of two-round multi-signatures," in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019, pp. 1084–1101.

[20] P. S. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in *International conference on the theory and application of cryptology and information security*. Springer, 2005, pp. 515–532.

[21] S. Shen, H. Wang, and Y. Zhao, "Identity-based authenticated encryption with identity confidentiality," *Theoretical Computer Science*, vol. 901, pp. 1–18, 2022.

[22] S. Srivastava and S. Prakash, "Security enhancement of iot based smart home using hybrid technique," in *International Conference on Machine Learning, Image Processing, Network Security and Data Sciences*. Springer, 2020, pp. 543–558.

[23] R. Singh, S. Prakash *et al.*, "Privacy preserving in tpa for secure cloud by using encryption technique," in *2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*. IEEE, 2017, pp. 1–5.

[24] H. Du, Q. Wen, S. Zhang, and M. Gao, "A new provably secure certificateless signature scheme for internet of things," *Ad Hoc Networks*, vol. 100, p. 102074, 2020.

[25] F. Hess, "Efficient identity based signature schemes based on pairings," in *International workshop on selected areas in cryptography*. Springer, 2002, pp. 310–324.

[26] P. K. Kancharla, S. Gummadidala, and A. Saxena, "Identity based strong designated verifier signature scheme," *Informatica*, vol. 18, no. 2, pp. 239–252, 2007.

[27] R. Kumar and D. Gupta, "Security in real time multimedia data based on generalized keys," in *Proceedings of the International Conference on Advances in Computing and Artificial Intelligence*, 2011, pp. 93–96.

[28] R. Gaur and S. Prakash, "Performance and parametric analysis of iot's motes with different network topologies," in *Innovations in Electrical and Electronic Engineering*. Springer, 2021, pp. 787–805.

[29] K. Gu, W. Jia, and J. Zhang, "Identity-based multi-proxy signature scheme in the standard model," *Fundamenta Informaticae*, vol. 150, no. 2, pp. 179–210, 2017.

[30] B. Lee, H. Kim, and K. Kim, "Secure mobile agent using strong non-designated proxy signature," in *Australasian Conference on Information Security and Privacy*. Springer, 2001, pp. 474–486.

[31] Z. Shao, "Proxy signature schemes based on factoring," *Information Processing Letters*, vol. 85, no. 3, pp. 137–143, 2003.

[32] R. A. Sahu and S. Padhye, "Provable secure identity-based multi-proxy signature scheme," *International Journal of Communication Systems*, vol. 28, no. 3, pp. 497–512, 2015.

[33] J. Zhang and Y. Zhao, "A new multivariate based threshold ring signature scheme," in *International Conference on Network and System Security*. Springer, 2015, pp. 526–533.

[34] A. Petzoldt, S. Bulygin, and J. Buchmann, "A multivariate based threshold ring signature scheme," *Applicable Algebra in Engineering, Communication and Computing*, vol. 24, no. 3, pp. 255–275, 2013.

[35] F. S. Monteiro, D. H. Goya, and R. Terada, "Improved identification protocol based on the mq problem," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 98, no. 6, pp. 1255–1265, 2015.

[36] M. Bellare and G. Neven, "Multi-signatures in the plain public-key model and a general forking lemma," in *Proceedings of the 13th ACM conference on Computer and communications security*, 2006, pp. 390–399.

[37] K. Cohn-Gordon, C. Cremers, B. Dowling, L. Garratt, and D. Stebila, "A formal security analysis of the signal messaging protocol," *Journal of Cryptology*, vol. 33, no. 4, pp. 1914–1983, 2020.

[38] I. Ali, T. Lawrence, and F. Li, "An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in vanets," *Journal of Systems Architecture*, vol. 103, p. 101692, 2020.

[39] L. Deng, X. He, and T. Xia, "Secure identity-based blind signature scheme for online transactions," *Wireless Personal Communications*, vol. 116, no. 3, pp. 1525–1537, 2021.

[40] H. Guo, W. Li, E. Meamari, C.-C. Shen, and M. Nejad, "Attribute-based multi-signature and encryption for ehr management: A blockchain-based solution," in *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2020, pp. 1–5.

[41] Z. Jin, Q. Wang, and Z. Li, "A formal construction of certificateless proxy multi-signature scheme," *International Journal of Security and Networks*, vol. 11, no. 3, pp. 126–139, 2016.

[42] J. Liu, H. Wang, M. Xian, and K. Huang, "A secure and efficient scheme for cloud storage against eavesdropper," in *Interna-*

tional Conference on Information and Communications Security. Springer, 2013, pp. 75–89.

[43] Z. Cheng, L. Vasiu, and R. Comley, "Pairing-based one-round tripartite key agreement protocols," *Cryptology ePrint Archive*, 2004.

[44] X. Liu, H. Zhu, J. Ma, Q. Li, and J. Xiong, "Attribute based multisignature scheme for wireless communications," *Mobile Information Systems*, vol. 2015, 2015.

[45] H. Chen, M. Pendleton, L. Njilla, and S. Xu, "A survey on ethereum systems security: Vulnerabilities, attacks, and defenses," *ACM Computing Surveys (CSUR)*, vol. 53, no. 3, pp. 1–43, 2020.

[46] S. Verma and B. K. Sharma, "An efficient proxy signature scheme based on rsa cryptosystem," *signature*, vol. 51, 2013.

[47] N. Tahat and A. A. Tahat, "Identity-based threshold group signature scheme based on multiple hard number theoretic problems." *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 10, no. 4, 2020.

[48] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2794–2830, 2019.

[49] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, vol. 107, pp. 841–853, 2020.

[50] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1508–1532, 2019.

[51] "Google Trends — trends.google.com," https://trends.google.com/trends/?geo=IN, [Accessed 24-Sep-2022].

[52] C. Ma, J. Weng, Y. Li, and R. Deng, "Efficient discrete logarithm based multi-signature scheme in the plain public key model," *Designs, Codes and Cryptography*, vol. 54, no. 2, pp. 121–133, 2010.

[53] Q. Chen, Z. Huang, Y. Ding, Y. Zhou, and H. Huang, "A new provably secure identity-based multi-proxy signature scheme," in *International Symposium on Cyberspace Safety and Security*. Springer, 2019, pp. 230–242.

[54] L. Zhou, A. Fu, S. Yu, M. Su, and B. Kuang, "Data integrity verification of the outsourced big data in the cloud environment: A survey," *Journal of Network and Computer Applications*, vol. 122, pp. 1–15, 2018.

[55] G. Maxwell, A. Poelstra, Y. Seurin, and P. Wuille, "Simple schnorr multi-signatures with applications to bitcoin," *Designs, Codes and Cryptography*, vol. 87, no. 9, pp. 2139–2164, 2019.

[56] J. Chang, H. Wang, F. Wang, A. Zhang, and Y. Ji, "Rka security for identity-based signature scheme," *IEEE Access*, vol. 8, pp. 17 833–17 841, 2020.

[57] K. U. Maheswari, S. M. S. Bhanu, and S. Nickolas, "A survey on data integrity checking and enhancing security for cloud to fog computing," in *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*. IEEE, 2020, pp. 121–127.

Rajkumar Gaur is pursuing PhD (Information Security) in Department of ITCA, Madan Mohan Malaviya University of Technology Gorakhpur, India. He has received his M.Tech (Information Security) from Motilal Nehru National Institute of Technology Allahabad, Prayagraj, India in 2009. He has received his B. Sc (Maths) from DDU, Gorakhpur, India in 2000. He has selected for MHRD scholarship during his M. Tech and TEQIP by Ph.D. He has qualified GATE-2007 in CSE conducted by IIT-Kanpur. His research area includes IoT and Cryptography. He has published international journals and international conference papers in various top-level. He is reviewing in many journals like Springer, Elsevier, IEEE, etc.

Shiva Prakash , (Professor & Head of Department of ITCA) and area of Wired/Wireless Networks, IoT, Mobile and Cloud Computing, Algorithms The teaching experience in UG is 22 years and PG is 20 years.