Enhanced Security for Large-Scale 6G Cloud Computing: A Novel Approach to Identity based Encryption Key Generation

[1]Gopal Rathinam, [2]M Balamurugan, [3]V Arulkumar, [4]M Kumaresan, [5]S Annamalai and [6]J Bhuvana
[1]Information and communication Engineering, College of Engineering, University of Buraimi, Al Buraimi, Oman. [2]Department of CSE, CHRIST(Deemed to be University), Bengaluru-560074, India.
[3]School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, TamilNadu, India.
[4,5]Department of Computer Science and Engineering, Jain Deemed-to-be University, Karnataka, India.
[6]Department of CSIT, Jain(Deemed to be University), Bengaluru – 560069, India.
[1]gopal.r@uob.edu.om, [2]balamurugan.m@christuniversity.in, [3]arulkumar.v@vit.ac.in, [4]phdkumaresan@gmail.com, [5]annamalaiphd@gmail.com, [6]j.bhuvana@jainuniversity.ac.in

Correspondence should be addressed to Gopal Rathinam : gopal.r@uob.edu.om.

Article Info
Journal of Machine and Computing (http://anapub.co.ke/journals/jmc/jmc.html)
Doi: https://doi.org/10.53759/7669/jmc202303009
Received 25 August 2022; Revised from 18 December 2022; Accepted 31 December 2022.
Available online 05 April 2023.

Abstract – Cloud computing and 6G networks are in high demand at present due to their appealing features as well as the security of data stored in the cloud. There are various challenging methods that are computationally complicated that can be used in cloud security. Identity-based encryption (IBE) is the most widely used techniques for protecting data transmitted over the cloud. To prevent a malicious attack, it is an access policy that restricts access to legible data to only authorized users. The four stages of IBE are setup, key extraction or generation, decryption and encryption. Key generation is a necessary and time-consuming phase in the creation of a security key. The creation of uncrackable and non-derivable secure keys is a difficult computational and decisional task. In order to prevent user identities from being leaked, even if an opponent or attacker manages to encrypted material or to decode the key this study presents an advanced identity-based encryption technique with an equality test. The results of the experiments demonstrate that the proposed algorithm encrypts and decrypts data faster than the efficient selective-ID secure IBE strategy, a competitive approach. The proposed method's ability to conceal the identity of the user by utilizing the Lagrange coefficient, which is constituted of a polynomial interpolation function, is one of its most significant aspects.

Keywords – Cloud Computing, Identity-Based Encryption, Large Scale 6G, Cloud Security, Equality Test.

I. INTRODUCTION

The application of cloud computing has expanded significantly in recent years. Increasing numbers of files are being kept on cloud servers, and in order to stop data leaks, these files have been encrypted. However, in order for users to use this encrypted data in the future, cloud servers must also process them in addition to storing them. One of the most popular methods used to protect communication between two parties is public key infrastructure (PKI). Private keys are produced at the moment of communication, whereas public keys are just the user's identification, such as their organization name and email address, and are known to all. PKI is built on public and private keys. The success rate of decryption and encryption accuracy has been found to be relatively low because it necessitates prior information of cryptography [1].

To protect communication between two users, Shamir [2] pioneered the first identity-based cryptographic technique in 1984. This method makes use of a master private key and public key and, or both keys altogether. These keys are used for encryption and decryption, are created using a private key generator (PKG). It can be difficult to provide an effective key generation mechanism for several service users or accessors in an identity-based approach, because producing the private key takes up the majority of the computational resources [3,4]. The key generator authority must always provide keys to users because they are time-based, meaning they expire after a particular amount of time. Key is the most crucial component in ensuring the security of the user's data in addition to these other factors. The main objective is to generate a secure key with the least amount of computational cost. Identity-based encryption (IBE) creation has been the subject of extensive research due to the difficulty in efficiently creating keys. The size of the generated key has a significant impact

on both the encryption and decryption methods employed in (IBE). An unauthorized user cannot decrypt material that has been encrypted in order to obtain the identity, key, or any other valuable information. The identifying vector, the secret key it is paired with, and the encrypted data are needed for the decryption process.

The [5] proposed Public Key Encryption with Keyword Search (PKEKS), a revolutionary concept for searching encrypted material. PKEKS techniques are able to search for encrypted data, but cannot decode it. To implement the decryption function, The [6] developed a novel approach called public key encryption scheme with equality test (PKEET). A sort of method that combines searchable encryption (SE) with public key encryption enables users to decode ciphertexts and identify if the messages corresponding to the ciphertexts are same, even if the public keys used to encrypt the messages are different (PKE). In [7] developed a new, more successful PKEET technique that accomplished security in the standard model (SM). Unfortunately, PKEET confronts a problem with certificate management.

Later, Ma presented the identity-based encryption with equality test (IBEET) as a new approach to address this issue [8]. She also presented the first actual IBEET system that was successful in achieving one-way security against chosen-ciphertext attack. Authors [9] presented a new equality test scheme that makes use of identity-based cryptography to address the issue. However, the [10] demonstrated through the use of an attack that Wu's plan failed to provide the security they needed and provided a modification technique. Later [11] suggested a novel technique employing a witness-based cryptographic primitive with an additional pairing operation to withstand insider attack in cloud computing. The primary drawback of the IBE technique is the lengthier decryption and encryption times. The key created using The IBE technique can be computationally or briefly rapid by employing the fewest bits possible, as well as the fewest bilinear pairings and group multiplications. This paper's main objective is to suggest an effective key generation approach that increases the security of cloud data while being computationally efficient.

Further sections arranged as follows: **Section 2** discusses related work. Preliminaries relating to bilinear mapping and computational assumptions are introduced in **Section 3**. A security definition is presented in **Section 4**. The intended work is detailed in **Section 5**; **Section 6** presents the Results and Discussions with time graphs, and paper concluded in **Section 7**.

II. LITERATURE REVIEW

In [2] created an identity-based cryptosystem in which the identities of the users serve as the private key and a public key generator (PKG) generates the private keys corresponding to their identities. This study also offered an identity-based authentication and signature approach based on an equality test. To identify malware and validate encrypted data, work [12] applied their innovative IBEET approach. In [13] established an efficient identity-based method for exchanging private information. The method uses a similarity test to cloud-encrypted data in search of data that is comparable to the target data. IBEET resolves the PKEET issue, however it still has a problem with key escrowing. To overcome this issue, in [14] presented a new analytic framework certificateless PKEET (CL-PKEET). Later, [15] established that Ma's IBEET system is not OW-CCA secure, and they subsequently updated the strategy. Work [16] presented IBEET to provide flexible authorization (IBEET-FA). Based on the RSA assumption [17] established an efficient IBEET approach. Eventually [18] created a novel concept known as group IBEET (G-IBEET) by including group mechanism into IBEET. Work [19] combined the concepts of key-insulated encryption (KIE) with IBEET to produce key-insulated IBEET. In addition, their strategy featured a key-isolating technique to reduce the likelihood of key exposure. Paper [20] have recently developed a broad strategy for achieving security in the SM for PKEET that may also be applied to the IBEET scheme.

Other than a wide technique offered by Lee et al. [20] that can achieve security in the SM, we are aware that all other approaches for IBEET systems achieve security in the random oracle model (ROM). In addition, they state that the hierarchical IBE scheme must have three levels and that the signature must only be used once. In order to ensure the scheme's equality test function, security in the SM, and the validity of ciphertexts, the general method must additionally employ the HIBE scheme to encrypt twice and the signature scheme to sign once. So, their plan is not very effective. In this paper, we describe a brand-new IBEET strategy for securing the SM fully. Then, the security model and the IBEET model are defined. Using prime order bilinear groups, we demonstrate that our IBEET approach achieves one-way and indistinguishability security against chosen-identity and chosen-ciphertext assaults (OW/IND-ID-CCA). The plan is compared to the existing IBEET systems. We describe the first known practical IBEET approach for comprehensive security in the SM.

For the cloud computing environment [21] suggested an identity-based encryption system that also leverages the equality test and gets beyond [8]'s issue. This strategy entails six stages: setup, extraction, trapdoor, encrypting, decrypting, and testing. The data is encrypted using the first five phases, and the equality test is performed using the final phase, Test. It accepts the inputs CA, IDA, and tdA as well as CB, IDB, and tdB and outputs a binary value. The CA and CB plaintexts are identical if the outcome of the algorithm is 1, otherwise it returns 0.

In order to secure the healthcare system, [22] presented an IBE approach. The health-care industry now heavily utilizes cloud services. The organization must secure the cloud server where it maintains confidential patient information. The data in this work is protected from the attacker during transmission by using IBE and a signature technique. This strategy makes use of a unique public identification (ID) to guarantee that only the user who has been verified can access

information. In [23] presented an upgraded secure key generation large-scale 5G for cloud computing employing enhanced IBE. The IBE and key generator is depicted in **Fig 1.**

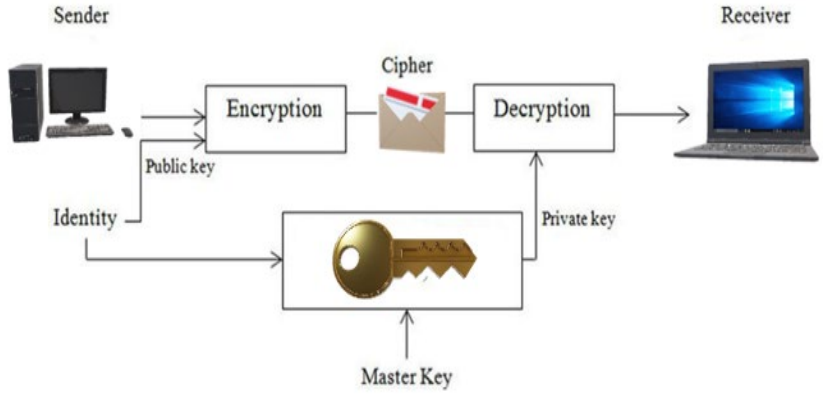

Fig 1. IBE and key generator

The Sixth-Generation Network

Compared to the fourth and the fifth generation network standard would offer increased service quality in addition to new functions. The latest frequency bands, including the optical spectra and mmWave, better spectrum use controls the unlicensed and licensed bands are all included in the fifth-generation network standard. However, the automated and data center-based centric systems' fastest growth may also outpace the capabilities of structures for 5G Wi-Fi. [24].

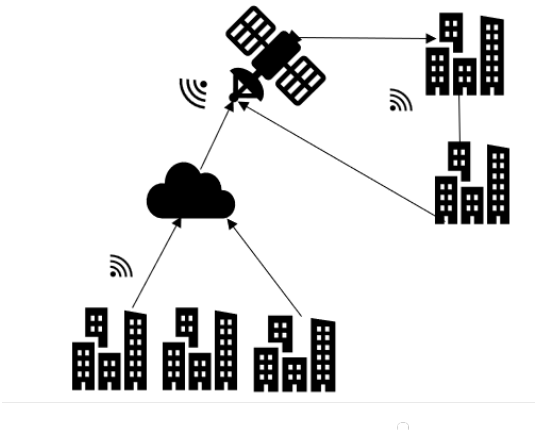

Fig 2. Sample 6G network usage.

Fig 2. displays the sample 6G network usage. Some gadgets, including virtual reality (VR) equipment, would demand at least a 10 Gbps data rate, which would make them go beyond 5G. The convergence of prior capabilities, such as high dependability, reduced energy usage, and increased security and data for connection, may be the primary drivers of sixth generation [27]. The rate of internet access would speed up geometrically [28]. The impact of this technology would result in various exciting benefits for society, including: (1) high-level special healthcare; (2) zero traffic accidents; and (3) zero local crime rates [29].

III. PRELIMINARIES

Lagrange Interpolating Polynomial

Assume p as a prime and $f(x) = a_0 + a_1 x + \cdots + a_t x^t (\mathrm{mod} p)$ a polynomial of degree t, where $a_0, a_1, \cdots, a_t \in \mathbb{Z}_p$ are coefficients. Considering any $t+1$ points $(x_1, y_1), \cdots, (x_{t+1}, y_{t+1})$ on $f(x), a_0 = f(0)$ can be calculated using a polynomial of Lagrange interpolation $(0) = \sum_{i \in A} \Delta_i y_i$ $A = \{1, \cdots, t+1\}$.

Traditional Public Key Encryption

Each of the following algorithms makes up a PKE scheme

- PKE.Setup (k) : This algorithm generates the system parameter pp from an input security parameter k.
- PKE.Enc (pk, m) : This algorithm outputs C as the ciphertext after requiring a message m and the public key pk as inputs.

- PKE.KeyGen (pp) : This algorithm outputs the public/private pair of keys after receiving the system parameter pp as input (pk, sk).
- PKE.Dec (sk, C) : This algorithm generates the matching message m from the private key sk and a ciphertext C.

Identity-Based Encryption
The following algorithms represent an IBE scheme

- IBE.Setup (k) : This algorithm outputs the master key msk and the system parameter pp after receiving as input a security parameter k.
- IBE.KeyGen (msk, ID) : This method outputs the user's private key sk_{ID} after receiving the master key msk and the identification ID of the user as inputs.
- IBE.Enc (ID, m) : This algorithm generates C as the ciphertext from an input of a message m and a user's identity ID.
- IBE.Dec (sk_{ID}, C) : This algorithm generates the matching message m using the ciphertext C and the user's private key sk_{ID}.

Identity-Based Encryption with Equality Test
The algorithms in an IBEET scheme are as follows

- IBEET.Setup (k) : The technique includes a security parameter as input and outputs the master key msk along with the system parameter pp.
- IBEET.KeyGen (msk, ID) : This algorithm outputs the associated private key sk_{ID} after receiving the master key msk and the receiver's identification ID as inputs.
- IBEETJEnc (ID, m) : This algorithm outputs C as the ciphertext after taking as inputs a message $m \in \mathbb{M}$ with a message space of M and a receiver's identification ID.
- IBEET.Dec (sk_{ID}, C) : This technique generates the matching message m from the receiver's private key sk_{ID} and ciphertext C.
- IBEET.Aut (sk_{ID}) : This procedure outputs the trapdoor's td_{ID} from the receiver's private key, sk_{ID}.
- IBEET.Test $(td_{ID}, C, td_{ID'}, C')$: This method receives as input two pairs of ciphertexts /trapdoor $(td_{ID'}, C')$ and (td_{ID}, C), then outputs either 1 or 0 depending on whether C and C' were produced on the same message.

Computational Assumptions
These presumptions provide information about how difficult it would be to crack the encryption standard using either an identification scheme or an attribute scheme. Let's take into consideration two identically ordered cyclic groups q, G_1 and G_2, in order to explain these presumptions. P is a generator of G_1, and the bilinear mapping $e: G_1 \times G_1 \rightarrow G_2$ is valid. The following are the presumptions; in addition, they can be modified for greater security:
(i) Computational Diffie-Hellman (CDH) problem: Computing P^{xy} in G_1 is difficult if $\langle P, P^x, P^y \rangle$ for some $x, y \in Z_q{}^*$.
(ii) Decisional Diffie-Hellman (DDH) problem: It is difficult to anticipate $P^{xy} \in G_2$ from $P' \in G_2$ if $\langle P, P^x, P^y \rangle$ for some unknown $x, y \in G_1$.
(iii) Bilinear Diffie-Hellman(BDH) problem: Computing $e(P, P)xyz \in G_2$ is difficult if $\langle P, P^x, P^y \rangle$ for some $a, b, c \in Z_q{}^*$.

Bilinear Groups
Let g be a generator of G_1, if G_1 and G_2 are two cyclic groups of order q, that is cyclical to create bilinear groups. The symbol notation used throughout the study is displayed in **Table 1**. From G_1 to G_2 a bilinear mapping can be described as

Table 1. Description Table.

Symbol	Name description
Z	Finite group of prime order
G	Cyclic group of prime order
U, V, W and a	Generator of group A
e: P ⟶ Q	Cyclic group bilinear mapping P to Q
C	Cipher text
M	Message

Table 1.	**Continue**
PP	Public parameters
α, g, r	Random numbers
G_1	Elliptic curve group
GT	Multiplicative group
Ik	IBE private key
l	Level of authentication

$$\text{e: } G_1 \times G_1 \to G_2 \tag{1}$$

The characteristics of this bilinear mapping are as follows:
(i) Bilinearity: $e(xU; yV) = e(U,V)^{xy} \forall U, V \in A_1$, and $x, y \in Z_q$
(ii) Nondegeneracy: let $e' = e(U,V)$, and then, $\exists e'$: $e' \neq 1$. A bilinear group will not be bilinear if all of its mappings are identical to 1; i.e., if $e(U,V) = 1 \forall U, V \in G_1$, G_1 will then be referred to as a linear group.
(iii) Computability: $e(U;V)$ can be calculated using the effective algorithm $U, V \in G$.

Such that

$$\begin{aligned} &e(U+V,W) = e(U,W) * e(V,W) \forall \mathrm{U}, V, W \in G_1. \\ &e(\mathrm{U}, \mathrm{V}+\mathrm{W}) = e(U,V) * e(V,W) \forall U, V, W \in G_1. \end{aligned} \tag{2}$$

IV. PROPOSED IBEET SECURITY SCHEME

Here, we first provide a thorough analysis of the IBEET system's physical components, which is based on the IBE scheme put forth by Lewko and Waters [25]. We utilize a bilinear group with a prime order of $N = u_1 u_2 u_3$, and the element of $\mathbb{Z}_N$ serves as the identity. The full security of our plan is then demonstrated in the SM.

Construction

The current generic IBEET approach [20] employs a one-time signature mechanism to enhance the system's security and double-encrypts data to achieve the encryption and testing function. Yet, our system only needs to encrypt using the same ID twice. The initial encryption immediately encrypts message M, so completing the encryption function. The second encryption consists of encrypting (R 1 (M), which is primarily used to perform the equality test and correctness verification of the decrypted message. Additionally, even if we possessed (R 1 (M))and u, we could not get R 1 (M) due to the difficulty of solving the discrete logarithm issue. Hence, the second encryption does not disclose M. Hence, unlike the system in [20], our approach does not require any additional computations to boost security.

The specific scheme design is as follows:

Setup. The input is a security parameter $Ik \in \mathbb{Z}^+$, and the output is the public parameter $PK = (N, \alpha, g, r, e, e(g,g)^{\mu_1}, e(g,g)^{\mu_2}, R_1, R_2)$.

The specific meaning is as follow:

- G is a multiplicative group, G_T is a cyclic group and their order is N. G_{ui} represents the subgroup of group G of order u_i.
- $N = u_1 u_2 u_3$, where u_1, u_2, u_3 denote three different prime numbers.
- e: $G \times G \to G_T$ is a bilinear map.
- R_1: $G_T \to \mathbb{Z}_N$ and R_2: $G_T \to G_{p_1}$ are two collision-resistant hash functions.
- $\alpha, g, r \in G_{u_1}, \mu_1, \mu_2 \in \mathbb{Z}_N$, and they are random.
- The master key msk consists of μ_1, μ_2, and the generator of group $G_{u\mu}$.

Extract. The inputs are an identity ID and msk, and the output is the following private key $sk_{ID} = \left(sk_{ID,1}, sk_{ID,2}, sk_{ID,3}, sk_{ID,4}\right)$ for ID where $s_1, s_2 \in \mathbb{Z}_N, U_3, U_3' \in G_{u_2}$ are chosen at random: $\mathbb{Z}_N, U_3, U_3' \in G_{u_3}$ are chosen at random:

$$\begin{aligned} sk_{ID,1} &= g^{s_1} U_3 \\ sk_{ID,2} &= g^{\mu_1} (\alpha^{ID} r)^{s_1} U_3' \\ sk_{ID,3} &= g^{s_2} U_3 \\ sk_{ID,4} &= g^{\mu_2} (\alpha^{ID} r)^{s_2} U_3' \end{aligned} \tag{3}$$

Encrypt. The inputs are ID and a message M, and the output is the following ciphertext $C = (C_a, C_\mathrm{b}, C_\mathrm{c}, C_\mathrm{d})$ where $\vartheta \in \mathbb{Z}_N$ is chosen at random:

$$\begin{aligned} C_a &= Me(g,g)^{\mu_1\vartheta}, \\ C_\mathrm{b} &= (\alpha^{ID}r)^{\vartheta}, \\ C_\mathrm{c} &= g^{\vartheta}, \\ C_\mathrm{d} &= p^{\vartheta R_1(M)} R_2\big(e(g,g)^{\mu_2\vartheta}\big). \end{aligned} \tag{4}$$

Decrypt. The algorithm accepts as inputs sk ID and C encrypted with ID, computes a message M' using the orthogonality of subgroups of group G and the bilinearity of the bilinear map, and then outputs the message. The procedure for calculating is as follows:

$$\begin{aligned} \frac{e(sk_{ID,2},C_\mathrm{c})}{e(sk_{ID,1},C_\mathrm{b})} &= \frac{e(g,g)^{\mu_1\vartheta} e(\alpha^{ID}r,g)^{s_1\vartheta}}{e(\alpha^{ID}r,g)^{s_1\vartheta}} \\ &= e(g,g)^{\mu_1\vartheta} \end{aligned} \tag{5}$$

$$\frac{C_\mathrm{a}}{e(g,g)^{\mu_1\vartheta}} = M' \tag{6}$$

It's worth noting that we need to verify the validity of the message M', the process is as follows:

$$\begin{aligned} P &= \frac{e(sk_{ID,4},C_\mathrm{c})}{e(sk_{ID,3},C_b)} \\ W &= \frac{C_\mathrm{d}}{R_2(P)} \\ e(W,g) &= e(p,C_\mathrm{c})^{R_1(M')} \end{aligned} \tag{7}$$

If $e(W,g) = e(p,C_c)^{R_1(M')}$, then output M', otherwise output $\perp$.

Trapdoor. The inputs are ID and sk_{ID} and the output is a trapdoor $td_{ID} = (td_{ID}, td_{ID'})$ that is formed as:

$$\begin{aligned} td_{ID} &= sk_{ID,3} = g^{s_2}U_3, \\ td_{ID'} &= sk_{ID,4} = g^{\mu_2}(\alpha^{ID}r)^{s_2}U_3''. \end{aligned} \tag{8}$$

Test. The algorithm accepts as input a ciphertext C encrypted with an identity ID, the trapdoor td ID for the identity ID', and a ciphertext C' encrypted with an identity ID', the trapdoor td (ID') for the identity ID'. The algorithm then verifies whether the corresponding message M of C is equal to the corresponding message M' of C', and outputs the result. The procedure for calculating is as follows:

To begin, the algorithm determines the parameters in the following manner:

$$\begin{aligned} E &= \frac{e(td_{\mathrm{ID},2},\mathrm{C},2)}{e(td_{\mathrm{ID},1},C,1)} = e(g,g)^{\mu_2\vartheta} \\ P &= \frac{C,3}{R_2(E)} = \alpha^{\vartheta R_1(M)} \\ E' &= \frac{e\left(td_{\mathrm{ID}',2},C',2\right)}{e\left(td_{\mathrm{ID}',1},C',1\right)} = e(g,g)^{\mu_2\vartheta'} \\ P' &= \frac{C',3}{R_2(E')} = \alpha^{\vartheta' R_1(M')} \end{aligned} \tag{9}$$

Then it verifies if $e(\mathrm{C},2,P') = e(C',2,P)$ is true. If it is true, M is equal to M', otherwise, they are not equal.

Precision

Here, we confirm the accuracy.

Validity of the Decryption Algorithm.

$$\begin{aligned} P &= \frac{e\big(sk_{ID,4},C_\mathrm{c}\big)}{e\big(sk_{ID,3},C_\mathrm{b}\big)} \\ &= \frac{e(g,g)^{\mu_2\vartheta} e(\alpha^{ID}r,g)^{s_2\vartheta}}{e(\alpha^{ID}r,g)^{s_2\vartheta}} \\ &= e(g,g)^{\mu_2\vartheta} \\ \mathrm{W} &= \frac{C_\mathrm{d}}{R_2(e(g,g)^{\mu_2\vartheta})} = \alpha^{\vartheta R_1(M)} \\ e(W,g) &= e\big(\alpha^{\vartheta R_1(M)},g\big) = e(\alpha,g)^{\vartheta R_1(M)} \end{aligned}$$

$$\mathrm{e}(\alpha, C_c)^{R_1(M')} = e\left(\alpha, g^{\vartheta}\right)^{R_1(M^{\vartheta})} = e(\alpha, g)^{\vartheta R_1(M^{\vartheta})}. \tag{10}$$

So, if $e(W, g) = e(\alpha, C_c)^{R_1(M')}$, then $M' = M$.

Correctness of Test Algorithm.

$$\begin{aligned} e\left(C_{,2}, P'\right) &= e\left(g^{\vartheta}, \alpha^{\vartheta_\mu} R_1(M')\right) \\ &= e(g, \alpha)^{\vartheta \vartheta_n R_1(M_n)} \\ e\left(C'_{,2}, \mathrm{P}\right) &= e\left(g^{\vartheta_\mu}, \alpha^{\vartheta} R_1(\mathrm{M})\right) \\ &= e(g, \alpha)^{\vartheta^{\mathrm{n}} \vartheta R_1(\mathrm{M})}. \end{aligned} \tag{11}$$

So if $e\left(C_{,2}, P'\right) = e\left(C'_{,2}, \mathrm{P}\right)$, then $\mathrm{M} = M'$, otherwise $M \neq M'$.

Security

First, we present the complexity presumptions that are required for the proof. These suppositions are comparable to those made by [25]. These presumptions are constant regardless of how many questions an adversary poses. The subgroup decision issue in assumption 1 has the order determined by the product of three different prime numbers. Additionally, Lewko and Waters demonstrated in Appendix A of [25] that these assumptions are true for the general group model if it is challenging to compute a nontrivial factor for the group order.

Assumption 1. (Subgroup decision problem for three primes).
We define the distribution as follows, where $\mathcal{G}$ represents a group generator:

$$\begin{aligned} \mathrm{G} = \quad & (N = u_1 u_2 u_3, G, G_T, e) \overset{D}{\leftarrow} \mathcal{G}, g \overset{D}{\leftarrow} G_{u_1}, \\ & Z_1 \overset{D}{\leftarrow} G_{u_3}, \\ X = \quad & (G, g, Z_1), T_1 \overset{D}{\leftarrow} G_{u_1 u_2}, T_2 \overset{D}{\leftarrow} G_{u_1}. \end{aligned} \tag{12}$$

The definition of the advantage that Assumption 1 is broken by an algorithm $\mathcal{A}$ is as follows: $Adv1_{\mathcal{G},\mathcal{A}}(\mathrm{I}k) := |\Pr[\mathcal{A}(X, T_1) = 1] - \Pr[\mathcal{A}(X, T_2) = 1]|$.

It can be noticed that T_1 is an element of $G_{u_1 u_2}$, so it can be seen as the product of the elements in G_{u_1} and G_{u_2}. And these elements are called the "G G_{u_1} part of T_1 " and the "GG_{u_2} part of T_2 " respectively. This nomenclature is going to be used in the proof.
In addition, we define $\mathcal{G}$ satisfies Assumption 1 if for polynomial time algorithm $\mathcal{A}$, $Adv1_{G,\mathcal{A}}(\mathrm{I}k)$ is negligible.

Assumption 2. We give the following definition of the distribution, where $\mathcal{G}$ is a group generator:

$$\begin{aligned} \mathbb{G} = \quad & (N = u_1 u_2 u_3, G, G_T, e) \overset{D}{\leftarrow} \mathcal{G}, g, P_1 \overset{D}{\leftarrow} G_{u_1}, \\ & Q_1, Q_2 \overset{D}{\leftarrow} G_{u_2}, Z_1, Z_2 \overset{D}{\leftarrow} G_{u_2} \\ X = \quad & (\mathbb{G}, g, P_1 Q_1, Z_1, Q_2 Z_2), T_1 \overset{D}{\leftarrow} G, T_2 \overset{D}{\leftarrow} G_{u_1 u_2}. \end{aligned} \tag{13}$$

The definition of the advantage that Assumption 2 is broken by an algorithm $\mathcal{A}$ is as follows:

$$Adv2_{G,A}(\mathrm{I}k) := |\Pr[\mathcal{A}(X, T_1) = 1] - \Pr[\mathcal{A}(X, T_2) = 1]|. \tag{14}$$

If Assumptions 1, 2, and Collision-resistant hash function, then both ciphertexts and semi-functional private keys are unable to decrypt semi-functional ciphertexts since they are only partially functional, hence it is equally probable that each message will be encrypted. Hence, the likelihood of an attacker accurately guessing the message M is $\frac{1}{N}$. This chance is small, hence the attacker's advantage in breaking the IBBET system is insignificant, as the value of M is concealed with an overwhelming likelihood. The SM is therefore OW-ID-CCA secure with our IBEET protocol.

V. PROPOSED ADVANCED IBEET ALGORITHM

Let G represent a prime order p group. Bilinear map formed by Group G is expertly computed into G_1. Let g is the generator of group G, and as $e: G \times G_1 \rightarrow G_2$ is the formulation of the bilinear map representation of G_1. The group size is determined by a security parameter, and each identity is represented by four strings, each of length n.

$$\mathrm{ID}' = (\mathrm{ID}_1, \mathrm{ID}_2, \mathrm{ID}_3 \cdots . \mathrm{ID}_n)' \quad (15)$$

From random length ID' bit strings, fixed length n bit strings can be created using the collision-free hash function. The proposed IBEET algorithm includes the following phases:

Setup Phase. Set the system parameters. From Z_p, a secret is randomly selected. Choose a randomly generated number g from G such that $g \in G$, fix the value $gl = g^{\mu}$, and choose g_2 at random from G. Choose two random numbers, u and n-length vector, such that $\alpha' \in \mathrm{G}$ and $U = \{\alpha_i\}$, after selecting all the authority parameters. Finally, the public parameters, g, g_1, g_2, α' and U are made available, along with the master key g_2^{μ}.

Generation Phase. Assuming that β represents a user's n-bit string identity, the, i^{th} bit of β is indicated by β_i, and $V \subseteq \{1, \cdots, n\}$, denotes the set of all i for which $\beta_i = 1$. V is split into two parts, namely $V = \{\beta_1, \beta_2, \cdots, \beta_m\}$ and $\{\beta_{\vartheta_1}, \beta_{\vartheta_2} \ldots, \beta_{\vartheta_m}\}$, therefore $m + \vartheta_m = n$ where β_{ϑ_i} stands for a random value that is introduced to the proposed approach to increase security. The private key corresponding to identity β is obtained by selecting a random value.

$$d'_{\beta} = \left(g_2^{\mu}(\alpha' \textstyle\prod_{i \in V} \beta_i)^{\vartheta} \cdot g^{\vartheta}\right)' \quad (16)$$

$\mathrm{U}' = \{\alpha_1, \alpha_2 - \alpha_n\}'$ and $\mathrm{V}' = \{\beta_1, \beta_2 - \cdots - \beta_m\}'$ such that

Table 2. A Comparison of the Suggested Approach with the Encryption Phase of the Water's and 5G Algorithm

Encryption phase	Water's IBE	5G construction	Proposed approach
Number of G group operation	$n/1$ (avg case or n (worst case)	$m/2$ (avg case or m (worst case)	$m'/2$ (avg case or m' (worst case)
Number of G_1 group operations	1	1	1
No of exponentiation in G	2	2	2
No of exponentiation in G_1	1	1	1
Size of the generated key	Large (relative to n)	Small (relative to m)	Very small (relative to m)
Polynomial interpolation	No	Yes	Yes
The group operation formula for key generation	$\alpha' \prod_{i \in V} \alpha_i$	$\alpha' \prod_{i \in V} \beta_i$	$\left(\alpha' \prod_{i \in V} \beta_i\right)'$

The proposed decryption phase does not require any additional optimization in context of **Table 2**, but a higher level of security is still attained due to the usage of the Lagrange coefficient. By concealing the original identity, generating keys using only a part of the original identity, security is obtained. The most important thing to remember is that, although using the same decryption technique as Water's IBE, our suggested solution is far more secure since, even if one knew the key decryption technique (such as key generator), they could never predict which identity key has been generated [26].

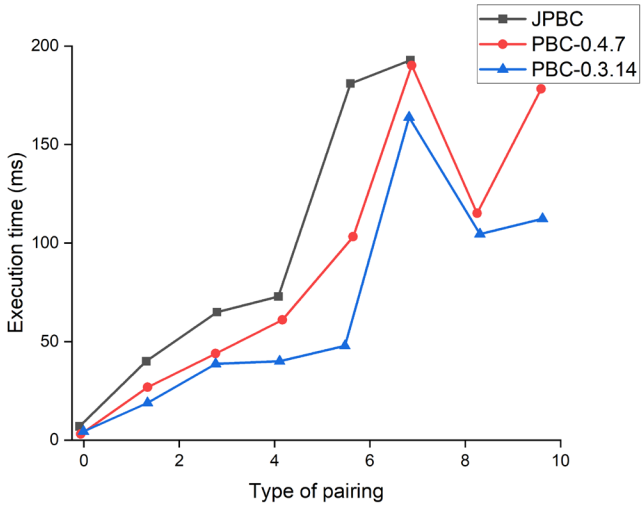

Fig 3. Bilinear Mapping Execution Time Using JPBC and PBC Versions

Table 3. Comparison of the Suggested Method During the Decryption Phase with the 5G Method.

Decryption phase	5G construction	Proposed 6G
Group operation in G_1	1	1
Bilinear map computation	2	2
Inversion in G_1	1	1

$m < n$. Now, generate a polynomial function using the Lagrange coefficient method and perform polynomial interpolation. We can conceal certain β values that can be effectively reconstructed from the available data points with the help of polynomial interpolation. For the suggested strategy, the polynomial equation is

$$U(a) = \frac{(a-a_1)(a-a_2)-\cdots--(a-a_n)}{(a_0-a_1)(a_0-a_2)---(a_0-a_n)} b_0 + \frac{(a-a_0)(a-a_1)-\cdots-(a-a_{n-1})}{(a_1-a_0)(a_1-a_2)---(a_1-a_n)} b_1 - \cdots - \cdots \frac{(a-a_1)(a-a_2)-\cdots-(a-a_n)}{(a_n-a_0)(a_n-a_1)-\cdots-(a_n-a_{n-1})} b_n \quad (17)$$

Lagrange coefficient is

$$\Delta_{i,b}(a) = \sum_{i=0,Ik\in V}^{n} \left(\prod_{0<i<n,j\neq i} \frac{a-a_j}{a_i-a_j} \right) b_{Ik'} \quad (18)$$

where $a = \alpha_i$ and $b = \beta_{Ik}$.

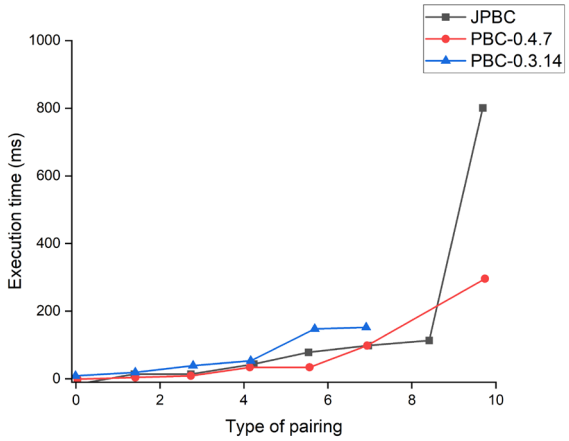

Fig 4. Performance of JPBC better than PBC Versions

For each user identity, the random set α_i is created once, and the same α_i value is used to construct the Lagrange coefficient for each identity. The usage of m-terms of identification value by the authority prevents a challenger from learning the true identity of an authorized user. As a result, it will be challenging to retrieve or deduce the key created for a specific ID. Now let's consider all of the user identity and U values were the same. In this scenario, the error produced by $U(a)$ would be 0, meaning that the challenger would be unable to deduce anything from the key.

Encryption Phase. Assume that " c " is a random number selected from Z_p and message $M(M \in G_1)$. Equation (19) can be used for encryption for some identities β.

$$C' = (e(g_1, g_2)M, g^c, (u' \prod_{i=V} \beta_i)^c)' \quad (19)$$

Decryption Phase. Assume that the cipher text $C' = (C_a, C_b, C_c)$ is appropriate for message M with user identity β. Then, using the $d_V = (d_1, d_2)$ from the Equations (20)–(23), the cipher string C' may be decrypted:

$$= \left((e(g_1, g_2)^c M) \frac{e\left(g^{\vartheta}, (\alpha' \prod_{i=V} \beta_i)^c\right)}{e\left(g_2^{\alpha}, (\alpha \prod_{i=V} \beta_i)^{\vartheta}, g^c\right)} \right)' \quad (20)$$

$$= \left((e(g_1, g_2)^c M) \frac{e\left(g, (\alpha' \prod_{i=V} \beta_i)^{\vartheta c}\right)}{e(g_1, g_2)^c e\left((\alpha' \prod_{i=V} \beta_i)^{\vartheta c}, g\right)} \right)' \quad (21)$$

$$= \left((e(g_1, g_2)^c M) \frac{e\left(g,(\alpha' \prod_{i=V} \beta_i)^{\vartheta c}\right)}{e(g_1,g_2)^c e\left(g,(\alpha' \prod_{i=V} \beta_i)^{\vartheta c}\right)} \right)' \quad (22)$$

$$= M' \quad (23)$$

VI. RESULTS AND DISCUSSIONS

IBEET with type A pairings can be performed with one of the efficient libraries for creating bilinear mapping is the Java pairing-based cryptography (JPBC) library. Since Type A curve pairing uses the super single curve $Q^2 = P^3 + P$, it is the optimal curve for cryptosystems. The effectiveness of the suggested strategy is assessed using Ubuntu Intel Core ^{TM}i7 − 3770CPU with 2 GB RAM and a 3.4GHz processor. Compared to other pairing types, a fastest pairing technique is type A pairing.

Fig 3. displays the pairing's execution time as being reduced. **Table 3** shows comparison of the suggested method in bilinear mapping.

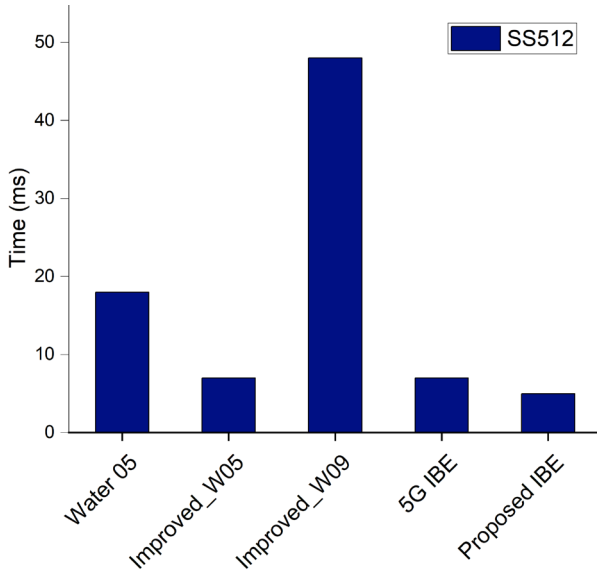

Fig 5. Key Generation Phase Timing Comparison Graph

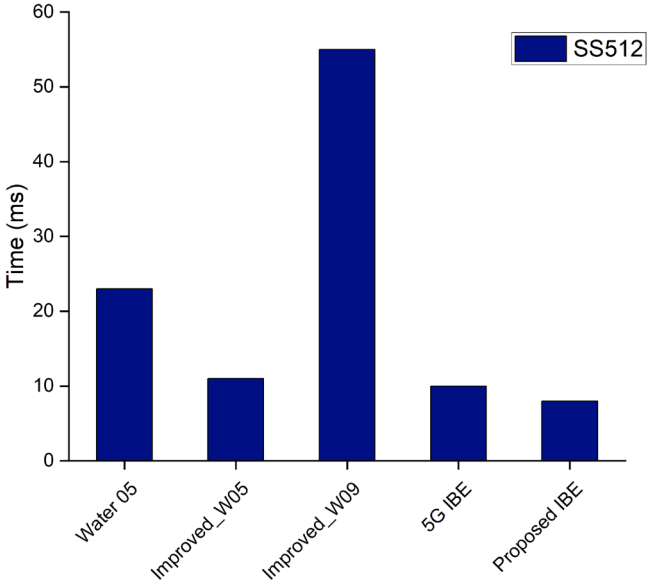

Fig 6. Encryption Phase Timing Comparison Graph

computationally challenging pairing due to logarithmic calculations. With 12 pairings, type "g" pairing is too slow to be useful, thus type "a" curves are typically utilized in cryptographic computing.

JPBC library is a java-based pairing technique that may be used on systems running Windows and Linux (Ubuntu). Performance of the JPBC library and PBC versions vary for the same system configuration. For pairing implementation at the preprocessing stage, the graph is obtained. JPBC versions perform far better than PBC versions.

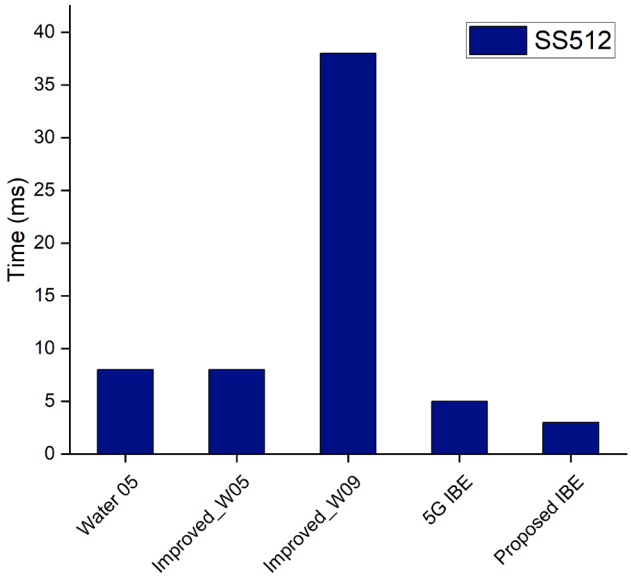

Fig 7. Decryption phase timing comparison graph

It is clear from **Fig 4** that JPBC outperforms PBC in terms of run-time performance. Although the IBE with equality test has a very effective toolkit for implementing the IBE technique on Ubuntu-based systems, utilizing the JPBC library to execute the code more quickly is preferable to using the standard PBC library. Here, graphs relating to the execution time of the suggested method are shown and contrasted with others. On the other hand, pairing cryptography based on Java is used to implement the suggested framework. In the critical generation phase of the SS512 (type A) curve, the computation times for suggested IBE, 5G IBE, improved W09, improved W05, and Water 05 are shown in **Fig 5**. It is clear that using the proposed method results in faster key creation than using other methods. Because we are utilizing a more sophisticated function for key generation, which increases the security of the model.

Fig 6. illustrates how the suggested method, which use the SS512 curve for encryption, is more effective and requires less calculation time during the encryption phase. Since for the encryption, we use equation (5), which is simple to calculate, the suggested encryption method is more computationally efficient. The proposed method, which implements the decryption using the SS512 curve, is more effective and requires less calculation time in the decryption phase, as displayed in **Fig 7**. For the decryption, we use **Equ (20)–(23)** which is simple to execute, the suggested decryption strategy is more computationally efficient.

VII. CONCLUSION AND FUTURE WORK

Identity-based encryption is the most used user identification and authorization approach in the cryptography field (IBE). IBEET is a crucial cryptographic approach for searching encrypted cloud data. It can decrypt and compare ciphertexts to determine whether or not the associated messages are identical. There is just a basic IBBET scheme that provides security for the SM, but its effectiveness is low. Using the JPBC package, we applied the IBE approach with an equality test to ensure full security in the SM. And in order to avoid the misuse of trapdoors, we have modified our method such that each ciphertext corresponds to a unique trapdoor. This study presents the enhanced IBE approach with equality testing in contrast to the competitive methodology. Using the Lagrange coefficient, which is a polynomial interpolation function, to disguise the user's identity is one of the most important components of the recommended strategy. Furthermore, our methods do not require additional calculations to improve security, hence under same conditions, our schemes are more efficient than the generic system. On the basis of the subgroup choice issue, we demonstrate that our systems provide OW/IND-ID-CCA security for the SM. Thus, our future efforts will focus on enhancing the efficacy of our programmes.

Data Availability Statement

There is no data associated with this article.

Conflict of Interest

The authors declare that there is no conflict of interest.

Funding
No funding was received to assist with the preparation of this manuscript.

Ethics Approval and Consent to Participate
The research has consent for Ethical Approval and Consent to participate.

Competing Interests
There are no competing interests.

References

[1]. K. Lee and J. Park, "Identity-based revocation from subset difference methods under simple assumptions," IEEE Access., vol. 7, pp. 60333-60347, 2019.
[2]. A. Shamir, "Identity-based cryptosystems and signature schemes," Workshop on the Theory and Application of Cryptographic Techniques (CRYPTO), 2000.
[3]. R. K. Gupta and R. K. Pateriya, "Balance resource utilization (BRU) approach for the dynamic load balancing in cloud environment by using AR prediction model," Journal of Organizational and End User Computing (JOEUC), vol. 29, no. 4, 2017.
[4]. C. Mukundha and B. Chandar, "Identity based encryption in cloud computing with outsourced revocation using Ku-CSP," IOSR Journal of Engineering, vol. 8, no. 8, pp. 12-21, 2018.
[5]. D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in International conference on the theory and applications of cryptographic techniques, pp. 506–522. Springer, 2004.
[6]. G. Yang, C. H. Tan, Q. Huang, and D. S. Wong, "Probabilistic public key encryption with equality test," in Cryptographers' Track at the RSA Conference, pp. 119–131. Springer, 2010.
[7]. K. Zhang, J. Chen, H. T. Lee, H. F. Qian, and H. x. Wang, "Efficient public key encryption with equality test in the standard model," Theoretical Computer Science, vol. 755, pp. 65–80, 2019.
[8]. S. Ma, "Identity-based encryption with outsourced equality test in cloud computing," Information Sciences, vol. 328, pp. 389–402, 2016.
[9]. T. Wu, S. Ma, Y. Mu, and S. K. Zeng, "Id-based encryption with equality test against insider attack," in Australasian Conference on Information Security and Privacy, pp. 168–183. Springer, 2017.
[10]. H. T. Lee, H. X. Wang, and K. Zhang, "Security analysis and modification of id-based encryption with equality test from acisp 2017," in Australasian Conference on Information Security and Privacy, pp. 780–786. Springer, 2018.
[11]. S. Alornyo, A. E. Mensah, and A. O. Abbam, "Identity-based public key cryptographic primitive with delegated equality test against insider attack in cloud computing," International Journal of Network Security, vol. 22, no. 5, pp. 743–751, 2020.
[12]. S. Alornyo, M. Asante, X. Hu, and K. K. Mireku, "Encrypted traffic analytic using identity based encryption with equality test for cloud computing," in 2018 IEEE 7th International Conference on Adaptive Science & Technology (ICAST), pp. 1–4. IEEE, 2018.
[13]. F. Wu, W. Yao, X. Zhang, Z. M. Zheng, and W. H. Wang, "Identity based privacy information sharing with similarity test in cloud environment," in International Conference on Cloud Computing and Security, pp. 69–78. Springer, 2018.
[14]. H. P. Qu, Z. Yan, X. J. Lin, Q. Zhang, and L. Sun, "Certificateless public key encryption with equality test," Information Sciences, vol. 462, pp. 76–92, 2018.
[15]. R. Sivaguru, G. Abdulkalamazad, G. Babu, K. R. Leakashri, R. Sathya Priya, N. Subha, "A Composed Work on Internet of Things And Its Applications", vol.2, no.2, pp. 038-045, January 2022. doi: 10.53759/181X/JCNS202202007.
[16]. G. Leelavathi, K. Shaila, and K. R. Venugopal, "Hardware performance analysis of RSA cryptosystems on FPGA for wireless sensor nodes," International Journal of Intelligent Networks, vol. 2, pp. 184–194, 2021, doi: 10.1016/j.ijin.2021.09.008.
[17]. Y. J. Liao, H. J. Chen, W. Huang, R. Mohammed, H. T. Pan, and S. J. Zhou, "Insecurity of an ibeet scheme and an abeet scheme," IEEE Access, vol. 7, pp. 25087–25094, 2019.
[18]. H. B. Li, Q. Huang, S. Ma, J. Shen, and W. Susilo, "Authorized equality test on identity-based ciphertexts for secret data sharing via cloud storage," IEEE Access, vol. 7, pp. 25409–25421, 2019.
[19]. M. Ramadan, Y. J. Liao, F. G. Li, S. J. Zhou, and H. Abdalla, "Ibeet-rsa: Identity-based encryption with equality test over rsa for wireless body area networks," Mobile Networks and Applications, vol. 25, no. 1, pp. 223–233, 2020.
[20]. Y. H. Ling, S. Ma, Q. Huang, R. Xiang, and X. M. Li, "Group id-based encryption with equality test," in Australasian Conference on Information Security and Privacy, pp. 39–57. Springer, 2019.
[21]. S. Alornyo, Y. Zhao, G. Zhu, and H. Xiong, "Identity based key-insulated encryption with outsourced equality test.," Int. J. Netw. Secur., vol. 22, no. 2, pp. 257–264, 2020.
[22]. H. T. Lee, S. Ling, J. H. Seo, H. X. Wang, and T. Y. Youn, "Public key encryption with equality test in the standard model," Information Sciences, vol. 516, pp. 89–108, 2020.
[23]. L. Qin, Z. Cao, and X. Dong, "Multi-receiver identity-based encryption in multiple PKG environment," in IEEE GLOBECOM 2008 - 2008 IEFE Global Telecommutications Conference, Pp. 1-5, New Orleans, LA, USA, 2008.
[24]. A. Sudarsono, M. Yultana, and H. A. Darwito, "A secure data sharing using identity-based encryption scheme for ehealthcare system," in 2017 3rd International Conference on Science in Information Techalogy (ICSITech). Pp. 1-9, Bandung, Indonesia, 2017.
[25]. R. K. Gupta, K. K. Almuzaini, R. K. Pateriya, K. Shah, P. K. Shukla and R. Akwafo, "An improved secure key generation using enhanced identity-based encryption for cloud computing in large-scale 5G." Wireless Communications and Mobile Computing, 2022.
[26]. S. V. Anand and S. P. S. Kumar, "A modular data link layer (M-DALL) for NEXT GEN mobile terminals enabling wireless aware applications: a platform independent software design," in 2010 Global Mobile Congress, Shanghai, China, 2010.
[27]. A. Lewko and B. Waters, "New techniques for dual system encryption and fully secure hibe with short ciphertexts," in Theory of Cryptography Conference, pp. 455–479. Springer, 2010.
[28]. M. Gupta, K. K. Gupta, and P. K. Shukla, "Session key based fast, secure and lightweight image encryption algorithm," Multimedia Tools and Applications, vol. 80, no. 7, pp. 10391– 10416, 2021.
[29]. Rimma Padovano, "Critical Analysis of Parallel and Distributed Computing and Future Research Direction of Cloud Computing", Journal of Computing and Natural Science, vol.1, no.4, pp. 114-120, October 2021. doi: 10.53759/181X/JCNS202101017.