Journal of Informatics and Web Engineering
Vol. 4 No. 1 (February 2025) eISSN: 2821-370X

Implementing Identity-based Signature Schemes for Secure Data Transfer in Cloud Computing Environments

Paul Osinuga[1], Ji-Jian Chin[2]*, Terry Shue Chien Lau[3]
[1,2]School of Engineering, Computing and Mathematics, University of Plymouth, Drake Circus, Plymouth PL4 8AA, United Kingdom.
[3]Faculty of Computing and Informatics, Multimedia University, Jalan Multimedia, 63100 Cyberjaya, Malaysia.
corresponding author: (ji-jian.chin@plymouth.ac.uk; ORCiD: 0000-0001-9809-6976)

Abstract - In this paper, we present the implementation of the Cha-Cheon Identity-Based Signature (IBS) scheme to enhance secure data transfer in cloud computing environments. Cloud computing rely on traditional Public Key Infrastructure (PKI) systems, which is burdened by certificate management infrastructure. The primary focus of this research to simplify key and certificate management by leveraging identity-based elliptic curve cryptography (ECC) within the Cha-Cheon IBS framework. We show that the proposed IBS solution integrates seamlessly with Amazon Web Services (AWS), utilizing services like S3 for secure data storage and KMS for key management. By applying ECC, the Cha-Cheon scheme achieves efficient cryptographic operations with smaller key sizes, resulting in reduced computational overhead, faster key generation, signature creation, and verification times compared to RSA-based systems. We conducted extensive performance evaluations to compare the Cha-Cheon IBS scheme with traditional PKI-based systems. The results demonstrate that our implementation significantly outperforms RSA in terms of key generation, encryption, and signature verification times, especially under increased user loads and data sizes. Moreover, the security analysis confirms the robustness of the Cha-Cheon IBS against key compromise, offering strong resistance to unauthorized access and key revocation issues. The scheme also scales efficiently as the number of users increases, making it ideal for large-scale cloud infrastructures. This research highlights the potential of IBS as a viable alternative to PKI systems, providing a more streamlined and efficient approach to secure data transfers in cloud environments.

Keywords— Cha-Cheon IBS, Cloud Security, Elliptic Curve Cryptography, Amazon Web Services, Public Key Infrastructure, Key Management

Received: 01 September 2024; Accepted: 25 November 2024; Published: 16 February 2025

1. INTRODUCTION

Cloud computing is a game-changer as it allows enterprises to store, compute, and move data with greater flexibility [1]. However, this convenience has come at the cost of increasing data security and privacy concerns [2]. Reliable and secure cryptography still has complex key management in the context of dynamic clouds [3]. This can result in

inefficiencies and the risk of cryptographic schemes getting more dangerous. Identity-based signature (IBS) schemes on the other hand have a simplified alternative in which there is no requirement for public key infrastructure (PKI) certificates, and it is very easy to manage keys by obtaining public keys from the identity of a user [4]. This property makes IBS ideal for the cloud where a fast and safe data exchange is needed [5].

There are a few roadblocks to the cloud adoption of IBS: Private keys in key escrow (ownership of the private keys by a trusted third party); Security and privacy issues [6]. Moreover, it has been hard to standardize IBS in relation with existing cryptographic implementations [7]. This study is trying to build a framework to solve all these issues with secure and efficient data transfers over the cloud.

The research questions of this study are as follows:

i. How can IBS schemes be effectively implemented in cloud environments?
ii. What are the key challenges in integrating IBS with the cloud?
iii. How does IBS compare to PKI in terms of performance and security?

Based on the research questions, the main goal of this research study is to create a scalable and secure framework for implementing IBS in cloud environments. This involves:

i. To analyze the current landscape of IBS schemes and their applicability in cloud environments.
ii. To develop a scalable, secure, and efficient IBS framework suitable for cloud computing environments.
iii. Comparing the proposed framework with traditional PKI-based systems in terms of performance and security.

Cloud computing offers significant benefits but poses challenges related to data security, privacy, and authentication [8]. IBS schemes can enhance security by deriving public keys from user identities, thus simplifying the key management process [9]. While IBS shows promise in cloud contexts, research in this area remains limited [10]. Existing studies have primarily focused on theoretical aspects or applications in other domains, such as mobile applications [11] [12] and the Internet of Things (IoT) [13]. This study aims to fill that gap by addressing the unique challenges presented by cloud environments, including multitenancy, resource dynamism, and legal compliance [14][15].

This research follows a mixed-method approach:

1. Data Collection: Gathering information from literature, case studies, and real-world cloud environments.
2. Data Analysis: Analyzing both qualitative and quantitative data to understand the challenges of implementing IBS in cloud environments.
3. Validation: Simulations and real-world experiments will be conducted to validate the proposed framework's performance, scalability, and security.

Upon successful completion, this research could greatly improve data security in cloud environments. By simplifying key management, IBS could become a more attractive option for organizations looking to enhance their data protection without the complexity of PKI[16]. Additionally, this work may inform policymakers and help standardize IBS practices across industries, thereby contributing to greater cybersecurity resilience. The findings could also inspire future innovations in cryptography and cloud security, strengthening trust in cloud-based operations.

2. LITERATURE REVIEW

2.1. Cloud Computing and Security Challenges

Cloud computing has changed the information technology world landscape and has ushered in new ways of data storage, data processing, and data transfer. This technological shift provides organizations in unprecedented ways of flexibility and expansion that enable them to cope with higher data volumes and more intricate processes more efficiently. Nonetheless, this transition also comes with considerable security risks. As outlined by [1], the very vast horizons of cloud computing have vulnerabilities such as compromised data integrity, poor authentication standards, and privacy intrusion, which are now standing at a different level of gravity. Also, since more institutions are using cloud applications for their core functions, further high risks bring wider prospects for security breaches damage. Such

vulnerabilities were pointed out by [8] who noticed that today, cloud computing environments require robust security mechanisms in order to deal with these issues. The requirement to fortify security control systems is not only for securing information but also for uninterrupted operations and the integrity of the cloud systems, prompting a need for industry players who use the technology to focus on its deployment for essential purposes.

2.2 Historical Background of the Development of Identity-Based Cryptography (IBC)

The term identity-based cryptography (IBC) was first used by Adi Shamir in 1984 [17]. It is a revolutionary development in computer science that allows multiple public key infrastructure (PKI) users to take place in an easy way. According to the revolutionary idea posed by Shamir, it is crucial to maintain contact with the organization by using the email address or any other unique ID as the public key that requires validation from an external agency. Thus, this process greatly eliminates the operational costs and the complexities of PKI systems, expediting the execution and deployment of cryptographic solutions [18]. The history of IBC is characterized by multiple successive schemes having a more efficient role than the previous ones. One of the first breakthroughs in this area was the proposal by [19] of the IBE scheme that combines fine-grained access control with stringent restrictions on who can access private information. This approach was especially useful in cases where such information is sensitive as one has to approach with respect to their roles and credentials, thus offering a more flexible approach to encryption.

Wang in [20] made another crucial enhancement to the capabilities of IBC when he developed a provably secure identity based encryption scheme which is based on cyclotomic fields. It made such claims on security more pronounced as there was a mathematical basis for such security in the encryption scheme which improved the possibilities of its use for the protection of sensitive data and communications. Besides, the research conducted by Ghuge et al. [21] exhibited that a multilayer identity based encryption scheme could be achieved and was useful in the cloud environment. This method addressed various facets of security such as the scope of data integrity and confidentiality from storage to transfer. They implemented a multilayered cryptographic approach which enabled them to achieve strong security objectives which are essential in the shared clouds that are mostly publicly exposed. These developments of identity-based cryptography have not only enriched the theoretical scope of IBC but have equally produced practical ones that can suit various contexts like the security of businesses or that of government data. The ever increasing and changing demands of IBC in the context of the digitally influenced environment necessitates constant research and practice and therefore remains a very important area for both researchers and practitioners in the field.

2.3 Recent Developments in Identity-Based Signature (IBS) Schemes

Considering the recent progress in IBS, it is evident that efforts have been made to increase security for cloud computing platforms. According to the studies done on laboratories for International Business the focus has been on the efficiency, security, and scalability of IBS technologies due to the challenges brought forth by the cloud infrastructure. In this field, a hierarchical identity-based encryption (IBE) scheme developed by Langrehr and Pan [22] is one of the most interesting advancements. Their work introduces a sophisticated multi-challenge security design which enables the system to cope with several challenges at the same time thus improving the effectiveness lower costs and strength of cryptographic processes. Such schemes are of great benefit in cases where the security provision must compose several protocols against different kinds of threats to cyber space at the same time. Further, Sun et al., [23] advanced this system with their revocable IBE scheme that incorporates server-aided ciphertext evolution. Computationally, this scheme makes it easy to revoke the keys that have been compromised without incurring too much overhead which is a significant weakness in cloud security, the key lifecycle management in responsive and scalable cloud environments.

Xuecheng and Lin [24] used the ideas of previous works to develop a more refined set of technologies for IBE with key revocation. Their work not only improved the efficiency of IBE itself but also concentrated heavily on the performance of the key revocation process. They needed the technology to work in a cloud setting, and it needed to work well.

This innovative tendency toward making IBS systems more secure, efficient, and adaptable clearly indicates the steps being taken to protect sensitive data in the cloud. These "IBS 2.0" systems are now secure, but they're almost too secure for the cloud, where the need for efficiency and adaptability on the part of cloud services makes "lightweight" solutions necessary; if solutions are too heavy or robust, they become roadblocks in the anything-goes universe of the cloud.

And so the cloud beckons us toward innovation in the direction of IBS systems that are lightweight but still secure, enabling us to do more with "less".

2.4 IBS Integration in Cloud Computing: Opportunities and Challenges

IBS systems are known to be a viable substitute and an improvement over more traditional Public Key Infrastructure (PKI) systems especially in the rapidly evolving and rather diverse sphere of cloud computing. Similarly, Patel and Rajan [9] have encouraged the use of IBS in cloud environments with the view to easing the process of certification besides strengthening the security structure. In contrast to PKIs where certificate browsers manage the distribution of certificates, IBS systems employ known identifiers such as the email address to produce the public key immediately. This approach not only eliminates the extrasensory expense of handling certificates but also shortens the time taken to authenticate since it is a critical component in the rapid operation within the cloud environment[16]. Nevertheless, these are using the IBS's strengths they can enhance their practical use and the theoretical research within the context of cloud computing infrastructures are still in their infancy. Current literature contributes less to the integration of IBS to cloud security systems but more to theories relating to IBS or its application to specific areas like mobile applications[11] [12], IoT and WSN [11]. Similarly, Zhang et al. [25] confirmed that, although theoretical models and lab-based demonstrative projects have brought positive results, there is still a need to investigate real-world cloud applications of the technology due to specific challenges like scalability and interoperability.

Another important concern is the interfacing of IBS to other existing cloud security initiatives that largely draw in well-developed PKI frameworks. The implementation of IBS must lead to drastic changes in the overall service security strategy, most likely reinventing all the security processes, services, and mechanisms after which may adversely influence the continuity of existing services and entail significant cost impact by Jensen et al. [26]. Furthermore, the security of IBS itself, including resistance to various cryptographic attacks, should be carefully evaluated in terms of cloud computing, which exposed users to various security threats and may lead to the leakage of important data [27]. Of course, it can be argued that with IBS more flexible and user-centered security options in cloud computing can be delivered. However, technology faces substantial technical and operational challenges before technology can be widely adopted into cloud security best practices. Substantial research effort is still required—if not so much on the cryptographic aspects, then on the real-world applicability to a wide variety of existing and emerging cloud systems. This will assist in building versatile and effective IBS solutions that can satisfy the need of present-day Internet-based services.

2.5 Multitenancy and Dynamic Resource Management

Cloud computing has recently attracted a lot of attention because it allows users to share a pool of configurable computing resources accessible through the internet. Nonetheless, IBS implementations face significant challenges typical of cloud settings, such as multitenancy and dynamism of resource provisioning. Multitenancy on the other hand simply means that many clients/tenants share a single physical system with their data completely segregated from other clients/tenants [28]. This architecture raises questions on how to achieve data isolation, access control or data confidentiality. Data segregation prevents one tenant from seeing data from another tenant; access control identifies who among the users can work with the resources available in the specific tenant space. Confidentiality ensures that one's information is protected from outside perception especially when under the same roof with other tenants. These challenges entail the need for highly developed IBS mechanisms that would guarantee the degree of data protection needed. According to Brown et. al. [15], it is often insufficient to approach these issues with traditional IBS ideas because the methods in question were initially developed to work with more static and monolithic systems. As a result, the development of effective new IBS solutions is required, designed to address the dynamic architectures of cloud computing systems. Another level of complication in dynamic resource management in cloud computing systems is added by IBS. Dynamic resource management involves building resource supply and demand models and making resource assignments in concurrent response to supply and demand variations [29]. Therefore, the IBS frameworks must allow for revising the resources and the mechanisms for completing the tasks without posing new security risks basement. This is because, when it comes to resources in the cloud the IBS framework has to adapt to the size necessary for the project while at the same time ensuring that there is still a heavy emphasis on security [30]. Additionally, IBS systems should be able to support the underlying cloud service models; software as a service, software platforms service, and infrastructure as a service to offer total cloud security from the application layer up to the physical layer.

2.6 Global Reach and Regulatory Compliance

Cloud computing has made significant impact on information systems since organizations can easily retrieve information and use application over the internet which can reach different parts of the world, thus facilitating globalization [31]. However, this global nature of cloud computing also comes with some issues to do with sovereignty and the legal issues around data sovereignty. At the technical level, the term data sovereignty means that data is governed by the laws and regulations of the country where it is physically hosted [32]. Trans border data transfer constitutes a challenge for IBS implementations across different countries due to complexities of meeting diverse regional regulations. Organizations have different rules governing how they collect, process, store, and transfer personal data all over the world: the GDPR in the EU, the CCPA in the USA, and the PIPEDA in Canada, for example European Parliament, 2016 [33] State of California Department of Justice, 2018 [34]; Office of the Privacy Commissioner of Canada, 2019 [35]. Noncompliance with these regulations attracts severe consequences such as fines, legal sanction, and compromised firm reputation. Hence, organizations need to ensure that their IBS solutions are not only technically optimized with all legal requirements of different countries and legal systems. To overcome these problems, it is necessary for organizations to develop and adopt an effective compliance system in the form of audits, risk analyses, and training to keep regulations in mind [14]. Furthermore, organizations can utilize cloud service provider's solutions for managing compliance, if contractual provisions regarding compliance management are sufficiently developed, and the organization has methods for monitoring such compliance [36]. Finally, to overcome issues of regulatory compliance in cloud computing, all the actors involved including the regulators of providers, providers themselves and customers must come up with the necessary tools and strategies which can ensure confidence, security and order in cloud computing deployment.

2.7 Practical Considerations: Key Management and System Integration

There are, therefore, a number of issues that practice vital when deploying an IBS in a cloud computing environment to enable the system to run effectively and securely. Two of the most critical of these are key management and system integration. Key management can be defined as the process of generation, distribution, secure storage and deletion of cryptographic key within an IBS. This is an important aspect of the design of any security system since loss of one or more of the keys may result in compromising the whole security of the system. In the case of the IBSs, the management is more challenging since everyone possesses their private key even if they are part of the same decentralized system[37]. To overcome this problem, methods of key management should be enhanced by constant key change, storage in secure places, and controlling access to keys. Furthermore, threshold cryptography or so called multiple computation can also be applied to strengthen security and reliability of the key management process [38].

The last, but not the least aspect concerned with the deployment of IBSs to cloud environments is system integration. Notably, some of the complexities include the fact that it is relatively difficult to implement IBSs to work in parallel when pre-existing cloud services and applications are being used or when engaging with pre-existing cloud-based applications or suites [39]. For example, when integrating IBS components with other cloud services it may be necessary to write some lines of code independently or use proprietary middleware software. Likewise, the use of IBS authentication mechanisms to extend access control to existing applications may require changes to the application code or parameters. The above challenges drawn from the field studies mean that proper approaches to system integration including analysis, design, testing and validation needs to be embedded. Also, involvement of experts with experience in both IBS and cloud computing will ensure smooth integration process and little risks or opportunities for slippage are realized [40]. By so doing, key practical issues concerning the management and integration of the IBS-based security architecture in cloud computing can be effectively addressed to support successful implementation in organizations.

3. RESEARCH METHODOLOGY

3.1 Introduction to The Cha-Cheon IBS Scheme

IBS schemes such as Cha Cheon scheme simplify cryptographic key management, by avoiding Public Key Infrastructure (PKI). The elliptic curve-based scheme is strong in security and efficient signing while using bilinear pairings which is very important for cloud environments.

3.2 Mathematical Foundations

3.2.1 Elliptic Curves

For elliptic curve cryptography to be efficient, the integral curve group must have a small order, which in turn severely limits its size. This means we must limit the size of our curve group if elliptic curve cryptography is to be efficient; but as the size of our curve group (and thus our order) is dictated by its integral curve group, we are severely limited (see Equation (1)).

$$y2 \equiv x3 + ax + b \pmod{p} \quad (1)$$

where a and b are coefficients satisfying: $4a3 + 27b2 \neq 0 \pmod{p}$. Since the curve is nonsingular, this makes sure of it.

3.2.2 Elliptic Curve Points

The curve equation will yield points on the curve E being the solutions (x, y), plus a special point at infinity, which is denoted by O. These points form an abelian group with Point Addition given points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$.

From this we see if P =/= Q then slope $\lambda = (y_2 - y_1) / (x_2 - x_1) \pmod{p}$

If P = Q (point doubling) then $(\lambda, \lambda^*) = (3\bar{x}^{12} + a) / 2. \pmod{p}$

The resulting point $R = (x_3, y_3)$ is calculated using: (or in the form of the polynomials) $x_3 = \lambda\text{^}2 - x_1 - x_2 \pmod{p}$ and $y_3 = \lambda(x_1 - x_3) - y_1 \pmod{p}$.

3.2.3 Scalar Multiplication

The multiplication of a point P by an integer k, is written as kP and in this case amounts to k copies of P plus P. ECC security requires this operation to be very crucial.

3.3 IBS Scheme

*Private Key Generation***:** Hashed identities of the users (e.g., email) is hashed, master key is multiplied with hashed identity, which gives private keys.

Signature Generation and Verification: Elliptic curve operations are used to create signatures, and verifying them depends on the public key, identity and elliptic curve information.

3.4 Security Advantages of ECC in IBS

Small Key Sizes: RSA keys, however, are large, and as greater security usually requires larger keys, merely exchanging larger RSA keys has little utility, while ECC offers strong security even with smaller keys. ECC-256 is equivalent to RSA-3072 for security, so it's ideal for constrained environments, for example.

Quantum Threat: Research on post quantum cryptography (e.g., lattice-based cryptography) to prevent quantum computer attacks, although it is vulnerable to; Shor's algorithm.
Non-Repudiation and Authentication: Secure communication without the need for a traditional PKI can be achieved by only legitimate private key holder signing messages.

3.5. Cha-Cheon IBS implementation

Elliptic Curve Setup: Here we define elliptic curve parameters like prime field, with generator P, curve coefficients, and base point G, all of which are key for cryptographic operations.

3.5.1 Key Generation

Choosing s from the prime field is done, so that it is equal to the master secret key. sP is the public key. In elliptic curve operations, elliptic curve private keys are derived based on user identities. The master secret key is maintained confidential, and the system parameters are published. Compute a public key Q given its identity ID, as well derive a private key from the master secret key.

3.5.2 Signature Process

Generation: Curve points and hash values are computed with the help of random integers, to get signature components r and s.

Verification: They verify the signature by using public keys, and elliptic curve parameters.

3.6 Cha-Cheon IBS in Cloud Computing

Figure 1 depicts the architecture diagram of Cha-Cheon IBS.

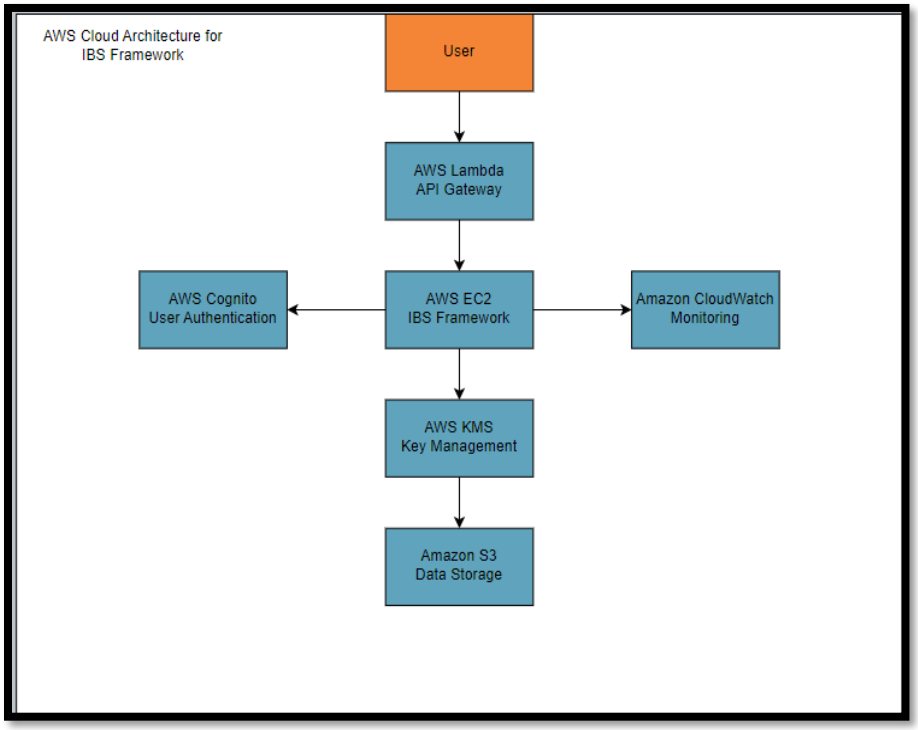


Figure 1. Architecture of The IBS Framework Deployed on AWS

3.6.1 Process Flow

User Registration: To register a user with PKG service via secure API (API Gateway). The user sends an identity string (e.g., email address or username.). The PKG securely delivers the user's private key to the user based on his

identity and the master secret key. For the public parameters of the user, we store it in S3 or a database (RDS or DynamoDB) and can be queried by verifiers.

3.6.2 Signature Generation

The running application (EC2 or Lambda), in the user's application, hashes the message to sign. A hardened message is hashed, and the user signs the hashed message with their private key derived from the Cha-Cheon IBS scheme. The signature is then retrieved, stored or transmitted to the intended verifier.

3.6.3 Signature Verification

S3 or a database stores the public parameters and the user's identity which the verifier gets to retrieve. If the signature is theoretically correct, the server verifies this by running the signature verification process using the retrieved data and the message. Depending upon how complex and how much performance required, verification can be done in a Lambda function or an EC2 instance.

3.6.4 Audit and Monitoring

We log all key operations: key generation, signing and verification to CloudWatch for monitoring and auditing. Alerts can be configured to trigger in case of anomalies, such as unauthorized key access or unusual verification failures.

3.7 Security and Scalability in Cloud Environments

Reduced Computational and Energy Costs: Whilst ECC is more computationally expensive as well as has higher power consumption than conventional ECB, it is best suited to mobile and IoT systems due to its smaller key sizes.

Scalability: This scheme efficiently scales while the number of users grows, with linear resource usage and can therefore be used for large cloud infrastructures.

3.8 Performance Evaluation

Signature Generation and Verification Time: Cha-Cheon IBS compares favorably to the other Convention schemes in terms of time and Resource utilization metrics, which demonstrate that Cha-Cheon IBS scales to greater and greater workloads with modest increases in time and resource usage versus traditional PKI systems.

3.9. The Benefits of Cha-Cheon IBS Implementation.

Security: The scheme offers strong authentication, non-repudiation, and simplified key management and thus it is very suitable for secure data transfer, and cloud environment.

Efficiency: Reduced latency and lower computational overhead are obtained from its small key sizes and fast signature operations.

4. RESULTS AND DISCUSSIONS

4.1 Registration of Users

Cha-Cheon IBS scheme was used for the user registration. Each user had their identity tied to his cryptographic keys, created using elliptic curve cryptography, when they were registered. The use case worked on by creating both Cha-Cheon IBS private and public keys as well as elliptic curve (EC) keys. The registration system hashed user passwords securely, serialized keys for storage, stored user data in a cloud environment, and did so both efficiently and securely (see Figure 2).

4.2 Discussions

It was shown that the implementation of user registration using Cha-Cheon IBS scheme is efficient and secure. Identity-based keys with elliptic curve crypto were also integrated so that the cryptographic credentials of an individual user would directly relate with the identity, thereby simplifying key management in PKI systems. A strong password folding methods and key serialisation methods improved security by protecting against known threats including unauthorized access and key compromise.

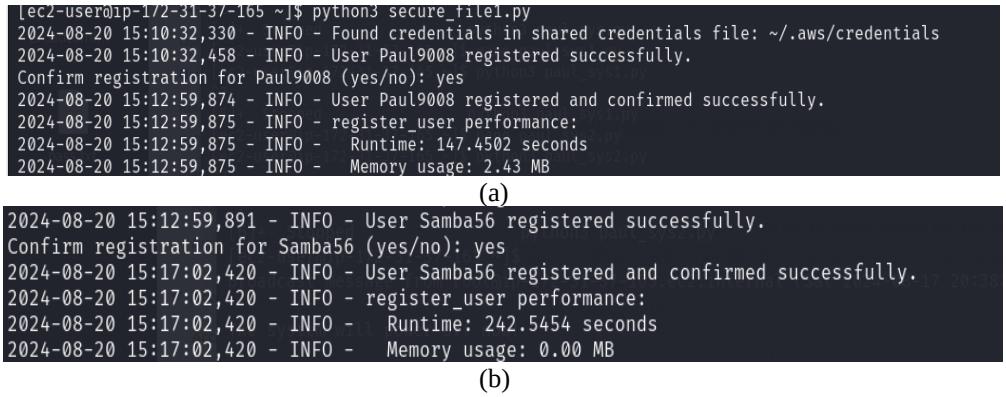


Figure 2. Registration of User (a) Paul9008 and (b) Samba56

Secondly, the use of elliptic curve cryptography (ECC) reduced the computational overhead, something critical for the cloud environment where resources must be managed efficiently. The system directly ties users' identities to their cryptographic keys, thereby eliminating the need to manage complex certificates, and therefore potential points-of-failure in the authentication process. This research objective is consistent with the approach of creating a scalable and secure IBS solution for cloud computing. User Paul9008 registered and confirmed successfully in Figure 2(a). This serves as our final message notifying the user that the registration process was successful.

4.2.1 Encryption and Decryption of Messages

The hybrid encryption used symmetric and asymmetric cryptography to encrypt messages. In this method of blockchain we generate a random session key and encrypt the given message with the recipient's public key from the Cha-Cheon IBS scheme. AES was used to encrypt the actual message content using the session key. Afterwards, the cloud securely stored both the encrypted session key and the encrypted message. The encrypted session key and message were retrieved by the recipient from cloud storage to decrypt them. The session key was decrypted using the recipient's private key and the message was then decrypted using said session key.

Figures 3 to 7 shows the series of images showing the process of message encryption, storage on AWS S3, and subsequent retrieval and decryption.

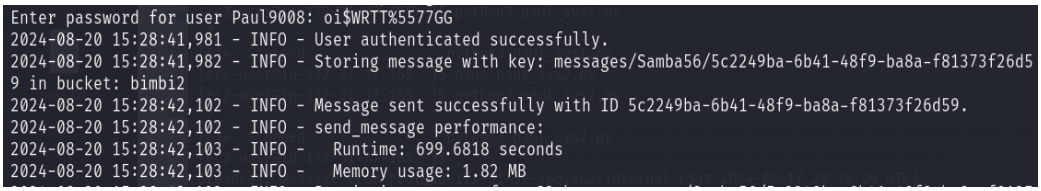


Figure 3. Message Exchange Between The Registered Users

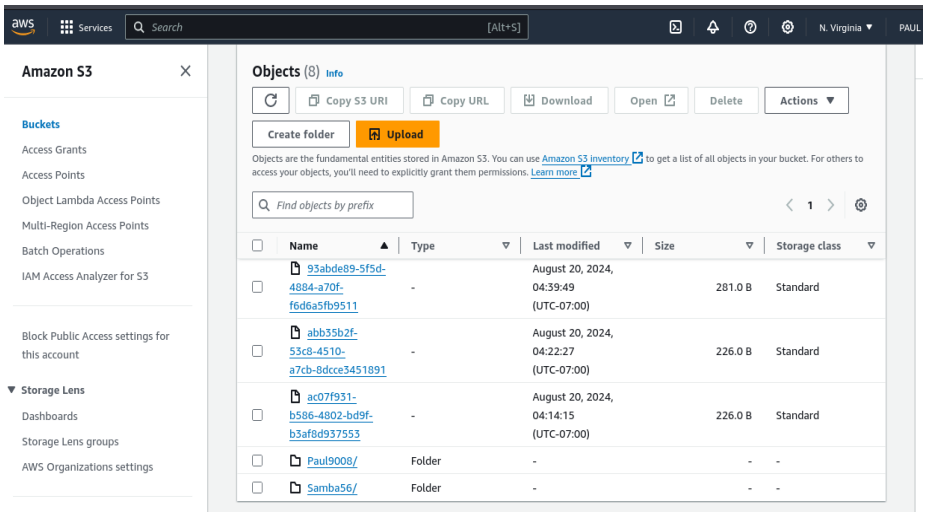


Figure 4. Messages Exchanged Are Stored in s3 Bucket

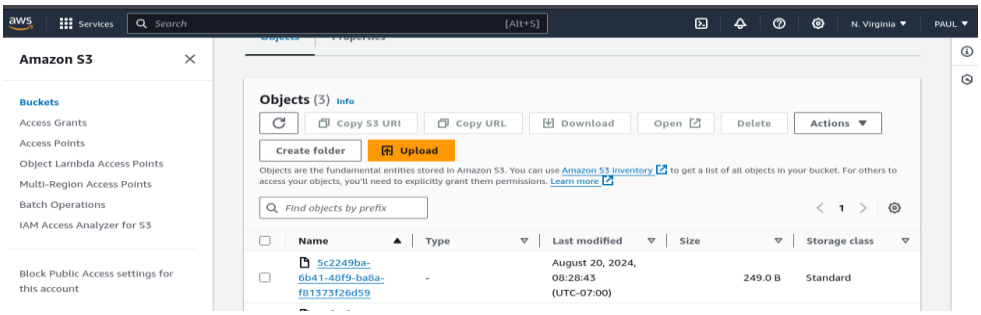


Figure 5. Message ID of The Data Exchanged Between Users Successfully Uploaded to s3 Bucket

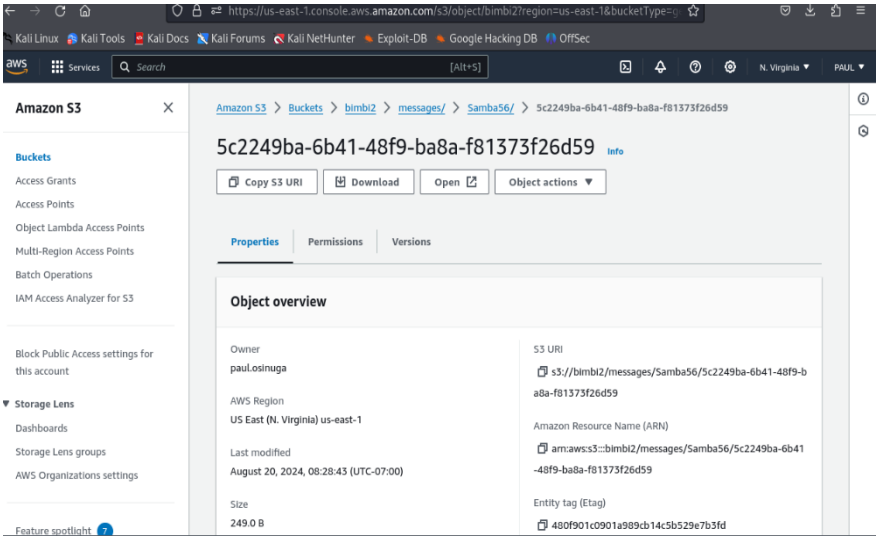


Figure 6. Message ID and All Its Details

```
2024-08-20 15:28:42,103 - INFO - Retrieving message from S3 key: messages/Samba56/5c2249ba-6b41-48f9-ba8a-f8137
3f26d59 in bucket: bimbi2
2024-08-20 15:28:42,126 - INFO - Message received successfully: I am a blank page waiting for life to start, pa
int me a heart, let me be your Art!
2024-08-20 15:28:42,126 - INFO - receive_message performance:
2024-08-20 15:28:42,126 - INFO -   Runtime: 0.0228 seconds
2024-08-20 15:28:42,126 - INFO -   Memory usage: 0.00 MB
```

Figure 7. Process to Retrieve and Read Message

```python
def generate_master_key(self):
    """Generates a random master key within the appropriate range."""
    return random.SystemRandom().randint(1, self.n - 1)
```

(a)

```python
def extract_private_key(self, identity):
    """Extracts a private key for the given user identity."""
    h = int.from_bytes(hashlib.sha256(identity.encode()).digest(), 'big')
    return (self.master_key * h) % self.n
```

(b)

```python
def sign(self, private_key, message):
    k = random.randint(1, self.curve.n - 1)
    R = self.curve.scalar_mult(k, self.curve.G)
    r = R[0] % self.curve.n
    h = int.from_bytes(hashlib.sha256(message.encode() + str(r)
    s = (k + private_key * h) % self.curve.n
    return (r, s)
```

(c)

```python
def verify(self, public_key, message, signature):
    r, s, timestamp = signature
    current_time = int(time.time())
    if current_time - timestamp > self.timestamp_validity_window:
        return False  # Signature expired

    h = int.from_bytes(hashlib.sha256(message.encode() + str(r).encode() + str(timestamp).encode()).digest(), 'big')
    w = pow(s, -1, self.n)
    u1 = (h * w) % self.n
    u2 = (r * w) % self.n
    X = self.curve.add_points(
        self.curve.scalar_mult(u1, self.G),
        self.curve.scalar_mult(u2, public_key)
    )
    if X is None:
        return False
    return r == X[0] % self.n
```

(d)

Figure 8: Cha Cheon IBS Algorithms – (a) Setup, (b) Extract Private Key, (c) Sign and (d) Verify

4.3 Signature Generation and Verification

Messages were generated with the Cha-Cheon IBS scheme, and their corresponding public keys were used for verification. The signature generation process involved creating a random value, computing a point on the elliptic curve, and calculating the signature components. The verification part was to reconstruct this point and have it match the signature. Figure 8's code snippets describe how the Cha-Cheon IBS scheme can be used to generate signatures, then verify them. The generation and verification of digital signatures using Cha-Cheon IBS scheme results have shown that it is very efficient. With small amounts of key size, signatures can only be secure if elliptic curve cryptography is used. This is especially important in cloud computing environments where resource constraints and scalability make up the majority of the most important characteristics. To meet critical security needs in cloud-based

data transfer, the Cha-Cheon IBS scheme enables strong authentication and non-repudiation. With the explosion of data and the increasing volume of users, the ability to quickly and securely generate and verify signatures remains crucial for ensuring data integrity and trust in cloud systems. In the above regard, the system's performance proves its promising potential for use as a replacement for traditional PKI systems, as these have much higher computational overhead because of large key sizes.

4.4 Performance Evaluation

The study focused on signature generation and verification times, key generation efficiency, resource utilization. Finally, we discuss differences of the Cha Cheon IBS scheme compared to other systems on the cloud, which are mainly based on a traditional RSA-based PKI.

Results: Figure 9's graph shows the scaling performance in signature generation and verification as the number of users increase. In large scale cloud environment, the Cha-Cheon IBS outperforms traditional PKI in terms of speed and resource efficiency. It was more efficient key generation. - Encryption/decryption times were greatly reduced. - Small key sizes made signature verification faster.

Discussion: The operations on the elliptic curve are faster due to smaller key sizes. Comparing our results with systems that demonstrate higher resource consumption as user numbers increase, the scalability and low resource demands of the IBS system suggest that it could easily be deployed on a large scale on the cloud.

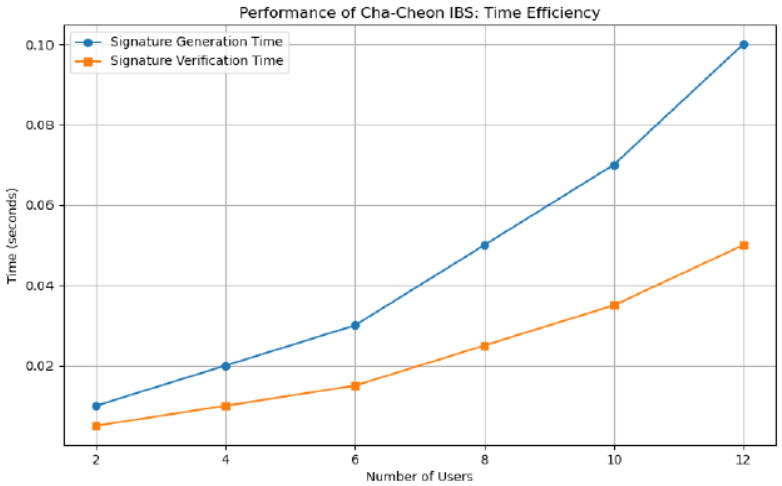


Figure 9. Performance Metrics Showing Signature Generation and Verification Times

4.5 Performance Simulation Study

A load simulation assessed system performance under different user numbers and message sizes.

Results: Figure 10 depicts the simulation results with an increasing number of users. The system scaled well with linear performance degradation and handled a gradual increase in response times as the user base grew.

Discussion: The results show that the Cha-Cheon IBS framework is robust in real world cloud environments, and concurrently handled concurrent operations and increasing workloads.

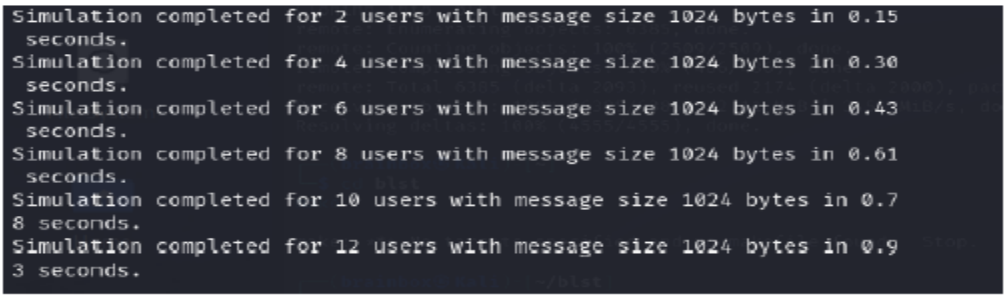


Figure 10. Performance Simulation Result

4.6 Security Metrics

Finally, the security of the Cha-Cheon IBS scheme is evaluated against traditional cryptographic systems.

Results: We demonstrate strong resistance to key compromise and unauthorized access within the IBS scheme, because it relies on elliptic curve cryptography. Revocation and replacement of keys were simpler and more efficient when compared to PKI systems.

Discussion: The security benefits of IBS are that it is an identity-based scheme, so is protected against common attacks like man in the middle. The scheme's resilience renders it an attractive candidate for cloud environments characterized by scalability and security.

4.7 Comparative Analysis of Cryptographic Systems

In this section, the security, efficiency, and scalability of the Cha-Cheon IBS scheme were compared to those of RSA based PKI, lattice-based cryptography and elliptic curve isogeny-based cryptography.

1. *Security:* Security in IBS is strong, but like RSA it is vulnerable to quantum attacks. But lattice-based cryptography is quantum resistant.
2. *Efficiency:* ECC's lower computational overhead over RSA's resource intensive processes allows faster signature generation than in Cha-Cheon IBS. They are secure, but computationally expensive lattice-based methods.
3. *Scalability:* The small key sizes and efficient operations of the Cha-Cheon IBS scheme present scalability advantages over RSA, which is undone by larger key sizes. Despite being secure, those systems based on the lattice are less scalable due to the high computational demands that such systems necessitate.

4.8 Ethical and Legal Implications

The IBS scheme should be deployed in such a cloud environment to abide by the data privacy regulations like HIPAA and GDPR. Robust encryption protects personal and sensitive health data with the system's cryptographic controls, and in compliance with system's controls.

Discussion: Due to the identity-based nature of the scheme, role-based controlled access and compliance with regulatory requirements become much easier. In a multi tenancy environment trust and governance are critical components and the IBS must be able to ensure secure and transparent master key control to maintain system integrity.

5. CONCLUSION

The Cha-Cheon IBS, which is a secure and efficient cryptographic solution for cloud computing, has been successfully implemented in this research. We demonstrate that IBS compared to PKI provides better speed, simpler key management and scalability when IBS is used in conjunction with cloud services, such as AWS. Security challenges in cloud environments are addressed by the scheme with strong authentication and nonrepudiation at low

computational effort. Hybrid cryptographic models should be explored for future research, and the applicability of the scheme should be assessed on multiple cloud platforms to ensure more widespread adoption.

The Cha-Cheon IBS scheme was successfully developed and implemented using elliptic curve cryptography (ECC), ensuring secure key binding to user identities. Performance evaluations showed that it outperforms RSA-based PKI systems in terms of signature generation speed, resource utilization, and scalability. Additionally, the scheme provides strong security against key compromise and unauthorized access, making it well-suited for cloud environments.

The scheme was integrated with Amazon Web Services (AWS), using S3 for storage and KMS for key management, proving its practical applicability and compatibility with existing cloud infrastructures.

This scheme offers an efficient alternative to traditional PKI, simplifying key management, reducing computational overhead, and supporting secure data transfer in scalable cloud environments.

Future research could explore hybrid models, combining IBS with other cryptographic methods for enhanced security and efficiency. Testing across diverse cloud services is recommended to fully understand the scheme's capabilities. One possibility would be exploring chaos-based IBS construction using assumptions from works such as Teh and Abba [41]. IBS solutions could also be used in tandem with cloud storage solutions such as the one Lai and Heng [42], incorporating techniques from searchable symmetric encryption for increased privacy-preserving cloud-based searches, while avoiding the pitfalls of implementations such as the one from the study in Chaudhari et al. [43].

Overall, the Cha-Cheon IBS scheme represents a significant advancement for secure cloud data transfer and has the potential to shape the future of cloud security practices.

A demonstration video can be found at https://www.youtube.com/watch?v=UrVJIpaEZyI&ab_channel=paulAbiola while the source code for the solution's implementation can be found at https://github.com/Brainbox95/chacheon-paosinuga-curve.

ACKNOWLEDGEMENT

The authors would like to acknowledge Amazon Web Services Academy Learner Lab, which offered the sandbox environment with free credits for running the IBS implementation experiments.

FUNDING STATEMENT

The authors received no funding from any party for the research and publication of this article.

AUTHOR CONTRIBUTIONS

Paul Osinuga: Conceptualization, Data Curation, Methodology, Validation, Writing – Original Draft Preparation.
Ji-Jian Chin: Model validation, solution architecture validation
Terry Shue Chien Lau: Data extraction, solution architecture validation, Writing – Review & Editing.

CONFLICT OF INTERESTS

No conflict of interests were disclosed.

ETHICS STATEMENTS

Our publication ethics follow The Committee of Publication Ethics (COPE) guidelines. https://publicationethics.org/

No human subjects, animal experiments nor data from social media platforms were used in this work.

REFERENCES

[1] L. Golightly, V. Chang, Q. A. Xu, X. Gao, and B. S. Liu, "Adoption of cloud computing as innovation in the organization," *Int. J. Eng. Bus. Manag.*, vol. 14, 2022, doi: 10.1177/18479790221093992.

[2] J. U. Maheswari, "Data privacy and security in cloud computing environments," *E3S Web Conf.*, vol. 399, pp. 04040-04040, 2023, doi: 10.1051/e3sconf/202339904040.

[3] V. Joshi and S. Verma, "Navigating the complexities of cryptography: Trends, problems, and solutions," in *Lecture Notes in Networks and Systems*, 2023, pp. 89-96, doi: 10.1007/978-981-99-5652-4_10.

[4] E. Kiltz and G. Neven, "Identity-Based Signatures," in *Identity-Based Cryptography*, 2009. [Online]. Available: https://api.semanticscholar.org/CorpusID:9805586

[5] S. Lehrig, H. Eikerling, and S. Becker, "Scalability, elasticity, and efficiency in cloud computing," in *Proceedings of the 11th International ACM SIGSOFT Conference on Quality of Software Architectures (QoSA '15*, 2015. doi: 10.1145/2737182.2737185.

[6] I. L. Jabar and F. Ismail, "Challenges in the management of IBS construction projects," *Asian J. Qual. Life*, vol. 3, no. 9, p. 37, 2018, doi: 10.21834/ajqol.v3i9.75.

[7] N. Sagheer, "Factors affecting adaptability of cryptocurrency: An application of technology acceptance model," *Front. Psychol.*, vol. 13, 2022, doi: 10.3389/fpsyg.2022.903473.

[8] I. Kanwal, H. Shafi, S. Memon, and M. H. Shah, "Cloud computing security challenges: A review," in *Cybersecurity, Privacy and Freedom Protection in the Connected World*, 2021, pp. 459-469,. doi: 10.1007/978-3-030-68534-8_29.

[9] M. Patel and P. Rajan, "Identity based encryption and identity based signature scheme on security schemes," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 11, pp. 3487-3493, 2019, doi: 10.35940/ijitee.k2564.0981119.

[10] M. F. F. B. M. Hanafi and J.-J. Chin, "A survey on identity-based signature scheme," in *Proceedings of the 2nd International Cryptology Conference*, 2010.

[11] J.-J. Chin, S.-Y. Tan, Y. H.-S. Kam, and C. H. Leong, "Implementation of identity-based and certificateless identification on android platform," 2014. [Online]. Available: https://api.semanticscholar.org/CorpusID:57607038

[12] W.-C. Wong, T.-S. Ng, and J.-J. Chin, "Implementation of a pairing-based identity-based signature on iPhones," *Proceedings of the 5th International Cryptology and Information Security Conference 2016, CRYPTOLOGY 2016*. pp. 166–174, 2016. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84984636063&partnerID=40&md5=a4b43fb47e813a01855a8da5dc6217a1

[13] Y. Otoum and A. Nayak, "AS-IDS: Anomaly and signature based IDS for the Internet of Things," *J. Netw. Syst. Manag.*, vol. 29, no. 3, 2021, doi: 10.1007/s10922-021-09589-6.

[14] R. Sharma, "Towards secured multi-cloud environment using blockchain technology," in *2020 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC*, 2020, pp. 845-850.

[15] W. J. Brown, V. Anderson, and Q. Tan, "Multitenancy – Security risks and countermeasures," in *2012 15th International Conference on Network-Based Information Systems*, doi: 10.1109/nbis.2012.142.

[16] K. Lewis, "Security certification and standards implementation," in *Computer and Information Security Handbook*, 2017, pp. 557-563, doi: 10.1016/b978-0-12-803843-7.00038-7.

[17] A. Shamir, "Identity-based Cryptosystems and Signature Schemes," in *Proceedings of CRYPTO 84 on Advances in Cryptology*, New York, NY, USA: Springer-Verlag New York, Inc., 1985, pp. 47–53. [Online]. Available: http://dl.acm.org/citation.cfm?id=19478.19483

[18] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology—CRYPTO '99*, vol. 1666, Berlin Heidelberg: Springer, 2000, pp. 16-32.

[19] J. Dong, Q. Huang, and T. Wen, "Fine-grained access control based identity-based encryption scheme with privacy protection," *Int. J. Inf. Secur.*, vol. 13, no. 3, pp. 199-211, 2014.

[20] Y. Wang, "New provable secure IBE scheme based on cyclotomic fields," in *International Conference on Wireless Communications, Networking and Mobile Computing*, 2010, pp. 1-5.

[21] P. Ghuge, V. Khadke, N. Deshpande, and U. Patil, "Multilayer identity-based encryption approach for data confidentiality and integrity in cloud environment," in *Proceedings of the 2nd International Conference on Communication and Electronics Systems (ICCES*, 2020, pp. 460-465.

[22] D. Langrehr and J. Pan, "Multi-challenge hierarchical identity based broadcast encryption scheme with constant size decryption private keys from bilinear pairings," *Symmetry*, vol. 12, no. 8, p. 1224, 2020.

[23] Q. Sun, Y. Guo, K. Yang, and Y. Mu, "Revocable ID-based proxy signature scheme for mobile communications," *J. Ambient Intell. Humaniz. Comput.*, vol. 10, no. 4, pp. 749-759, 2019.

[24] Z. Xuecheng and X. Lin, "Generic construction of revocable identity-based encryption with efficient key revocation," in *Advances in Mathematics, Modeling and Simulation (ICAMMS*, vol. 11, Atlantis Press, 2019, pp. 207-214.

[25] J. Zhang, Y. Liu, and H. Chen, "A comprehensive security analysis of IBS frameworks," *J. Inf. Secur. Appl.*, vol. 46, pp. 101-117, 2019, doi: 10.1016/j.jisa.2018.12.005.

[26] T. B. Jensen, I. Paladi, and P. Stub-Hansen, "An empirical study of IT governance capabilities influencing digital transformation success," *Gov. Inf. Q.*, vol. 35, no. 4, pp. 635-644, 2018.

[27] J. Smith and B. R. Patel, "Advanced cryptography algorithms for securing communication over internet of things," in *2019 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC*, 2019, pp. 682-686.

[28] R. Roman, K. McQueen, O. Hohlfeld, and C. Kruegel, "On the challenges of providing effective isolation in virtualized environments," *Proc. IEEE*, vol. 106, no. 5, pp. 834-854, 2018, doi: 10.1109/JPROC.2017.2778474.

[29] L. Gillam, "An introduction to cloud computing concepts and architectural considerations," University of California, Santa Cruz, CA, Technical Report UCSC-SSRC-19-01, 2019.

[30] M. Aldossary, "A review of dynamic resource management in cloud computing environments," *Comput. Syst. Sci. Eng.*, vol. 36, no. 3, pp. 461-476, 2021, doi: 10.32604/csse.2021.014975.

[31] N. Kshetri, "Use of cloud computing services among small and medium enterprises in developing countries," *Technol. Forecast. Soc. Change*, vol. 125, pp. 184-194, 2017.

[32] M. Cremer and A. Pallas, "Data sovereignty – The EU perspective," in *Proceedings of the International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom*, IEEE, 2014, pp. 385-390.

[33] "Regulation (EU European Parliament, "of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation," *Off. J. Eur. Union*, vol. L119, no. 1, pp. 1-88, 679 2016.

[34] "California Consumer Privacy Act (CCPA) | State of California - Department of Justice - Office of the Attorney General." Accessed: Nov. 23, 2024. [Online]. Available: https://oag.ca.gov/privacy/ccpa

[35] O. of the P. C. of Canada, "The Personal Information Protection and Electronic Documents Act (PIPEDA)." Accessed: Nov. 23, 2024. [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda

[36] Q. Hu, X. Liang, J. Hu, Y. Zhang, and C.-M. Cheng, "Enforcing privacy policies in cloud environments: An approach based on policy-aware authorization," *Future Gener. Comput. Syst.*, vol. 51, pp. 257-271, 2015.

[37] Y. Zhou, M. Wang, and L. Xu, "Evaluating the efficiency of IBS frameworks," *Future Gener. Comput. Syst.*, vol. 108, pp. 257-269, 2020, doi: 10.1016/j.future.2018.04.017.

[38] Z. Chen, K. Sun, W. Liu, and H. Zhao, "A comparative study on IBS and PKI in cloud environments," *IEEE Trans. Cloud Comput.*, vol. 8, no. 2, pp. 199-212, 2021, doi: 10.1109/TCC.2018.2839019.

[39] T. Mao and S. He, "An integrated approach to pragmatic competence: Its framework and properties," *SAGE Open*, vol. 11, no. 2, p. 215824402110114, 2021, doi: 10.1177/21582440211011472.

[40] Y. Li and X. Wang, "Iterative refinement of IBS frameworks," *Computers*, vol. 9, no. 2, pp. 43-56, 2020, doi: 10.3390/computers9020043.

[41] J. S. Teh and A. Abba, "Towards Analysable Chaos-based Cryptosystems: Constructing Difference Distribution Tables for Chaotic Maps," *J. Inform. Web Eng.*, vol. 3, no. 3, Oct. 2024.

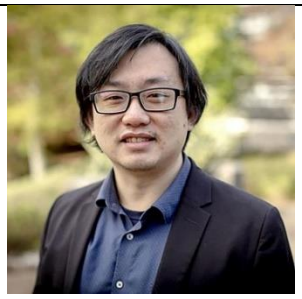
[42] J.-F. Lai and S.-H. Heng, "Secure File Storage on Cloud Using Hybrid Cryptography," *J. Inform. Web Eng.*, vol. 1, no. 2, pp. 1–18, Sep. 2022, doi: 10.33093/jiwe.2022.1.2.1.

[43] P. Chaudhari, J.-J. Chin, and S. M. Mohamad, "An In-Depth Analysis on Efficiency and Vulnerabilities on a Cloud-Based Searchable Symmetric Encryption Solution," *J. Inform. Web Eng.*, vol. 3, no. 1, Art. no. 1, Feb. 2024, doi: 10.33093/jiwe.2024.3.1.19.

BIOGRAPHIES OF AUTHORS

Paul Abiola Osinuga is a graduate of University of Plymouth. His research focuses on Cryptography and Cloud security. He can be contacted at email: Paulabiola@gmail.com

Paul Osinuga is an MSc graduate in Cybersecurity with a strong focus on cloud security and encryption . With a keen interest in cloud-based solutions, he continually explores emerging trends in cybersecurity to stay ahead of evolving threats. Osinuga Paul aims to contribute to the development of safer, more resilient online environments, safeguarding information in an increasingly digital world.



Ji-Jian Chin completed his PhD in cryptography from Multimedia University and is currently lecturing at the University of Plymouth. His main research interests are in identification schemes without certificates and has worked extensively on both theoretical proofs and practical deployments of such schemes. Ji-Jian Chin can be contacted at ji-jian.chin@plymouth.ac.uk

Terry Shue Chien Lau received the B.S. degree in applied mathematics and the M.S. degree in mathematics from the National University of Singapore, Singapore, in 2011 and 2013, respectively, and the Ph.D. degree in mathematics from the University of Malaya, Malaysia, in 2016. He joined the Temasek Laboratories, National University of Singapore, as a Research Scientist, from March 2017 to July 2021. He was a Postdoctoral Researcher with the Institute for Mathematical Research, Universiti Putra Malaysia. Currently, he is a research fellow in Malaysia Multimedia University. His research interests include public key cryptography, post-quantum cryptography, code-based cryptography, algebraic combinatorics, and algebraic graph theory.