A MULTI-RECEIVER ENCRYPTION SYSTEM IN A CLOUD USING THE SM2 SIGNATURE ALGORITHM INCLOUD COMPUTING

1st Saran Sujai T
Department of Information Technology
K. S. R College of Engineering
Tiruchengode, India

2nd Karthikeyan P
Department of Information Technology
K. S. R College of Engineering
Tiruchengode, India

3rd Sidhananth R
Department of Information Technology
K. S. R College of Engineering
Tiruchengode, India

4th Subash S
Department of Information Technology
K. S. R College of Engineering
Tiruchengode, India

***Abstract*— Elliptic Curve Cryptography (ECC) is the cornerstone of data security in the current cloud encryption systems, offering strong defence against unauthorized access. Nevertheless, ECC has drawbackssuch as complex key management, difficulties with scaling, problems with interoperability, and Vulnerability to quantum assaults. The Secure Multi-party (SM2) signature method is a transformative solution that we present in our suggested system. By streamlining essential management procedures, SM2 reduces computational overhead and improves systemperformance in order to overcome these constraints. Additionally, SM2 enhances system functionality and interoperability, enabling smooth interaction with various cloud architectures. Crucially, SM2 provides defence against quantum attacks, guaranteeing long- term data security in encryption systems based on thecloud. Our suggested method raises the bar for cloudsecurity by utilizing SM2, reducing current vulnerabilities and becoming ready for new problems that may arise in the quantum age.**

Keywords— unauthorized access, data security, SM2, cloud, Secure Multi-Party

I. INTRODUCTION

Cloud computing has emerged as a ubiquitous platform for data storage, processing, and sharing, offering unparalleled flexibility and scalability. However, amidst its myriad benefits, security concerns remain a significant challenge. Encryption plays a pivotal role in safeguarding sensitive data in the cloud, particularly in scenarios involving multiple recipients. Traditional encryption algorithms, such as Elliptic Curve Cryptography (ECC), have been widely employed for this purpose. Nevertheless, ECC exhibits certain limitations, particularly in multi-recipient encryption and key management, prompting the exploration of alternative cryptographic solutions.

In response to the shortcomings of ECC, this paper proposes the integration of the SM2 signature algorithm into a multi-receiver encryption system within cloud computing environments. SM2, a cryptographic scheme based on elliptic curves, offers several advantages over ECC, including enhanced efficiency in multi-recipient encryption and simplified key management. By leveraging SM2, we aim to address the challenges associated with ECC while bolstering security and optimizing resource utilization in cloud-based encryption systems.

The goal of this paper is to present a thorough knowledge of ECC's drawbacks in multi-receiver encryption scenarios and show how SM2 adoption can get over these restrictions. We compare the efficacy and performance of SM2 with ECC in cloud computing environments using both theoretical and empirical data. This study adds to the continuing efforts to strengthen cloud data protection methods by providing insights into the potential of SM2 to improve security.

A. Cloud Computing and Encryption

Cloud computing is a widely used platform for data storage, processing, and sharing due to its flexibility and scalability. However, security remains a significant challenge in cloud environments. Encryption is crucial for protecting sensitive data, especially when shared among multiple recipients. Traditional encryption methods like Elliptic Curve Cryptography (ECC) have limitations in multi-recipient encryption and complex key management.

B. SM2 Integration

This discusses the challenges of using Elliptic Curve Cryptography (ECC) for multi-receiver encryption in cloud computing. ECC is known for its strong security mechanisms but struggles with managing multiple keys for multiple recipients, impacting efficiency and scalability. To address these issues, the text introduces the SM2 signature algorithm, which uses elliptic curve-based principles but includes optimizations for multi-receiver contexts. This algorithm simplifies key management, potentially reducing overhead and complications associated with ECC. SM2 also enhances system efficiency, particularly in cloud environments where resources and quick access are crucial. Adopting SM2 offers significant advantages, including enhanced security and better resource utilization. This makes SM2 an attractive solution for enhancing data protection strategies in cloud computing.

C. Objectives and Comparative Analysis

This discusses the challenges of using Elliptic Curve Cryptography (ECC) for multi-receiver encryption in cloud

computing. ECC is known for its strong security mechanisms but struggles with managing multiple keys for multiple recipients, impacting efficiency and scalability. To address these issues, the text introduces the SM2 signature algorithm, which uses elliptic curve-based principles but includes optimizations for multi-receiver contexts.

II. LITERATURE REVIEW

[1] The combination of encryption and digital signature in one operation reduces computing and communication overhead in ad hoc networks. This reduces message size, reducing bandwidth requirements. Signcryption offers enhanced security by providing confidentiality, integrity, and authentication, reducing the risk of security lapses. The scheme supports multiple messages and receivers, enabling effective and low-cost communication between nodes. Scalability is also achieved when the network size is large.

[2] The Internet of Vehicles (IoV) standardization offers benefits such as interoperability, scalability, and increased safety. Interoperability allows for better collaboration and data exchange between vehicles, infrastructure, and other devices. Scalability allows for efficient growth of the IoV ecosystem, while increased safety promotes uniform procedures across vehicles and infrastructure components, reducing risks.

[3] GNSS data compression for autonomous vehicles offers several benefits, including reduced bandwidth usage, increased data transfer speed, and improved network efficiency. By compressing GNSS data, infrastructure-to-autonomous car communication can be faster, reducing latency and allowing cars to make quick decisions based on the latest positional data. Additionally, the compression of GNSS data enhances network efficiency, resulting in better overall performance and more efficient use of network resources.

[4] Physical-digital convergence offers several benefits, including improved communication, enhanced efficiency across industries like smart infrastructure, manufacturing, transportation, and healthcare, and fostering creativity and innovation. This integration of digital and physical systems allows for more fluid interactions, allowing for creative applications and services. It also promotes interdisciplinary cooperation, leading to the creation of fresh approaches to challenges, advancing technology and spurring economic expansion. Additionally, customization is a key benefit.

[5] Industry 4.0 models offer several benefits, including increased efficiency through the use of automation, artificial intelligence, and the Internet of Things. These technologies shorten manufacturing times, optimize resource usage, and boost productivity. They also enable real-time monitoring of supply chain logistics, equipment status, and manufacturing processes, promoting collaboration and proactive decision- making. Additionally, predictive maintenance algorithms, based on IoT sensors and AI analytics, help prevent equipment failures and downtime, reducing maintenance costs and minimizing unscheduled downtime.

[6] Physical-digital convergence offers benefits such as improved communication, enhanced efficiency in industries like smart infrastructure, manufacturing, transportation, and healthcare, and fostering creativity and innovation by integrating physical and digital technology. This interdisciplinary cooperation promotes fresh approaches to challenges, advancing technology and spurring economic expansion. Additionally, customization is a key benefit.

[7] A database scheme with effective keyword search that is publicly verified offers several benefits. It ensures transparency, ensuring the accuracy and integrity of data stored in the database without relying on a third party. It also ensures data integrity, a crucial aspect for applications like financial transactions or legal records. Additionally, the scheme's efficient keyword search features allow users to quickly find relevant information without manual labor.

[8] Down gradable Identity-Based Encryption (DIBE) offers enhanced flexibility in controlling access to encrypted data by enabling dynamic modification of access privileges. It provides fine-grained access control by allowing administrators to designate access levels for users or groups, improving security. DIBE simplifies key management by using identities as public keys, reducing costs related to key distribution and maintenance. Additionally, DIBE is more scalable, particularly in the context of large-scale applications.

[9] The certificate less multi-receiver threshold decryption technique offers several benefits, including efficiency, which can handle decryption for multiple receivers without significantly increasing computing costs, and being certificate less, which reduces the costs associated with certificate administration and streamlines key management. It is particularly useful for messages that need to be shared among authorized users, as it allows multiple receivers to decrypt the message. However, it also has drawbacks, suchas the need for a certificate authority and the need for multiple receivers.

[10] The server-assisted cipher text evolution revocable identity-based encryption (RIBE) scheme offers several benefits, including revocation, which allows users to withdraw access to encrypted data, improving system management and security. Unlike classical IBE, RIBE allows the server to disable or revoke a user's private key, allowing for easier key management. Additionally, RIBE uses identities as public keys, allowing recipients to obtain their public keys from their identities, such as email addresses or usernames, without the need for extra certificates or public keys. It facilitates server-side revocation of a user's private key, which simplifies key management. By using identities as public keys, RIBE allows receivers to access their public keys directly from their identities without the need for extra public keys or certificates.

III. EXISTING SYSTEM

Elliptic Curve Cryptography (ECC) is widely used for multi-receiver encryption techniques in the present cloud computing environment. Strong security protocols and

Effective key management, which is essential for guaranteeing data integrity and confidentiality in cloud environments, make ECC the preferred option. But there areissues with current ECC-based systems, especially with scalability and dynamic key distribution. Cloud systems findit more and more difficult to manage individual keys and uphold uniform encryption standards as the number of recipients rises. Furthermore, security issues like side- channel attacks and vulnerability to improvements in quantum computing demand constant attention to detail in order to keep ECC-based encryption systems resilient.

ECC has limitations when it comes to its effectiveness inmulti-receiver encryption scenarios in cloud computing settings, notwithstanding its benefits.

Key management is a complex procedure that may be quite difficult, especially in cloud systems that are dynamic and have shifting users and access capabilities. It is a challenging logistical issue to efficiently distribute and manage keys while preserving the speed and accessibility of cloud services. Furthermore, the scalability of ECC-based encryption systems becomes a critical concern as cloud systems develop to accommodate larger user bases and increasing data volumes. This calls for ongoing optimization to guarantee that security and performance are not jeopardized.

IV. PROPOSED SYSTEM

The proposed system addresses the difficulties associated with multi-receiver encryption systems by integrating the SM2 signature technique into cloud computing environments. Compared to conventional encryption techniques like ECC, the elliptic curve-based SM2 algorithm has a number of benefits. It is ideal for secure communication in cloud-based systems since it eliminates key management and enhances the efficiency of multi- recipient encryption.

Developing strong key management techniques to enable safe key distribution among several recipients and putting in place effective encryption and decryption procedures to maximize performance in cloud environmentsare important components of our suggested solution. Furthermore, steps will be made to resolve any possible security flaws and guarantee adherence to industry norms and laws pertaining to cloud computing data protection.

Strong key management procedures for safe key distribution, effective encryption and decryption procedures for maximum m cloud performance, and steps to resolve potential security flaws and guarantee adherence to regulatory and industry standards for cloud computing data security are all part of our suggested approach.

We shall assess the effectiveness and viability of our proposed system in comparison to current encryption schemes empirically and through performance analysis, offering important insights into its potential to improve security and scalability in cloud-based multi-receiver encryption scenarios. Our ultimate goal is to further the development of encryption technologies in cloud computing and offer workable solutions for guaranteeing the integrity and confidentiality of data sent to numerous receivers in the cloud.

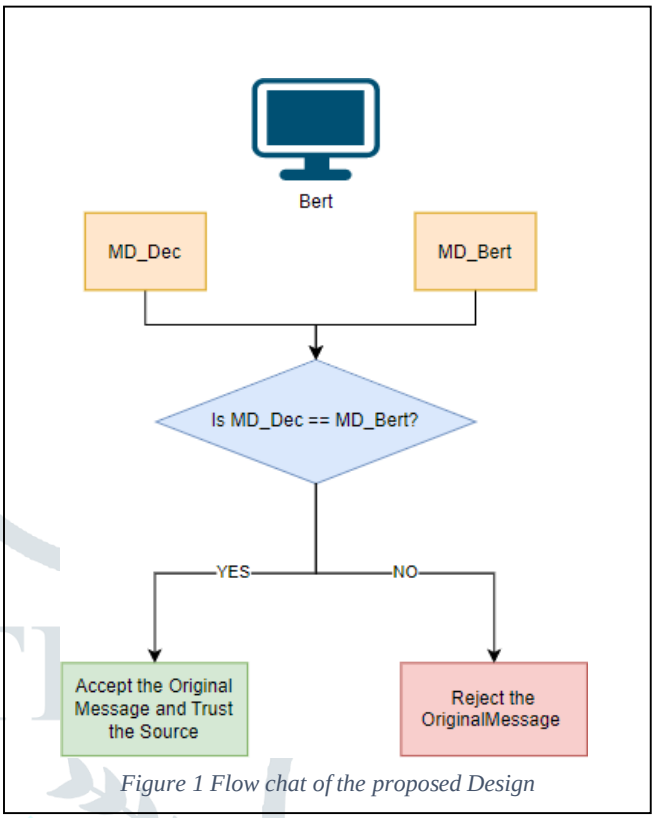

Figure 1 Flow chat of the proposed Design

V. SYSTEM DESIGN SYSTEM

A multi-receiver encryption scheme in a cloud using the SM2 signature algorithm requires several components. These include client applications, a cloud-based encryption and decryption service, a key management system, encrypted data storage, and authentication and authorization services. The system should be designed to scale horizontally, optimize cryptographic operations, monitor and log data, comply with data protection regulations, conduct thorough testing, and regularly backup cryptographic keys and encrypted data. Further refinement and consideration of specific requirements are necessary for a successful implementation.

A. System Architecture

In this system architecture, security is crucial in this multi-receiver encryption system, and it is attained by using centralized cloud server architecture and the reliable SM2 signature technique. A distinct set of cryptographic keys —a public key for encryption and a private key for decryption— are provided to each client. In order to prevent unwanted access, these keys are securely managed and stored by the cloud server, which serves as a reliable middleman. A client encrypts a message using the public keys of the intended recipients when it starts a conversation with several people. This procedure guarantees that the content of the message may only be decoded by the specified recipients who have the relevant private keys.

A key component in coordinating safe communication between clients and recipients is the central cloud server. The server uses its private key to decrypt the content after receiving the encrypted communication from the client. The intended receiver's public keys are then used to re-encrypt

the decrypted message. Through the use of this method, the server serves as a secure gateway, protecting the message's confidentiality while it is in transit. Because only the intended recipients have the decryption keys, this guarantees that evenif the encrypted message were to be intercepted, it would remain unintelligible to unauthorized parties.

This encryption system provides a strong solution for secure multi-receiver communication by utilizing the SM2 signature method and centralized cloud server architecture. Public-key cryptography is used to guarantee that messages stay private and are only accessible by those who are authorized. In addition, the central administration of cryptographic keys improves security by reducing the dangers connected with decentralized key management. All things considered, this solution offers a solid framework for securing privacy and integrity of communication when storing sensitive data in cloud-based settings.

B. Encryption Process

In order to effectively protect the message, a clientfirst generates a random symmetric encryption key when it starts a conversation with several receivers. It then creates numerous cipher texts by separately encrypting this symmetric key with the public keys of each intended recipient. The encrypted message is sent to the centralized cloud server along with these encrypted symmetric keys. The original message can be accessed once the server uses its private key to decrypt the symmetric key upon reception. It then uses each recipient's public key to re-encrypt the symmetric key for them individually, guaranteeing uniqueaccess. Ultimately, the server distributes the encrypted message and the re-encrypted symmetric keys to the appropriate recipients, protecting privacy and facilitating safe communication inside the multi-receiver encryption system.

The client sends the encrypted message and the cipher texts of the symmetric key to the central cloud server,both of which are securely encrypted and hidden behind several levels of encryption. The role of the server is crucial at this point. The server uses its private key to decrypt the symmetric key after receiving the communication, revealing the layers of encryption that the client painstakingly applied. After the symmetric key has been revealed, the server must perform an important function: it must re-encrypt the symmetric key using the receivers' public keys. By transforming the symmetric key into a new cryptographic envelope, this method makes sure that only the intended receivers may access it, protecting it from prying eyes and unwanted access.

C. Decryption Process

Every recipient uses their private key in a crucial decryption procedure after getting the encrypted message and the re-encrypted symmetric key from the cloud server. Equipped with their own cryptographic credentials, the beneficiaries remove the safeguards encircling the symmetric key, revealing the intricate digital architecture painstakingly created by the central server. By using this decryption technique, the original symmetric key—a crucial artifact that permits the decoding of the underlying message—becomes accessible to every recipient.

Recipients move smoothly to the last stage of the cryptographic journey: message decryption, when the symmetric key has been decrypted.

Recipients use symmetric encryption methods to decrypt the encrypted message and reveal its hidden contents by utilizing the encrypted message and reveal its hidden contents by utilizing the now-available symmetric key.

Cryptographic isolation is strengthened by the system's distribution of the decryption process across several recipients, each of whom has access to their private key. The system strengthens security measures and fortifies defenses against unwanted access and eavesdropping through the strategic deployment of cryptographic duties. In the end, this method provides a strong foundation for safe multi-receiver communication, where data quality and secrecy are top priorities and critical information is protected from possible attackers.

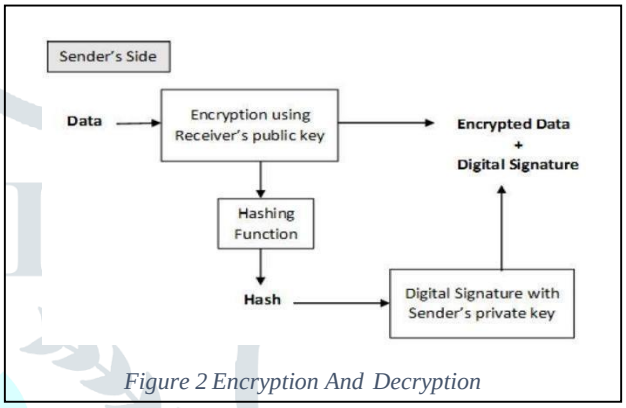

Figure 2 Encryption And Decryption

D. Security Measures

Several steps can be taken to guarantee the system's security. First, in order to safeguard the messages' confidentiality, robust encryption techniques like SM2 should be employed. To further prevent unwanted access, the cloud server should securely handle and store the clients' private keys.

Ensuring that only authorized clients are able to send and receive messages requires the implementation of access restrictions and authentication procedures. To find and fix any possible vulnerability in the system, regular security audits and updates should also be carried out.

The multi- receiver encryption system can offer strong protection for communication in the cloud environment by putting these security measures into place. To ensure data confidentiality, integrity, and availability in a cloud environment for multi- receiver encryption, several security precautions must be taken. These include strong encryption using the SM2 algorithm, proper key management, and the use of SM2 Signature Algorithm for digital signatures.

Message Authentication Codes (MACs) are used to protect against manipulation and ensure message integrity. Additionally, secure communication channels, such as TLS/SSL, must be established between clients and servers to ensure secure communication. To ensure strong security in a multi-receiver encryption system using the SM2 signature method and deployed in a cloud environment, tight access controls, strong authentication methods like multi-factor authentication, end-to-end encryption, regular security audits and updates to fix vulnerabilities, and constant monitoring of the cloud environment for unusual or suspicious activity are essential steps.

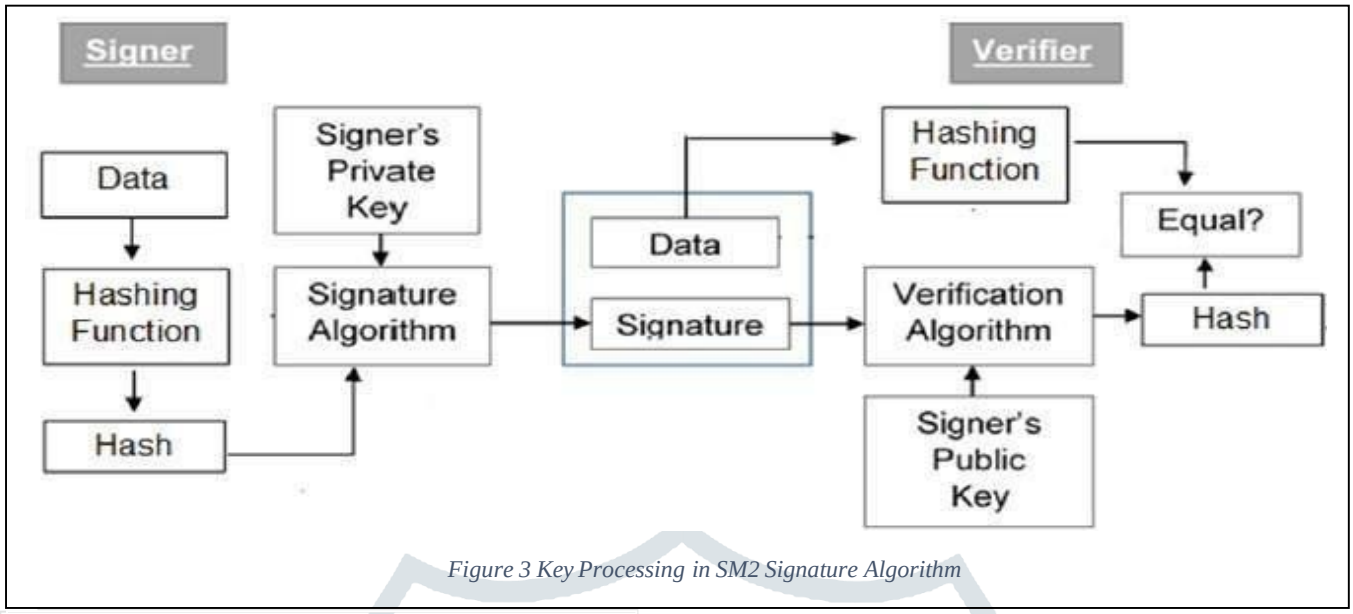

Figure 3 Key Processing in SM2 Signature Algorithm

1) Key Management

For any encryption system to be secure, effective key management is essential. To securely produce, store, and distribute cryptographic keys—public and private—in this setting, strict protocols need be put in place. Keys are safeguarded from theft, manipulation, and unwanted access with the help of a strong key management system. To limit key access to just authorized individuals or entities, access rules should be strictly enforced. To lessen the effects of key compromise or loss, additional measures like key rotation and key revocation should be used. Unauthorized activity can also be found and stopped with the aid of routine audits and key usage monitoring.

2) Data Confidentiality

Keeping data private and secure is crucial when using a multi-receiver encryption system. The SM2 Signature Algorithm is one of the encryption techniques that is essential for protecting data secrecy both during transmission and storage. Nonetheless, encryption must be used in conjunction with additional security measures like secure communication protocols, data authentication, and message integrity checks. Verifying the integrity and authenticity of data sent between clients and the cloud server can be facilitated by putting policies in place like message authentication codes (MACs) and digital signatures. To further improve data security, encrypted connections between clients and the server can be established via secure channels like Transport Layer Security (TLS). Frequent vulnerability scans and security assessments can assist in locating and addressing possible risks to the integrity and confidentiality of data.

E. Key Features

There are a couple of key features in the proposed design, and efficiency and integrity are the primary elements.

1) Efficiency

The method of encrypting a single encrypted message to the multiple cloud recipients is the effective and efficient. It allows the sender to encrypt the message once, producing a single ciphertext that can be decrypted by multiple authorized recipients. This reduces computational expenses for both the sender and cloud server, and improves communication efficiency by reducing the need for separate copies of the message.

The SM2 signature technique ensures secure communication between multiple recipients in cloud computing environments, minimizing computation and storage overhead. Cloud infrastructure's scalability and parallelism handle cryptographic processes, reducing latency and optimizing throughput. The system also promotes a balance between security and throughput in multi-recipient encryption situations, improving system performance and reliability. Overall, efficiency in cloud computing environments is crucial for efficient communication and resource management.

2) Integrity

The SM2 Signature Algorithm ensures data integrity and validity in encrypted communication. It works by creating a digital signature for the ciphertext after encryption for multiple recipients. This cryptographic assurance ensures the ciphertext remains unaltered during transmission or storage. Additionally, the SM2 signature provides authentication, allowing recipients to confirm the sender's identity and the message's integrity.

Integrity is crucial for ensuring the reliability and credibility of encrypted data transfer in cloud computing. It guarantees data preservation and authenticity, preventing alterations or tampering. The SM2 signature algorithm provides robust cryptographic algorithms to ensure integrity, protecting private data and increasing user trust in cloud-based encryption solutions.

VI. CONCLUSION

The SM2 signature algorithm is a powerful solution for organizations to securely transmit and share sensitive data in a cloud environment. It offers robust security against cryptographic attacks, ensuring only authorized recipients can access the information. Cloud computing resources enable efficient encryption and the

decryption processes, allowing for rapid and scalable handling of large volumes of data.

SM2 also offers computational advantages compared to other encryption algorithms. The cloud environment provides the flexibility to scale resources dynamically based on demand, accommodating an increasing number of users and data volumes without compromising performance or security. Proper key management is essential for the security of the encryption scheme.

Adherence to relevant data protection regulations, such as GDPR or HIPAA, is crucial for ensuring data privacy and security. The design of the encryption scheme should be an iterative process, with regular evaluations and updates to address emerging threats and vulnerabilities. This approach provides a balance between security, efficiency, and usability in data protection efforts.

VII. FUTURE WORK

This work discusses the importance of data security in cloud computing and the use of multi-receiver encryption schemes. It provides an overview of cloud computing architecture, security challenges, and existing encryption schemes. The SM2 signature algorithm is introduced, along with its cryptographic properties. The paper reviews existing research on encryption schemes in cloud computing and compares different signature algorithms.

The proposed multi-receiver encryption scheme is described, integrating the SM2 signature algorithm into the encryption process. The scheme addresses security and scalability in cloud environments, and it is detailed in cryptographic analysis. The implementation architecture is discussed, and performance evaluation metrics and benchmarks are provided.

The security analysis is discussed, including potential attacks and vulnerabilities, and the scheme's resilience against security threats. Experimental results are presented, and the paper concludes with a summary of the proposed scheme, its key findings, and its importance in enhancing data security in cloud computing.

VIII. REFERENCES

1. Wang, C.; Liu, C.; Li, Y.; Qiao, H.; Chen, L. Multi-message and multi-receiver heterogeneous signcryption scheme for Ad-Hoc Network. Inf. Secur. J. Glob. Perspect. 2017, 26, 136–152.
2. Wiseman, Y. Adapting the H. 264 Standard to the Internet of Vehicles. Technologies 2023, 11, 103.
3. Rakhmanov, A.; Wiseman, Y. Compression of GNSS Data with the Aim of Speeding up Communication to Autonomous Vehicles . Remote Sens. 2023, 15, 2165.
4. Piromalis, D.; Kantaros, A. Digital twins in the automotive industry: The road toward physical-digital convergence. App. Syst. Innov. 2022, 5, 65.
5. Tsaramirsis, G.; Kantaros, A.; Al-Darraji, I.; Piromalis, D.; Apostolopoulos, C.; Pavlopoulou, A.; Alrammal, M.; Ismail, Z.; Buhari, S.M.; Stojmenovic, M.; et al. A modern approach towards an industry 4.0 model: From driving technologies to management. J. Sens. 2022, 2022, -5023011
6. V. Hindumathi and K. R. L. Reddy, ‘‘Adaptive priority-based fair-resource allocation for MIMO-OFDM multicast networks,’’ Int. J. Netw. Virtua l Organisations, vol. 20, no. 1, pp. 73–89, Jan. 2019.
7. M. Miao, J. Wang, S. Wen, and J. Ma, ‘‘Publicly verifiable database scheme with efficient keyword search,’’ Inf. Sci., vol. 475, pp. 18–28, Feb. 2019.
8. O. Blazy, P. Germouty, and D. H. Phan, ‘‘Downgradable identity-based encryption and applications,’’ in Proc. Cryptographers’ Track RSA Conf. Cham, Switzerland: Springer, 2019, pp. 44–61
9. R. Gao, J. Zeng, and L. Deng, ‘‘An efficient certificateless multi-receiver threshold decryption scheme,’’ RAIRO-Theor. Informat. Appl., vol. 53, nos. 1–2, pp. 67–84, 2019.
10. Y. Sun, Y. Mu, W. Susilo, F. Zhang, and A. Fu, ‘‘Revocable identity-based encryption with server-aided ciphertext evolution,’’ Theor. Comput. Sci., vol. 815, pp. 11–24, May 2020.