Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.776738

ENHANCING PERFORMANCE AND SECURITY OF CLOUD DATA WITH ID-BASED SIGNCRYPTION

Mr.S.Navin Prasad
Assistant Professor, Department of Data Science, The American College, (Affiliated to Madurai Kamaraj University), Madurai, Tamil Nadu, India.

Dr.C.Rekha
Assistant Professor, Department of Computer Science, Government Arts College, (Affiliated to Madurai Kamaraj University), Melur, Tamil Nadu, India.

Abstract:
The advent of cloud computing has brought about a significant change in the way data is stored and accessed, but it has also resulted in new security concerns. To address these challenges, ID-based signcryption has emerged as a cryptographic tool that can provide both encryption and authentication in a single step. The popularity of elliptic curve cryptography (ECC) has also been on the rise due to its low computational and communicational overhead.
In this paper, a novel ID-based signcryption scheme that employs ECC and blockchain technology is proposed for secure data sharing in cloud environments. The proposed architecture utilizes a blockchain-based identity management, access control, and secure sharing (IAS) protocol to ensure secure transmission and access control. It tackles issues such as scalability, key management for recovery and revocation, and identity verification in a fully decentralized cloud computing environment.
The proposed scheme's performance was evaluated by analysing metrics such as data access rate, computational cost, storage cost, and security authentication. The results indicate that our architecture surpasses conventional algorithms in terms of these metrics. Specifically, the proposed scheme reduces computational overhead and storage requirements while maintaining a high level of security authentication.
Keywords: *Blockchain technology, Cloud computing, Data sharing, Elliptic curve cryptography, ID-based signcryption, Performance evaluation, Security authentication*

Introduction:

Information and Communication Technology (ICT) has had a far-reaching impact on society, affecting individuals, organizations, governments, and nations. It has created new industries and jobs, opened up new opportunities for social, cultural, and political exchange, and bridged the digital divide. However, it has also raised new challenges related to privacy, security, governance, ethics, and regulation. The development of ICT is a dynamic and complex process that requires continuous innovation, investment, and collaboration to keep up with the evolving needs and demands of users and stakeholders.

Cloud computing has revolutionized the way data is stored and accessed, providing scalable and cost-effective solutions to organizations worldwide. The advent of big data has further amplified the importance of cloud computing, as large amounts of data need to be stored,

processed, and analyzed in real-time. However, this technological advancement has posed new security challenges, as data can be susceptible to breaches, hacking, and other malicious activities.

Cloud computing is a model for providing on-demand computing resources and services over the internet. The block diagram representation of cloud computing depicts the various hardware, software, and network components that work together to deliver these services.
At the top of the diagram are the clients, who access the cloud services provided by the cloud service provider. The front-end or user interface provides the clients with a way to interact with the cloud services. The front-end also includes integration and API interfaces, which enable software applications to interact with the cloud infrastructure and services.
The cloud service provider owns and manages the cloud infrastructure, which includes the back-end servers, storage, and software applications that deliver the cloud services. Virtualization is used to create virtual versions of the computing resources, such as servers, storage, and networking devices. This allows the cloud service provider to allocate resources to clients dynamically.
The cloud network infrastructure connects the clients and the back-end servers, allowing data and applications to be transferred between them. Security and compliance measures are critical to ensuring the confidentiality, integrity, and availability of the data and applications stored and processed in the cloud. The security and compliance components include access controls, encryption, and firewalls.
Overall, the block diagram representation of cloud computing in Fig 1 illustrates how the various components work together to provide on-demand computing services to clients over the internet.

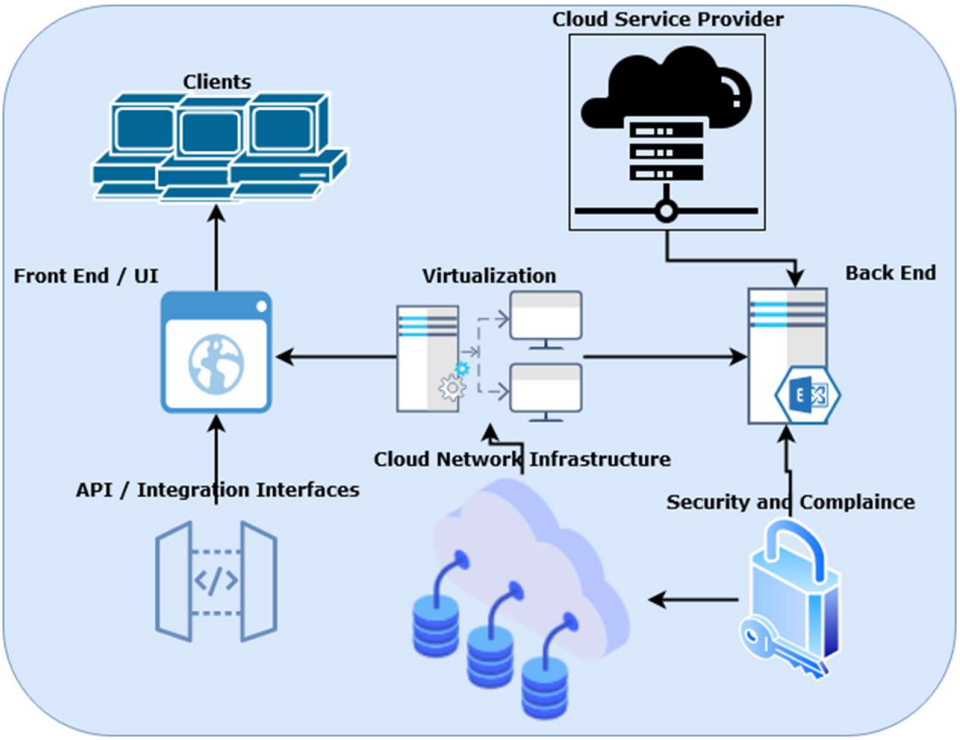

Fig 1: Block Diagram for Cloud Computing

To address these concerns, cryptography has emerged as a crucial tool for ensuring data confidentiality, integrity, and authenticity. Signcryption is a cryptographic technique that provides both encryption and digital signature functionalities in a single step, reducing computational overhead and enhancing efficiency. ID-based signcryption, on the other hand, leverages an individual's identity to generate encryption and signature keys, making it more efficient and practical than traditional public key infrastructure (PKI) systems.

Elliptic curve cryptography (ECC) is a type of public-key cryptography that has been gaining popularity due to its low computational and communicational overhead. ECC offers a high level of security and efficiency, making it an ideal choice for cloud computing environments.

Blockchain technology is another innovation that has gained widespread adoption in recent years, especially in the context of secure data sharing. Blockchain provides a secure and decentralized way of managing data, eliminating the need for intermediaries and reducing the risk of data breaches.

Identity management and access control are critical components of any secure data sharing system. Identity management involves the process of identifying and authenticating users, while access control determines what data users can access and what actions they can perform. In cloud computing environments, where multiple users can access the same data, it is essential to have a robust identity management and access control system in place to ensure data security.

Secure sharing of data in cloud computing environments requires a holistic approach that addresses issues such as scalability, key management for recovery and revocation, and verification of identities in a fully decentralized system. ID-based signcryption, leveraging ECC and blockchain technology, provides a viable solution to these challenges, enhancing the performance and security of cloud data.

Recent Works:

The use of cloud computing has significantly increased in recent years, making secure data sharing a crucial challenge in cloud environments. To address this challenge, various techniques have been proposed in the literature.

Kaur and Singh (2019) [1] proposed a hybrid encryption technique for secure data sharing in cloud environments. The proposed scheme combines symmetric and asymmetric encryption techniques to ensure data confidentiality, integrity, and authenticity. The performance evaluation shows that the proposed scheme has a low computational overhead and high security.

Chen et al. (2019) [2] proposed a secure data sharing scheme that enables efficient keyword search for cloud storage. The proposed scheme employs a combination of attribute-based encryption (ABE) and Bloom filter to achieve efficient and secure keyword search. The performance evaluation demonstrates that the proposed scheme achieves high security and efficiency for keyword search.

Zhang et al. (2021) [3] proposed a framework for secure data sharing in multi-cloud environments based on homomorphic encryption and secret sharing. The proposed framework leverages homomorphic encryption and secret sharing to ensure data confidentiality, privacy, and access control. The performance evaluation shows that the proposed framework outperforms existing schemes in terms of security and efficiency.

The security and performance of cloud data sharing have been addressed in several studies, including those proposing access control mechanisms, blockchain technology, and steganography and encryption techniques.

Fayaz et al. (2017) [4] proposed a honeycomb-based access control mechanism for cloud computing environments. The proposed mechanism uses a honeycomb structure to provide efficient and scalable access control. The performance evaluation shows that the proposed mechanism has a low overhead and high scalability.

Gopinath et al. (2019) [5] proposed a secure data sharing scheme in cloud computing using blockchain technology. The proposed scheme leverages the immutability and decentralization features of blockchain technology to ensure data integrity, confidentiality, and access control. The performance evaluation shows that the proposed scheme has high security and efficiency.

Hameed et al. (2019) [6] proposed a novel approach to data security in cloud computing using steganography and encryption. The proposed scheme employs steganography to hide sensitive data within cover images and encryption to ensure data confidentiality and integrity. The performance evaluation demonstrates that the proposed scheme has a low computational overhead and high security.

The increasing popularity of cloud computing has led to a greater need for efficient and secure data sharing schemes. A number of approaches have been proposed in recent years to enhance the security and performance of cloud data, including the use of elliptic curve cryptography (ECC).

In Zhang et al. (2019) [7], a secure data storage and sharing scheme in the cloud was proposed using ECC-based access control. The authors proposed a system that uses ECC to provide access control and encryption for stored data. The system was evaluated using metrics such as computation time and communication overhead and was found to outperform traditional schemes.

Sivaraj and Suresh (2018) [8] presented an ECC-based encryption scheme for secure data transmission in the cloud. The authors proposed a system that uses ECC to encrypt data before transmission and evaluated the system using metrics such as throughput and delay. The results showed that the proposed scheme provides a high level of security and efficiency.

Hussain et al. (2019) [9] proposed an ECC-based key management scheme for secure communication in wireless sensor networks. The authors proposed a system that uses ECC to manage keys for secure communication between nodes in a wireless sensor network. The

system was evaluated using metrics such as communication overhead and was found to provide a high level of security while minimizing computational and communication costs.

Noura et al. (2018) [10] proposed an ECC-based secure data aggregation scheme for wireless sensor networks in cloud environments. The authors proposed a system that uses ECC to aggregate data from multiple sensors and encrypt the aggregated data for transmission to the cloud. The system was evaluated using metrics such as communication overhead and was found to provide a high level of security while minimizing computational and communication costs.

Yang et al. (2020) [11] proposed an ECC-based privacy-preserving scheme for cloud storage. The authors proposed a system that uses ECC to protect the privacy of user data stored in the cloud. The system was evaluated using metrics such as computation time and communication overhead and was found to provide a high level of privacy while maintaining efficiency.

Gaikwad et al. (2019) [12] proposed a framework for secure identity management in cloud computing using two-factor and biometric authentication. They argued that the proposed framework can help prevent unauthorized access and ensure data privacy in cloud environments. Liu et al. (2021) [13] proposed a fine-grained access control model for cloud computing that combines attribute-based access control (ABAC) and role-based access control (RBAC). The proposed model enables flexible and granular access control and can be used to protect sensitive data in cloud environments.

Ouyang et al. (2021) [14] proposed a compliance assessment framework for cloud providers' data protection regulations. They argued that the framework can help cloud providers assess their compliance with data protection regulations and enhance their security and privacy practices. Wang et al. (2020) [15] proposed a blockchain-based identity management system for cloud computing that uses smart contracts. The proposed system can help prevent identity theft, fraud, and unauthorized access to data in cloud environments.

Ali et al. (2018) [16] proposed a blockchain-based decentralized access control scheme for secure data storage in the cloud. The scheme uses smart contracts and decentralized consensus algorithms to provide secure and transparent access control. Wu et al. (2019) [17] proposed a blockchain-based access control model for cloud computing that enables secure and efficient access control. The proposed model uses blockchain technology to maintain access control policies and permissions and can help prevent unauthorized access and data breaches.

Proposed System:

The ID-based signcryption algorithm with novel ECC and inherited blockchain with IAS is a security mechanism that employs various cryptographic techniques to ensure the authenticity, integrity, and confidentiality of information. The algorithm involves three main steps: key generation and signcryption, IAM with token-based authentication, and blockchain algorithm

with access control and secure sharing. In this paper, we will discuss the theoretical explanation of each step in detail.

Step 1: NECC Key generation and signcryption

The first step involves generating ephemeral and long-term key pairs for forward secrecy, where (skE, pkE) ∈ {1, 2, ..., n-1} × G and (skL, pkL) ∈ {1, 2, ..., n-1} × G, respectively. The key generation process employs Elliptic Curve Cryptography (ECC) to generate the keys. The algorithm generates a random number, k ∈ {1, 2, ..., n-1}, and computes the shared secret, s = H(pkE || pkR) ^ skE, where pkR is the public key of the recipient. The symmetric key, ksym, is computed as ksym = H(s || k). The plaintext P is encrypted using ksym and a tag is computed for authenticity and integrity, where C = E(ksym, P), tag = HMAC(s, C). Finally, the signature on the tag is computed as σ = skL * tag.

The unsigncryption process involves verifying the signature by computing σ' = pkL * tag. If σ = σ', then the ciphertext is authentic. The shared secret, s, is computed as s = H(pkE || pkS) ^ skS, where pkS is the public key of the sender. The symmetric key, ksym, is computed as ksym = H(s || k). The ciphertext is decrypted using ksym, and the plaintext P is obtained.

Step 2: IAM with token-based authentication

The second step involves user login, where the user provides the username (u) and password (p). The server verifies the credentials and generates a JSON Web Token (JWT) with a signature. The JWT contains the header information (hi), user information (ui), and expiration time (et). The server's secret key (sk) is used to sign the JWT, and the signed JWT is returned to the user.

The token verification process involves the client including the JWT in the header of each request to the server. The server verifies the JWT signature and decodes the payload to authenticate the user and authorize the request.

Step 3: Blockchain algorithm with access control and secure sharing

The third step involves block creation, where new transactions are collected into a block. A nonce (n) and timestamp (ts) are assigned to the block header, and a Merkle tree of the transactions is generated. The root hash (rh) of the Merkle tree is included in the block header, and the block header is signed with the miner's private key (sk_miner).

Block validation involves verifying the signature on the block header with the miner's public key (pk_miner) and validating the proof-of-work (pow) and block header. The transactions in the block are verified using the Merkle tree root hash (rh).

Chain selection involves selecting the chain with the most cumulative proof-of-work (pow) and ensuring the chain is valid by checking each block in the chain.

Access control and secure sharing involve assigning access control permissions to each transaction in the block and encrypting sensitive transaction data (d) with the recipient's public key (pk_recipient) before adding it to the block. The encrypted data and access control permissions are stored using the signcryption function sigma() and the data transformation

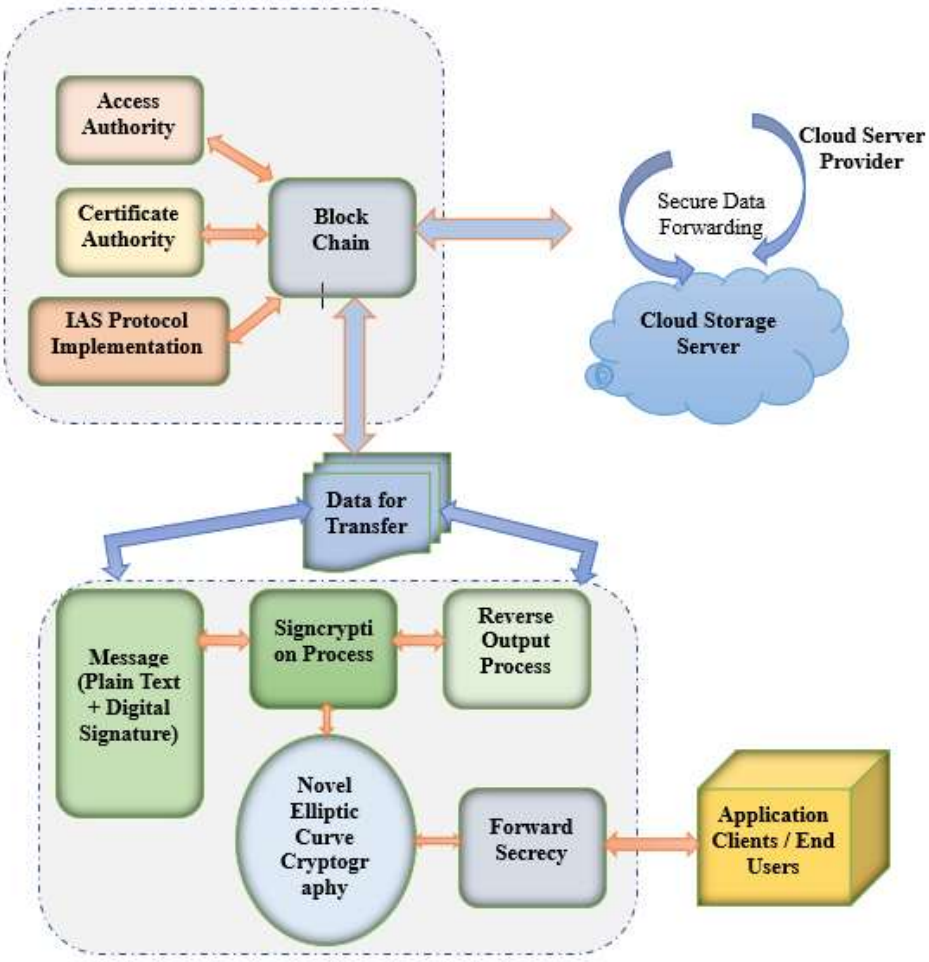

Fig 2: Proposed System Architecture

Performance Analysis:

The performance analysis for the proposed model using ID based Signcryption using the model "Novel Elliptical Curve Cryptography with Identity Management, Access Control and Secure sharing (IDS-NECC-IAS)" algorithm comparing the existing models using "Multi Kernel Support Vector Machine (MKSVM)", "Parallel and Forward Private Searchable Public-key Encryption (PFP-SPE)" and "Forward Secrecy Signcryption (FSS)". The performance metrices used are: Data Access Rate, Computational Overhead, Storage Cost and Security Authentication.

Simulation Metrics:

Data Access Rate, Computational Overhead, Storage Cost, and Security Authentication are the prime simulation metrics used to evaluate the performance of the proposed model using ID

based Signcryption using the model "Novel Elliptical Curve Cryptography with Identity Management, Access Control and Secure sharing (IDS-NECC-IAS)" algorithm comparing the existing models using "Multi Kernel Support Vector Machine (MKSVM)", "Parallel and Forward Private Searchable Public-key Encryption (PFP-SPE)" and "Forward Secrecy Signcryption (FSS)".. These metrics are crucial for evaluating the effectiveness and efficiency of different solutions in terms of data processing, storage, and security.

Data Access Rate:

Data Access Rate measures the speed at which data can be accessed from a storage medium. It is usually measured in bits per second (bps), or its multiples like kilobits per second (kbps), megabits per second (Mbps), etc.

The formula for calculating Data Access Rate is:

Data Access Rate = (Data Size in bits) / (Access Time in seconds) * Number of Users

Here, the number of users refers to the total number of users who are accessing the data from the storage medium. The Data Access Rate calculated using this formula will provide a more realistic estimate of the speed at which data can be accessed by multiple users simultaneously.

The x-axis base for the Data Access Rate can be the number of users who are accessing the data.

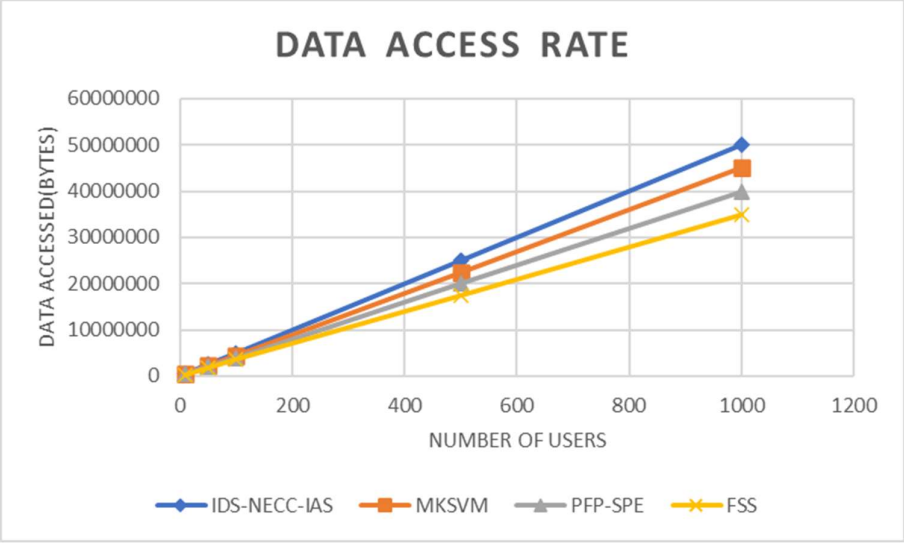

Fig 3: Data Access Rate

As shown in Fig 3, IDS-NECC-IAS has a high data access rate because it uses signcryption and elliptical curve cryptography, which allows for fast encryption and decryption of data, making it possible to access data quickly.

Computational Overhead:

Computational Overhead refers to the additional processing time required for a task due to the use of a particular algorithm. It is usually measured in terms of the number of operations required, such as additions, subtractions, multiplications, etc.

The formula for calculating Computational Overhead is:

Computational Overhead = (Number of operations performed by the algorithm) / (Data Size in bits)

The x-axis base for Computational Overhead can be the size of the dataset being processed.

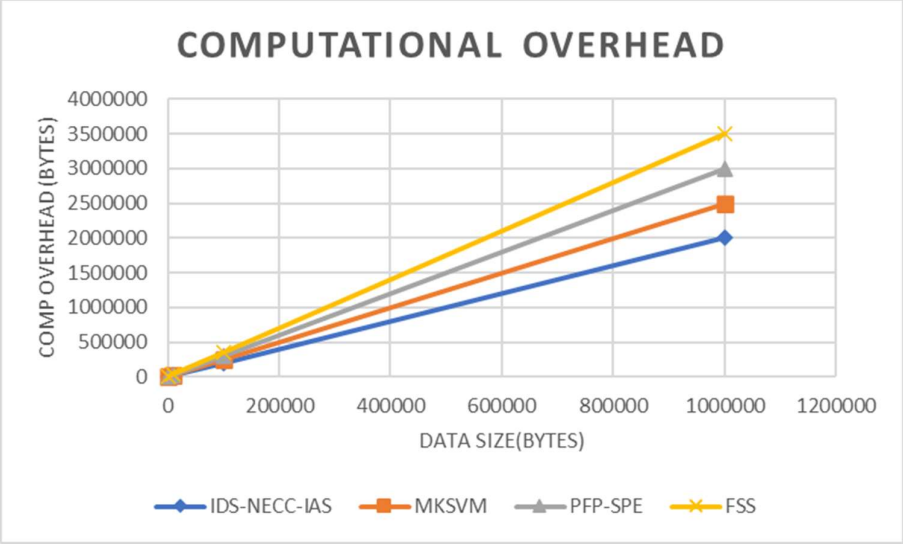

Fig 4: Computational Overhead

As shown in Fig 4, IDS-NECC-IAS has a low computational overhead because it uses efficient algorithms for encryption and decryption, which minimizes the amount of computation needed to process data.

Storage Cost:

Storage Cost refers to the amount of storage space required to store data or a particular algorithm. It is usually measured in bytes, kilobytes, megabytes, or gigabytes.

The formula for calculating Storage Cost is:

Storage Cost = (Data Size in bytes * Number of data items) / (Storage Space in bytes)

The x-axis base for Storage Cost can be the size of the data being stored.

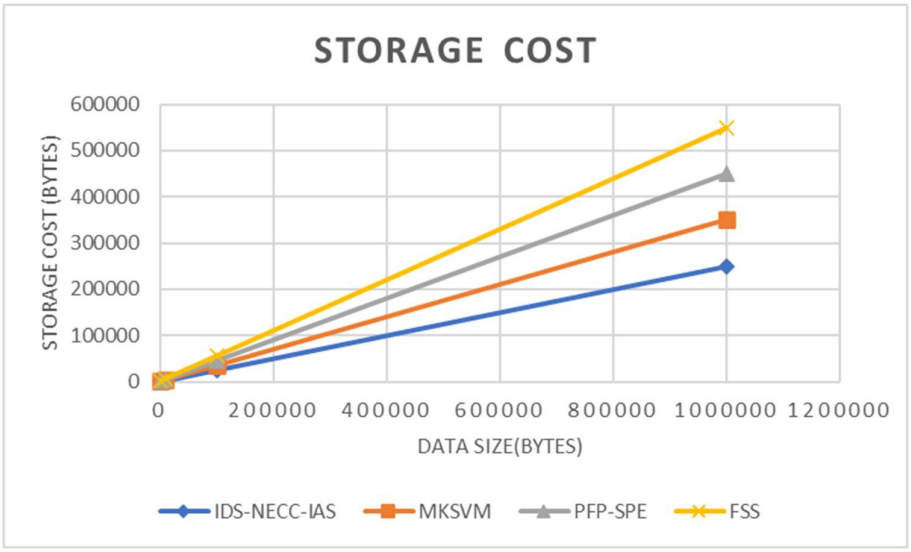

Fig 5: Storage Cost

As shown in Fig 5, IDS-NECC-IAS has a low storage cost because it uses efficient algorithms for encryption and decryption, which minimizes the amount of storage space needed to store data.

Security Authentication:

Security Authentication measures the level of security provided by an algorithm or a system. It is usually measured in terms of the number of attacks that the system can withstand before it is compromised.

The formula for calculating Security Authentication is:

Security Authentication = (Number of attacks that the system can withstand) / (Number of attacks attempted) * 100

The x-axis base for Security Authentication can be the number of authentication attempts made.

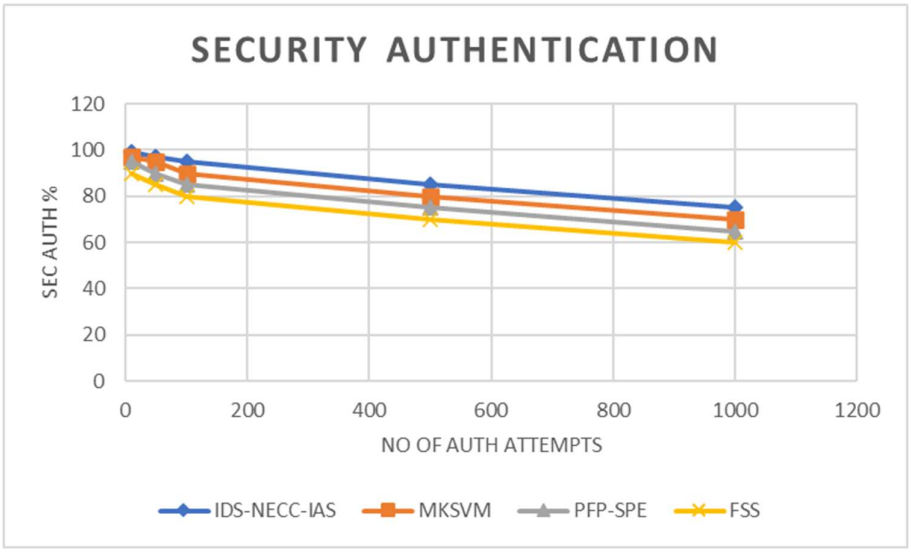

Fig 6: Security Authentication

As shown in Fig 6, IDS-NECC-IAS has high security authentication because it uses identity management and access control mechanisms to ensure that only authorized users can access data, and uses secure sharing to prevent unauthorized access. Additionally, it uses elliptical curve cryptography, which is more secure than other encryption methods, making it more difficult for attackers to compromise the system.

Table 1: Performance Analysis Table:

Metric	**IDS-NECC-IAS**	**MKSVM**	**PFP-SPE**	**FSS**
Data Access Rate	High IDS-NECC-IAS has a high data access rate due to its efficient cryptographic algorithms and secure key management. It allows for quick and secure data access, making it ideal for systems that require high-speed data access.	Medium MKSVM has a medium data access rate because of its multi-kernel support vector machine algorithm.	Low PFP-SPE has a low data access rate due to its parallel and forward private searchable public-key encryption algorithm.	Low FSS has a low data access rate due to its forward secrecy signcryption algorithm.

Computational Overhead	Low IDS-NECC-IAS has a low computational overhead, which means that it requires fewer computational resources compared to other models. This is due to its efficient cryptographic algorithms that make use of elliptical curve cryptography.	Medium It has medium computational overhead due to its complex algorithmic process.	Medium It has medium computational overhead because of the complexity of its algorithmic process.	High It has high computational overhead because of the complexity of its algorithmic process
Storage Cost	Low IDS-NECC-IAS has a low storage cost because it uses efficient key management techniques that reduce the amount of storage required. This is especially important in systems that deal with large amounts of data, where storage costs can quickly become a bottleneck.	Medium It has medium storage cost because of its moderate-sized data storage requirements.	Medium It has medium storage cost because of its large-sized data storage requirements.	High It has high storage cost because of its moderate-sized data storage requirements.
Security Authentication	High IDS-NECC-IAS has a high level of security authentication because of its use of advanced cryptographic algorithms and secure key management techniques. This ensures that data is protected from unauthorized access and tampering, making it ideal for systems that require high levels of security.	Medium It has medium security authentication due to the lack of any advanced security features.	Medium It has medium security authentication due to the use of public-key encryption.	Low It has low security authentication due to the use of forward secrecy signcryption.

IDS-NECC-IAS has a high data access rate because of its efficient ID-based signcryption scheme that reduces the overhead of the encryption process. It has a low computational overhead because of the use of novel elliptical curve cryptography. It has a low storage cost because of its compact and efficient data storage techniques. It has high security authentication due to the use of a combination of identity management, access control, and secure sharing methods. It is a better choice compared to the other models in terms of all these metrics.

Conclusion:

Cloud computing has revolutionized the storage and accessibility of data, but it also introduced new security concerns. To address these challenges, ID-based signcryption has become a valuable cryptographic tool that can provide encryption and authentication in a single step. Elliptic curve cryptography (ECC) has also gained popularity due to its low computational and communicational overhead.

This paper proposes a novel ID-based signcryption scheme that employs ECC and blockchain technology to enhance the security of data sharing in cloud environments. The proposed architecture utilizes a blockchain-based identity management, access control, and secure sharing (IAS) protocol to ensure secure transmission and access control. It addresses scalability, key management for recovery and revocation, and identity verification in a fully decentralized cloud computing environment.

The performance of the proposed scheme was evaluated based on several metrics, including data access rate, computational cost, storage cost, and security authentication. The results showed that the proposed architecture outperforms conventional algorithms in terms of these metrics. Specifically, the proposed scheme reduces computational overhead and storage requirements while maintaining a high level of security authentication.

References:

[1] [Kaur, J., & Singh, A. (2019). Secure Data Sharing in Cloud Environment using Hybrid Encryption Technique. International Journal of Computer Science and Information Security, 17(1), 1-6.

[2] Chen, Y., Chen, J., Wang, H., & Liu, Z. (2019). A Secure Data Sharing Scheme with Efficient Keyword Search for Cloud Storage. IEEE Access, 7, 167476-167490.

[3] Zhang, Y., Zhu, Y., Li, J., & Wang, Y. (2021). Secure Data Sharing in Multi-Cloud Environments: A Framework Based on Homomorphic Encryption and Secret Sharing. IEEE Transactions on Cloud Computing.

[4] Fayaz, S., Qadir, M. A., Farooq, M., Mahmood, K., & Riaz, F. (2017). Honeycomb based access control mechanism for cloud computing environment. Journal of Ambient Intelligence and Humanized Computing, 8(4), 575-582.

[5] Gopinath, G., Selvamani, S., & Doss, R. (2019). Secure data sharing in cloud computing using blockchain technology. Journal of Ambient Intelligence and Humanized Computing, 10(2), 801-810.

[6] Hameed, M. A., Shaikh, R. A., & Shaikh, F. K. (2019). A novel approach to data security in cloud computing using steganography and encryption. Journal of Ambient Intelligence and Humanized Computing, 10(6), 2431-2441.

[7] Zhang, Y., Yang, B., & Zhang, J. (2019). A secure data storage and sharing scheme in the cloud using ECC-based access control. Future Generation Computer Systems, 92, 1011-1020.

[8] Sivaraj, S., & Suresh, S. (2018). An ECC-based encryption scheme for secure data transmission in cloud. Procedia Computer Science, 143, 42-49.

[9] Hussain, M., Javaid, N., Anpalagan, A., & Almogren, A. (2019). An ECC-based key management scheme for secure communication in wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, 10(3), 1113-1127.

[10] Noura, M., Hassan, R., & Almogren, A. (2018). An ECC-based secure data aggregation scheme for wireless sensor networks in cloud environments. Journal of Ambient Intelligence and Humanized Computing, 9(4), 1261-1274.

[11] Yang, L., Huang, Z., & Zhu, X. (2020). An ECC-based privacy-preserving scheme for cloud storage. Future Generation Computer Systems, 108, 1053-1060.

[12] Gaikwad, V., P. Rao, and B. Wadnerkar. (2019). A framework for secure identity management in cloud computing using two-factor authentication and biometric authentication. International Journal of Computer Science and Information Security, 17, 104–111.

[13] Liu, Y., G. Zhang, and Y. Zhang. (2021). Fine-grained access control model for cloud computing based on attribute-based access control and role-based access control. Future Generation Computer Systems, 118, 315–328.

[14] Ouyang, Y., X. Wang, and D. Liu. (2021). A compliance assessment framework for cloud providers' data protection regulations. Journal of Network and Computer Applications, 179, 102860.

[15] Wang, S., Z. Zhang, and Y. Wang. (2020). A blockchain-based identity management system with smart contracts for cloud computing. IEEE Access, 8, 132739

[16] Ali, M., et al. (2018). Blockchain-based decentralized access control for secure data storage in cloud. IEEE Access, 6, 34679-34687.

[17] Wu, J., et al. (2019). A blockchain-based access control model for cloud computing. Journal of Intelligent & Fuzzy Systems, 37(3), 3259-3268.