POLICY AGREEMENT WITH DYNAMIC ELLIPTIC CURVE CRYPTOGRAPHY TO ENHANCE DATA SECURITY IN BLOCKCHAIN CLOUD

A. Banushri, R.A. Karthika
Department of Computer Science & Engineering,
Vels Institute of Science, Technology & Advanced Studies (VISTAS)

Abstract
Cloud computing is an internet-based processing model that is an important component of next-generation computing. It allows the distribution of resources on demand over the Internet. The present encryption algorithms are insufficient for encrypting big amounts of data due to the computation complications encountered in the existing algorithms. An effective methodology for data confidentiality and integrity in cloud systems is proposed in this study. To enhance Cloud Data Security via the Blockchain network, Policy Agreement with Dynamic Elliptic Curve Cryptography is proposed. The Blockchain Ledger information is used to identify users. Users' policies and files are verified, and it is reported whether or not any information has been changed, guaranteeing data integrity. Hyper Mementic Search is used in conjunction with the Block Chain network to optimize information searching and thus decrease authentication time complexity. This method, Policy Agreement with Dynamic Elliptic Curve Cryptography and Blockchain technology, improves cloud data security.

Keywords: Elliptic curve, Blockchain, Cloud computing, Data security, Blockchain ledger.

Nomenclature	
IT	- Information Technology
IaaS	- Infrastructure as a Service
PaaS	- Application as a Service
ECC	- Elliptic Curve Cryptography
ECIES	- Elliptic Curve Integrated Encryption Scheme
LGoE	- Logical Graph of Evidences
MDE	- Modern Digital Era
PA-DECC	-Policy Agreement with Dynamic Elliptic Curve Cryptography
KASE	- Key Aggregation Searchable Encryption
CP-ABE	- Cipher text-Policy Attribute Based Encryption

1.Introduction

Blockchain is a type of distributed ledger in which occurrences are recorded over time. Server update transactions from all involved nodes keep the universal ledger updated. Blockchain increases trust by conducting a validation process (Merkel tree) on each hashed transaction, making the transactions immutable. Due to the distributed nature of blockchain, there is no single point of failure, and each network node replicates the transaction data. Transactional integrity is ensured by blockchain. As a result, transactions between two individuals occur more quickly and with less need for mediation.

Blockchain technology has the ability to be permission-less or permission-granting. Permissionless blockchains, additionally referred to as public blockchains, are accessible to all users. The presence of an enormous potential blockchain that is publicly accessible, such as the digital currency, may not be appropriate for all company owners seeking authority over systems for processing transactions. In complex operations, business processes can function alongside customized solutions, limiting outsiders with specific requirements and needs. Scalability, regulatory, and oversight of development are some of the difficulties in permissionless blockchains as the chain's size grows. Companies that want to keep their own authority over the blockchain network and only enable trustworthy parties to join it began looking into alternatives. Another name for a blockchain that gives rights is a permissions blockchain.

We must cope with a wide range of threats and attacks when integrating blockchain. When we employ the Hyperledger fabric, it acts as a closed encrypted blockchain with network participants having less knowledge of data compared to the organization's leader, which prevents the most frequent 51% attack from occurring. Sybil attacks are the second most common form of blockchain network attack. The sybil attack serves to harm the image of the system through the generation of many different pseudonymous identities. By using elliptic curve digital signatures to authenticate and validate identities, the proposed model tries to eliminate the sybil attack.

The elliptic curve algorithm is widely used in the protection of miniature automated devices. ECC will be used for pictures and other multimedia content as well as hidden text protection and text allocation. As a result, ECC-based cryptology research is becoming more interdisciplinary, combining with expanding fields like math, digital, electrically, and computer science.

Cloud computing refers to a method of providing services related to information technology (IT) that uses web-based tools and applications for accessing assets via the World Wide Web rather than a direct link to a server. Files may be saved to a remote computer instead of a proprietary hard drive or local storage device when using cloud-based storage. Data and software apps can be obtained by any electronic device in internet access. Controllable cloud service components include network balance, connectivity, security, and information size. Since the data owner and the supplier of services do not reside in the same confided in domain, data privacy and security pose significant problems with cloud adoption. The overwhelming majority of infrastructure service providers (IaaS). In infrastructure as a service (IaaS) and application as a service (PaaS) deployments, security is becoming increasingly essential. (PaaS). Throughout its life, data goes through several phases. Create, transfer, use, exchange, shop, archive, and destroy are the phases. At all levels, computer protection is critical. An secure data lifespan refers to the entire process of generating data and deleting it from the cloud.

A number advancements associated to the blockchain technology have been just consolidated, notably: the opening of

blockchain 2.0, the blockchain network Ethereum , the Hyperledger Fabric , the enhancement of clever commitments and the use of encoding on the data flowing through the blockchain, such as Elliptic Curve Cryptography (ECC) [1]. Creating value and integrating data while improving privacy and data security is a significant task for modern big data organizations. Data security and privacy should be managed and empowered by storage platforms. Many researchers have lately proposed new approaches to cloud privacy and security empowerment. The designed technique ought to offer effective privacy and security of data schemes while also allowing for cross-organizational data sharing [2]. For cross-hospital diagnostics and study expansion, health information sharing is undoubtedly needed. In traditional techniques, there is constantly a tradeoff between health information precision and patient privacy [3].

If the data being transferred is confidential, the cloud storage service may be untrustworthy. As a result, any data sent can be intercepted or changed by a malicious person. The Cloud presents security problems, particularly for confidentiality and data integrity, as data is managed outside of cloud users' organizational structures and the company providing the service has unrestricted access to the data [4]. In a single master key system, the master key is the same for all nodes. This technique uses the master key to secure the message being sent between the sensor nodes during data transmissions, and it is simple to apply with only a few memory spaces. Any adversary who obtains a master secret jeopardizes the entire company [6].

Existing data processing techniques result in high computing overhead as well as unsecure data sharing, while an effective and safe data sharing mechanism can help microgrid business administration [7]. Providing patient data with other organizations such as research institutes and colleges is also regarded as a valuable social input for enhancing research and investigations [5]. With the arrival of 5G communication technologies, obstacles among patients, hospitals, and other groups offering excellent services are being removed. Patients save time, money, and risk through utilizing digital healthcare service choices [8]. In accordance to the security analysis, this plan has the potential to generate superior results. Our method saves approximately 64.55% of the transmission's overhead while validating the same number of verified messages in less time than other schemes. Incentive contracts founded on the theory of games could enable EV power trading by utilizing electricity currency rewards. This mechanism enhances the willingness and involvement of electric vehicles in network operations and stability interactions [9].

Small automated devices are frequently protected using the elliptic curve technique. ECC will be used to protect hidden text, allocate text, and secure images and other multimedia material [10]. The blockchain framework and cloud processing technology work together to reduce computational expenses in a variety of ways. Existing methods help identify anonymous papers sent as cloud server requests. When authorized users submit anonymous document requests, the cloud strengthens security and stops unauthorized users from accessing documents. However, the primary concern is the level of access authorized users have to the owner's sensitive data. [11]. The Elliptic Curve Integrated Encryption Scheme (ECIES) algorithm is employed in mobile devices to secure packets before they are sent to a cloud server. The SDN controller uses the SHA-256 Cryptographic Hash Algorithm to keep proof derived from information and user signatures on blockchain. The following processes are the responsibility of an authorized investigator: identification, evidence gathering, evidence analysis, and producing reports based on the Logical Graph of Evidences. (LGoE) [12].

Cloud computing is a way of providing information technology (IT) services that uses web-based tools and applications to access

assets via the Internet rather than connecting directly to a server [13]. EC is commonly used to better ensure the safety of open communication networks and to grant access to the Modern Digital Era to specific people with verified identities. (MDE). MDE users use a variety of technologies, such as networking sites, the cloud, and the IoT sector. Regardless of the tool, the whole system must be capable of safeguarding the users' confidentiality and privacy [14]. In recent years, the Internet-of-Things (IoT) sector has grown in significance, with an increasing number of devices or sensors connected to the World Wide Web and transmitting various kinds of data. In complex IT systems, it is usually essential to make sure that the IoT devices transferring the data have been authorized system components before delivering data to a storage server [15].

2. Proposed Methodology

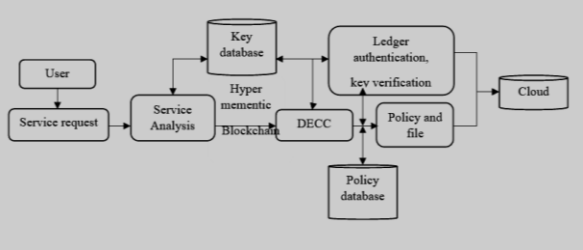

Fig. (1) Block Diagram

A technique for improving the security of cloud data is Policy Agreement with Dynamic Elliptic Curve Cryptography. (PA-DECC). The user requests some cloud services, which are then evaluated with the Service Analysis tool. Dynamic elliptic curve encryption is used to validate user profiles and encrypt cloud data. To enhance the security of the blockchain environment, a smart contract was created. The policy database stores the user access control guidelines that are used to legalize the authorized user policy. Finally, for authentication, key verification is done in the Ledger, and all network data is saved in the cloud. Users' policies and files are verified, and it is reported whether or not any information has been changed, guaranteeing data integrity. To maximize information searching and thus reduce authentication time complexity, Hyper Mementic Search is used in conjunction with the Block Chain network. Policy Agreement with Dynamic Elliptic Curve Cryptography and Blockchain Technology enhances online data security. Figure 1 shows Diagram of Blockchain.

3. Dynamic Elliptic curve Cryptography

ECC is a cryptographic method used in cryptocurrencies such as Ethereum and Bitcoin, as well as one-way data, email, and software encryption. It is similar to the RSA (Rivest-Shamir-Adleman) algorithm.By employing elliptic curve geometry, ECC provides security between key pairs for public key encryption.Because of its smaller key size and ability to maintain security, ECC has lately gained popularity. In contrast to RSA, ECC's public key cryptographic system method is based on the algebraic organization of elliptic curves over finite fields.

4. Lagrange's theorem for point selection

The elliptic curves dynamic point selection is based on user subgroups using a Lagrange's theorem.

Let H be any order 'n' subgroup of an order m finite group G. (Message). Assume H is G's coset. Consider the fact that each coset of H has n unique components. Let n denote the position of the given point on the curve. (the smallest number of times the point must be added to itself to get zero).

Step 1: Define, for all a, b $\in$ G, ab(mod H) if and only if $b^{-1} * a \in H$. Then the relation, a= (modH), "congruence modulo H", is an equivalence relation.

For all a $\in$ G, have $a^{-1} * a = e \in G$

So, a $\equiv$ a (mod H) thus $\equiv$ is symmetrically.

Step 2: For a$\in$ G, the equivalence class [a] is nothing but the left coset a * H. Further G is partitioned into distinct.

[a, b] = { x Î G / x $\equiv$ab (mod H) }

Step 3: Let G be a finite group and let H be a subgroup then o (H) |o (G).

Followed by the Step2,

$$G = a_1 b_1 * H \cup a_2 b_2 * H * \dots a_n b_n \cup H$$

Where the $a_1 b_1 * H$ are the distinct coset of G (and have no common elements)

Step 4: Consider a point P, message m and subgroup point x, y such that

$$m = G + \frac{x}{2y \bmod (H)}$$

$$a_1 = m - x_1 - x \bmod (H)$$

$$b_1 = m(x_1 - y_1) - y \bmod (H)$$

Using an elliptic curve over k(p) or k, determine the point value m (a,b).(2n). Then, in plain text, select the letter's corresponding point on the alphabetic table and the secret key value as d. Calculate the location using the d*e formula: e= (). Finally, designate e to be the public key and "d" to be the private key

Step 5: Encryption

. Allow 'A' to choose a point number p as plaintext and a private key d for the sender. Then, as cipher text, compute a set of points on the text. The cipher messages are as follows. Hence

Step 6: Decryption

Let 'B' calculate p, the plaintext, after getting message m using the formula p=m-(d*m). The minus sign here indicates to add the inverse.

6. Results and Discussion

This Proposed Method PA-DECC was implemented using Visual studio tool for Public Cloud(Accord framework) by using 1000 transactions with file size 100 MB,200MB,300MB.The performance metric used are throughput, Execution time for Encryption and Decryption, Access Control ,Delay time etc.,. This proposed Policy Agreement with Dynamic Elliptic Curve Cryptography (PA-DECC) framework has been compared to existing Key Aggregation Searchable Encryption (KASE), Cipher text-Policy Attribute-Based Encryption (CP-ABE) and AuthPrivacyChain**.** Figure 2 demonstrates the metric analysis use of throughput.

Table 1: parameter values

Parameter	**Value**
File size	100MB, 200MB, 300MB
Transaction	1000
Cloud type	Public cloud (Accord Framework)
Tool	Visual studio
Number of users	500

.

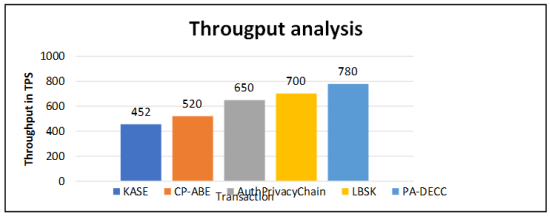

Fig. (2) Analysis of metric with throughput

The PA-DECC method has a 780tps higher transaction throughput rate than other existing methods. The PA-DECC to authenticate each user request transaction is based on ECC with fast encryption and low authentication time, improving the throughput rate over other methods.

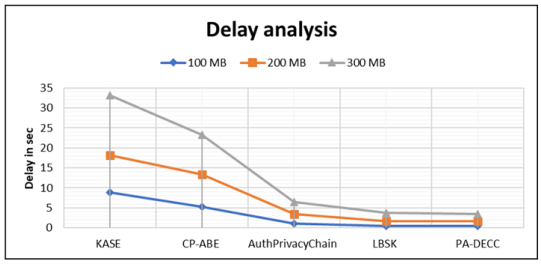

Fig. (3) Delay Analysis

The proposed system proves higher-end security's outstanding performance with a minor authentication delay of standard crypto ECC hyperledger blockchain. In this proposed method, each user policy agreement is verified and then the cloud database is allowed. Figure

3 shows PA-DECC method has a 1.8sec low authentication delay for 300 MB data than AuthPrivacy 3sec, CPABE 10sec and KASE 15sec of delay. The proposed Cloud System method's superiority is shown with PA-DECC comparing LBSK , AuthPrivacy, CP-ABE, and KASE.

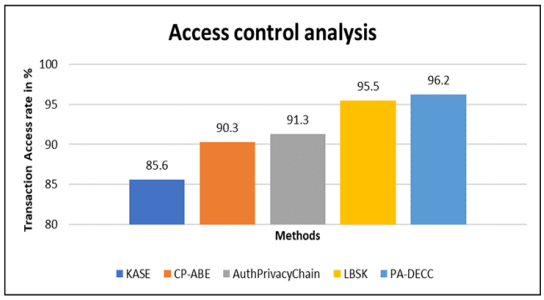

Fig (4). Analysis of Access and Control

The rate of access demonstrates in figure 4. The access rate in this operation is decided by the user accessing the data without interruption and retrieving it from a cloud database. When compared to another existing technique, the proposed PA-DECC method has a transaction access rate of 96.2%.

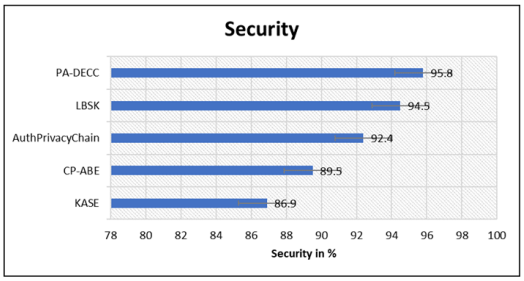

Fig. (5) PA-DECC Analysis

This analysis of the proposed PA-DECC method's security rate shows in figure 5, that it provides 95.8% more security than the current methods KASE and CP-ABE, which provide 86.9% and 89.5% less security, respectively. The suggested method is used to authenticate data encryption using a DECC algorithm, which increases the security of the blockchain network.

7. Conclusion

This Policy Agreement with Dynamic Elliptic Curve Cryptography (PA-DECC) structure substantiates the user policy whether any modifications is done in the data. Blockchain Network permits cloud to verify the user service list. This proposed structure has been designed to verify the user privacy agreement policy of each transaction using DECC. Policy and file Verification is done for the users and reports if any information is modified or not and thus maintains Integrity of Data.This method reduces the authentication time of block chain users. The experimental results show better and efficient results in securing storage in cloud computing and provide efficient data privacy solutions.

References

1. de Moraes Rossetto, Anubis Graciela, Christofer Sega, and Valderi Reis Quietinho Leithardt. "An Architecture for Managing Data Privacy in Healthcare with Blockchain." *Sensors* 22.21 (2022): 8292.
2. Alkhliwi, Sultan. "An efficient dynamic access control and security sharing scheme using blockchain." (2022).
3. Lee, Jung-San, et al. "Medical blockchain: Data sharing and privacy preserving of EHR based on smart contract." *Journal of Information Security and Applications* 65 (2022): 103117.
4. KOTEL, Sonia, and Fatma SBIAA. "A Data Security Algorithm for the Cloud Computing based on Elliptic Curve Functions and Sha3 Signature." *International Journal of Advanced Computer Science and Applications* 13.3 (2022).
5. Jamjoom, Mona, Hussein Abulkasim, and Safia Abbas. "Lightweight Authenticated Privacy-Preserving Secure Framework for the Internet of Vehicles." *Security & Communication Networks* (2022).
6. Lin, Hua Yi. "Integrate the hierarchical cluster elliptic curve key agreement with multiple secure data transfer modes into wireless sensor

networks." *Connection Science* 34.1 (2022): 274-300.

7. Shang, Jian, Runmin Guan, and Yuhao Tong. "Microgrid Data Security Sharing Method Based on Blockchain under Internet of Things Architecture." *Wireless Communications and Mobile Computing* 2022 (2022).

8. Hewa, Tharaka, et al. "Multi-access edge computing and blockchain-based secure telehealth system connected with 5G and IoT." *GLOBECOM 2020-2020 IEEE Global Communications Conference*. IEEE, 2020.

9. Chen, Xiaofeng, and Xiaohong Zhang. "Secure electricity trading and incentive contract model for electric vehicle based on energy blockchain." *IEEE access* 7 (2019): 178763-178778.

10. Sowmiya, B., et al. "Linear elliptical curve digital signature (LECDS) with blockchain approach for enhanced security on cloud server." *IEEE Access* 9 (2021): 138245-138253.

11. Hylock, Ray Hales, and Xiaoming Zeng. "A blockchain framework for patient-centered health records and exchange (HealthChain): evaluation and proof-of-concept study." *Journal of medical Internet research* 21.8 (2019): e13592.

12. Velmurugadass, P., et al. "Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm." *Materials Today: Proceedings* 37 (2021): 2653-2659.

13. Saravanan, Prabakeran, et al. "Hybrid Crypto System Using Homomorphic Encryption and Elliptic Curve Cryptography." *i-Manager's Journal on Computer Science* 7.1 (2019): 36.

14. Ullah, Shamsher, et al. "Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey." *Computer Science Review* 47 (2023): 100530.

15. Nita, Stefania Loredana, and Marius Iulian Mihailescu. "Elliptic Curve-Based Query Authentication Protocol for IoT Devices Aided by Blockchain." *Sensors* 23.3 (2023): 1371.