Applying Encryption and Decryption Algorithm for Data Security in Cloud

Fatima Ghaiyur Hayat
Department of Computer Science
Christ University
Bangalore, India

Mithun B.N.
Department of Computer Science
Christ University Bangalore, India

DOI: 10.56201/ijemt.v8.no2.2022.pg16.23

Abstract
Data security refers to the method involved with safeguarding information from unapproved access and information corruption all through its lifecycle. Data security includes information encryption, hashing, tokenization, and key administration practices that protect information across all applications and stages. Cloud framework for getting to information with mysterious confirmation gives safer client verification, client revocation and prevents replay attacks.
Access control is handled on cloud KDCs it is overall safer aimed at information encryption. Produced decentralized KDC's are then gathered by (KGC). Framework gives confirmation to the client, in which just framework approved clients can unscramble, view the put away data. Client approvals and access control plot is presented in cloud, which is important for hindering replay attacks and supports change of data set aside in the cloud. The entry control plot is procuring thought since just upheld clients should approach genuine examine. Our arrangement thwarts maintains creation, replay attacks, scrutinizing and adjust data set aside in the cloud. We in like manner address client disavowal. The issues of endorsement, access control, security affirmation should be handled simultaneously.

Keywords *Decentralized KDCs, Access control, Cloud, ECC, Encryption, Decryption*

I. INTRODUCTION

Research in the cloud computing is reached to its ideal and getting a great deal of consideration from each area in world. Development, reception of existing advancements and standards is distributed computing. Distributed computing is fundamentally where clients who can re-appropriate their calculation and stores information/data to the cloud utilizing the Internet. Distributed computing offers types of assistance (for example Office Web Apps), stages for designers to compose applications (e.g., Cloud Sigma, Windows Azure, Amazon's S3), foundations (e.g Nimbus, Amazon's EC2) these application presents cloud administrations. A large part of the information put away in cloud like interpersonal organizations, clinical records which are exceptionally delicate and requires security. Protection and security are in this way exceptionally basic issues in distributed computing. Significant thing is, the client ought to confirm itself prior to starting any exchange, and it should be safeguard that different clients don't have the foggiest idea about the congruity of the client. There is need of policing other than specialized answers for guarantee wellbeing, protection of the information [1]. The cloud can hold the client for capacity with for various reason, and in like manner, the actual cloud responsible for the administrations it gives. The respectability of the client who stores the data is additionally ensure.

Security gave in the cloud, is liable for different clients don't have the foggiest idea about the congruity of the other client. The legitimacy of the client who stores the information is likewise confirmed.

The cloud is likewise defenseless for server conniving attack and data adjustment. The rival can think twice about servers in server conspire attack, so server can change information records despite the fact that the servers are inside homogenous. Encryption on information is expected to give secure information storage . Nonetheless, the information is much of the time changed and this powerful property should be taken into considered while planning viable secure storage methods.

Responsibility isn't answerable for the cloud nor should clients not accept any tasks mentioned or performed. It is expected to have log of the exchanges that are performed.

Equal and appropriated frameworks characterizes, various hubs associated in the organization, it very well may be characterized as an assortment of handling components that impart and work together to accomplish objective. The hub to hub correspondence is done through messages. Green processing additionally manages the energy utilization during data move between hubs to hubs in the organization. The principal objective of the green processing is to diminish the expense by decreasing the energy utilization during data move between hubs to hubs.

The most widely recognized security risk enthusiasm for through an entrance control procedure is by essentially following a suitable client through an entryway. Frequently the lawful client will keep the door open for the gatecrasher. This chance element can be diminished through security mindfulness preparing of the populace, or more dynamic means like entryways. Security related applications risk is diminished by utilizing a sally port. Now and then called a wellbeing of

information man trap, where administrator intercession is required probably to get approved distinguishing proof.

Verification of information has appropriateness to different fields. In human studies, collectibles, craftsmanship a typical issue is distinguishing that a given relic was delivered by someone in particular or was created in time of history or a specific spot. In software engineering, ensure an individual's character is frequently expected to get to safely approval of data and frameworks.

Cloud waiter access control is getting thought since just affirmed clients genuinely should have section to adequate organization. Immense data is being put away on cloud servers; information put away on cloud has more exact data. Touchy or exact data is online long range interpersonal communication where clients (individuals) store their own It's important to guarantee intangibility of the client; not barely enough to record the items or data safely in the cloud. At times a client might want to store some extremely touchy data yet doesn't have any desire to be known, clients needs substantial security for their data or information that will be put anyplace. The client could have to post a comment on things; article anyway needn't bother with his/her conspicuous verification to be revealed. Anyway, the client should have the ability to infer to

substitute clients that he/she is a genuine client who set aside the information without revealing the ID or character.

Past work on access control in the cloud are amalgamated in nature. No matter what the way that a few isolated or decentralized approaches were existing doesn't support unmistakable confirmation for a client. Earlier work gives security safeguarding endorsed admittance control in the cloud. Regardless, the previous work take amalgamated or integrated technique where single key allotment center (KDC) scatters single mystery keys and credits to all clients.

II. LITERATURE SURVEY

[1] To guard the data from outside risk different cryptography techniques are used, for instance, symmetric, amiss and hashing. In this paper examination of AES which is a symmetric methodology is done with ECC. Results got are examined in view of different limits that that incorporate capacity, encryption time, decoding time, torrential slide impact and connection. Gained results show that the impact of this combination approach is critical and better than different calculations.[10]

[2] Information integrity in the limit model of CLOUD computing is a significant security concern. This could be an immediate consequence of the
Various spots information may dwell. After that security protection and security of this spread out data could be at any stake. The data at such different regions should be secure in the distributed storage. What should be centered this is the way a safer model can be given to the cloud design. Significantly, here a cross breed approach

ECC-AES encryption calculation is applied over the data. Considering this, further update or improvement upon the data will be concentrated here.[11]

[3] Data security is an important task in today's life. Information security should be possible utilizing GPS gadget. Among PC client generally use information in electronic format. The most effective method to give a security to data is important. In this paper, we propose a Location Based Data Security System to get information by applying Encryption-Algorithm and co-ordinate utilizing GPS gadget. Encryption method for productive secure number examination. The encryption technology restrict the location of data decryption. To satisfy the need of an area subordinate methodology area subordinate information encryption calculation is required.
An objective scope/longitude co-ordinate is resolved first and foremost. The co-ordinate is consolidated with an arbitrary key for information encryption. The beneficiary can decrypt the code text when the co-ordinate procured from GPS collector is coordinated with the objective co-ordinate. GPS-based encryption is an inventive strategy that utilizes GPS-innovation to encode area data into the encryption keys to give area based security. GPS based encryption includes one more layer of safety top of existing encryption techniques by limiting the decoding of a message to a specific area. Our experimental results not only validate the effectiveness of our scheme, but also demonstrate that the proposed integer comparison scheme performs better than previous bitwise comparison scheme [12]

[4] During the last decades, data security has turned into a major issue. Encrypting and decrypting data have recently been widely investigated and developed because there is a demand for a stronger encryption and decryption which is very hard to crack. Cryptography plays major roles to fulfillment these demands. Nowadays, many of researchers have proposed many of encryption and decryption algorithms such as AES, DES, RSA, and others. Be that as it. may, the greater part of the proposed algorithms encountered some problems, for example, such as lack of robustness and significant amount of time added to packet delay to maintain the security on the communication channel between the terminals. In this paper, the security goals were improved through "A New Approach for Complex Encrypting and Decrypting Data" which keeps up with the security on the correspondence channels by making it challenging the attacker to predicate a pattern as well as speed of the encryption / decryption scheme[13]

[5] The developing popularity and development of data mining technologies carry genuine danger to the security of person's delicate. data.
An arising research point in data mining, known as privacy preserving data mining (PPDM), has been extensively studied in recent years. The basic idea of PPDM is to modify the data in such a way so as to perform data mining algorithms effectively without compromising the security of sensitive information contained in the data.
Current investigations of PPDM for the most part of center around how to decrease the security hazard brought by information mining activities, while indeed, undesirable revelation of delicate data may likewise occur during the time spent information gathering, information distributing, and data (i.e., the information mining results) conveying. In this paper, we view the privacy issues related to data mining from a wider perspective and investigate various approaches that can help to protect sensitive information

Specifically, we distinguish four unique kinds of clients associated with information mining applications, in particular, information supplier, information gatherer, information excavator, and leader. For each sort of client, we talk about his security concerns and the techniques that can be taken on to protect delicate data.
We briefly present the essentials of related research topics, review state-of-the-art approaches, and present some preliminary thoughts on future research directions. Other than investigating the privacy-preserving approaches for each kind of client, we also review the game theoretical approaches, which are proposed for analyzing the collaborations among various clients in a data mining scenario, every one of whom has his own valuation on sensitive information [14]

III. OBJECTIVES

- The main objective of this project is to implement security to data by using encryption and decryption methods
- Unraveling of archive is allowed only for system approved/confirmed clients.
- Our plan supports prevention of replay attack , creation, change, seeing the information that set aside in the Cloud.

IV. PROJECT OUTCOME

After the completion of the project we will be able to-

- We have given a decentralized admittance control procedure unknown verification, which gives client denial and prevents replay attacks.
- The cloud doesn't have the identity idea about the character of the client who stores data, yet just checks the client's accreditations.
- One limitation is that the cloud knows the entrance strategy for each record put away in the cloud.
- Our plan additionally has the additional component of access control in which just legitimate clients can decode the put away data.

V. PROPOSED SYSTEM

- It gives access control taking into account client information. Access arrangements for client will be allotted and with the entrance strategies unknown validation is given to the client who requirements to store secure data on cloud.
    - Approvals are given to clients on the reason on key generation.

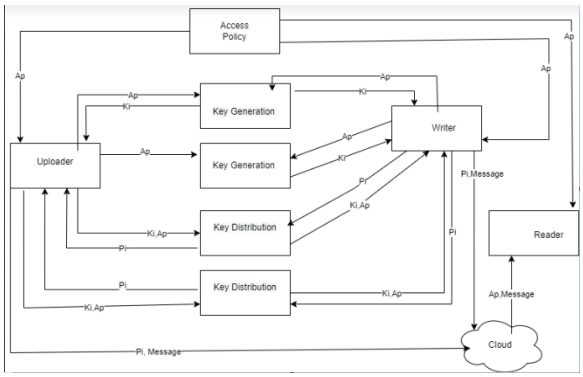

Fig 1: System architecture

- It gives access strategy on base of clients information. It gives security to client information in light of the trait based encryption methodology.
- It gets data on the reason of access strategy and access control method. Security controls are safeguarded watches or counter measures to avoid, check or limit security gambles related with individual property.

VI. METHODOLOGY

- We present our distributed storage model, adversary model and the suspicions we have made in the paper.
- that the cloud managers can be keen on review client's substance, yet can't adjust it. Clients can have either perused or compose or the two gets to a document put away in the cloud.

- We emphasize that cloud to adopt a decentralized strategy while conveying secret keys and characteristics to clients.

- The ciphertext C with mark is c, and is shipped off the cloud. The cloud confirms the mark and stores the ciphertext C. At the point when a reader needs to read, the cloud sends C. In the event that the client has ascribes coordinating with access strategy, it can decode and receive back unique message.
- The confirmation cycle to the cloud, it relieves the singular clients from time consuming checks. Whenever a reader needs to read a few information put away in the cloud, it attempts to decode it utilizing the mystery keys it gets from the KDCs.

VII. FLOW CHART

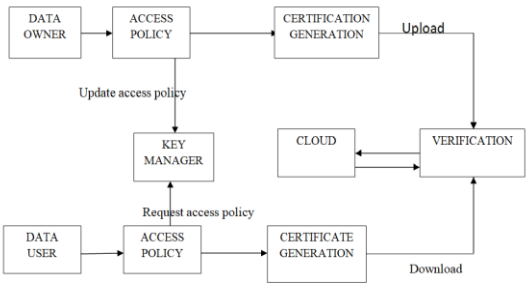

Fig 2: Flowchart

VIII. CONCLUSION

- The disadvantage of cloud administrations is the low information security which might be defeated through exceptional techniques and should be secured.
- In particular, for the generation of the key, ECC is utilized to diminish the intricacy of the tasks. Because of the relaxed size, the upgrade of ECC is obviously superior to other cryptographic methods.
- AES in mix with ECC can improve the advancement and security of the information. Notwithstanding, much security is as yet required in the future to grow the idea of distributed computing through cryptographic methods
- By using attribute based encryption the user can encrypt the data or user content.
- Using such type of encryption we can preserve the secrecy of the user from the administrator means user is anonymous
- As cloud knows the access policy, for the contents stored in the cloud, contents are not secret. The system is decentralized .The efficient and working attribute are the key factors for the success of the system.

IX. REFERENCES

[1]Shukla, D.K.; Dwivedi, V.K.; Trivedi, M.C. Encryption algorithm in cloud computing. *Mater. Today Proc.* 2020, *37*, 1869–1875.

[2]https://cryptobook.nakov.com/asymmetric-key-ciphers/ecc-encryption-decryption

[3]https://www.cloudflare.com/en-in/learning/ssl/what-is-encryption/

[4] Bhardwaj, K.; Chaudhary, S. Implementation of elliptic curve cryptography in 'C'. *Int. J. Emerg. Technol.* 2012, *3*, 38–51.

[5]Ogiela, U. Cognitive cryptography for data security in cloud computing. *Concurr. Comput. Pr. Exp.* 2019, *32*, e5557.

[6]Sood, S.K. A combined approach to ensure data security in cloud computing. *J. Netw. Comput. Appl.* 2012, *35*, 1831–1838. [Google Scholar]

[7] Mendonca, S.N. Data security in cloud using AES. *Int.J.Eng. Res. Technol.* 2018, *7*.

[8] Suresha, R.G. Enhancing security in cloud storage using ecc algorithm. *Int. J. Sci. Res.* 2013, 2–8. Available online: https://www.ijsr.net/archive/v2i7/MDIwMTM3NA==.pdf (accessed on 22 October 2021).

[9] Abbas, S.; Maryoosh, A.A. Improving data storage security in cloud computing using elliptic curve cryptography. *IOSR J. Comput. Eng.* 2015, *17*, 48–53.

[10]SamikshaSharma,VinayChopra"ANALYSIS OF AES ENCRYPTION WITH ECC"

[11]"Enhanced Cloud Storage Security Using ECC-AES A Hybrid Approach"

[12] Borse Manoj V. Bhandure Harshad D. Patil Dhiraj M. Bhad Pratik B "Location Based Encryption-Decryption Approach for Data Security"

[13] Obaida Mohammad Awad Al-Hazaimeh" A NEW APPROACH FOR COMPLEX ENCRYPTING AND DECRYPTING DATA"

[14] SHASHANK, S.K. Saravanan, G. Rekha" Information Security in Big Data using Encryption and Decryption"