International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 2 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT2062160

Ensuring Better Privacy of Cloud Storage Using Elliptic Curve Cryptography

Prof. A. V. Deorankar*, Khushboo T. Khobragade
CSE Department, Government College of Engineering Amravati, Maharashtra, India

ABSTRACT

Cloud technology is very profitable for the business evolution. In cloud computing, the data is mostly outsourced. The security and integrity of the data in the cloud system is always a main worry. Because of rapid development of adaptable cloud services, it becomes increasingly vulnerable to use cloud services to share data in a friend circle in the environment of cloud computing. The user privacy is also an important concern. Many systems and technique are being developed to address these issues, but still there is always a scope of improvement. While addressing the issues related to the user privacy and data security and integrity, we must consider the efficiency of the system while accessing and searching for the data. In this paper, we discuss about the major challenges in cloud environment. Also, presented is a brief overview on proposed system with elliptical curve cryptography is a public key encryption technique uses the properties of elliptic curve in order to generate keys instead of using the traditional methodology of generation of keys.

Keywords : Secure Transmission, Public Key Infrastructure, Privacy Preserving in cloud, Biometric in Cloud

I. INTRODUCTION

Cloud computing is broadly grasped by abundant association and people in view of its different amaze focal points like colossal size data storage, immense calculation, low-value benefit and adaptable come within reach of to get to the data. The fundamental idea driving cloud computing is virtualization. In cloud computing, virtualization intends to make a virtual variety of a asset, for example, a server, storage gadget. Cloud computing is a dominating administration of cloud storage, which enables data owner to store their data from their nearby computing system to cloud. Numerous clients store their data on cloud storage.

The integrity is the primary concern of the data. Once the data is outsourced, the data owner would be stress about his data in the cloud. In this manner, the greatest concern is the means by which to decide if a cloud storage system and specialist organization meet the client requirements for data security. In this manner, it is vital and noteworthy to increase proficient auditing plan to fortify data owners' confidence is cloud storage. There are different auditing models have been proposed, they can be sorted into two sorts Private auditing model and Public Auditing Model. Generally, in Private auditing model, the integrity of outsourced data is confirm by the data owner which is dependent on the two-party storage auditing convention. In this method, the data owner ought to have mastery. In some cases it expands the overhead of data owner and, it likewise happens the CSP cannot convince each other for the outcome.

The next concern is the accessing the data from the cloud is related to the security mechanism. Whereas encryption used as a Traditional Key generation mechanism is not capable of countering the advance attacks deployed by the attackers. In such a situation, an encryption method based on user feature could be an efficient way. It offers a unique key based on a user attribute, which can make the unauthenticated data access very difficult but still there is the definite scope of error. To overcome any such event and hybrid approach of an attribute-based mechanism coupled with user fingerprint can improvise the system and make the unauthenticated data access nearly impossible.

Focusing way too much on the security concerns and implementing the resolution for the same can also lead to the degradation in the efficiency of the data access by the legitimate user. Thus focusing solely on improving the security measures and ignoring efficiency cannot be a good idea. The system must be secure but the efficiency in the data access and searching of data must be maintained.

In this paper, we present the propose work on available mechanisms and researches which in some or other way tried to overcome or counter the above discussed issues. Firstly, we will cover the researches related to the implementation of biometrics for cloud environment. Then we will discussed about the existing public auditing schemes and try to find out which one could be a better option. After that, we will focus on the encryption and key distribution mechanism with an efficient way to search the data over encrypted environment.

II. REVIEW OF LITERATURE

Biometric identification has turned out to be progressively famous as of late. With the advancement of cloud computing, data owners are persuaded to redistribute the expansive size of biometric data and identification errands to the cloud to dispose of the costly storage and calculation costs, which, be that as it may, conveys potential dangers to clients' privacy. In this investigation [1], the author proposes a productive and privacy-saving biometric identification-redistributing plan. In particular, the biometric To execute a biometric identification, the database owner encodes the question data and submits it to the cloud. The cloud performs identification tasks over the scrambled database and returns the outcome to the database owner. Here author accept that the biometric data has been handled to such an extent that its portrayal can be utilized to execute biometric coordinate. Without loss of simplification, the system target fingerprints and utilize FingerCodes to speak to the fingerprints. To assess the proficiency and security prerequisites, the author actualizes another encryption calculation and cloud authentication confirmation. The evaluation result and examination indicate it can oppose the potential assaults.

In this study [2], the author proposes a lightweight secure access control conspire for IMDs amid crises. Our plan uses patient's biometric data to forestall unauthorized access to IMDs. The plan comprises of two levels: level 1 utilizes some essential biometric data of the patient and it is lightweight; level 2 uses patients' iris data for authentication and it is extremely viable. In this exploration, the author additionally makes commitments to human iris check: we find that it is conceivable to perform iris confirmation by looking at halfway iris data instead of the whole iris data. The evaluation after effects of the system demonstrates that the safe access control plot is exceptionally viable and has little overhead (henceforth possible for IMDs). In particular, the false acknowledgment rate (FAR) and false dismissal rate (FRR) of our safe access control conspire are near 0.000% with a reasonable edge, and the memory and calculation overheads are satisfactory.

For security, it is necessitated that the customer does not pick up anything on the database and the server ought not get any data about the asked for biometry and the result of the coordinating procedure. The proposed convention in this study [3] pursues a multi-party calculation approach and makes broad utilization of homomorphic encryption as fundamental cryptographic crude. To keep the convention intricacy as low as could be expected under the circumstances, a specific portrayal of fingerprint pictures, named Finger code, is received. In spite of the fact that the past chips away at privacy-saving biometric identification center around choosing the best coordinating character in the database, this arrangement is a nonexclusive identification convention and it permits to choose and report all the enlisted personalities whose separation to the client's Finger Codes is under a given limit. Variations for basic authentication reasons for existing are given. According to the evaluation result, these conventions gain a remarkable data transfer capacity sparing (around 8 to 24%) whenever contrasted and the best past work and its computational many-sided quality is still low and appropriate for down to earth applications.

Here in [4], the author introduces a productive coordinating convention that can be utilized in numerous privacy-safeguarding biometric identification systems in the semi-fair setting. Our most broad specialized commitment is another backtracking convention that uses the result of evaluating a jumbled circuit to empower productive neglectful data recovery. We additionally present a more effective convention for computing the Euclidean separations of vectors and streamlined circuits for finding the nearest coordinate between points held by one gathering and an arrangement of focuses held by another. For evaluation reason, usage of a down to earth privacy-safeguarding fingerprint coordinating system is been finished. The fundamental downside is that present conventions for privacy-protecting calculations are extremely costly and unfeasible for genuine scale issues. In this work, the author has demonstrated that those expenses can be significantly diminished for an expansive class of biometric coordinating applications by creating productive conventions for Euclidean separation, finding the nearest coordinate, and recovering the related record.

Data sharing turns into an outstandingly alluring administration provided by cloud computing stages in view of its accommodation and economy. As a potential procedure for acknowledging fine-grained data sharing, attribute-based encryption (ABE) has drawn wide consideration. The issue of at the same time accomplishing fine grainedness, high productivity on the data owner's side, and standard data privacy of cloud data sharing in reality still stays uncertain. This paper [5] addresses the testing issue by proposing another attribute-based data sharing plan reasonable for asset restricted portable clients in cloud computing. This plan dispenses with a lion's share of the calculation undertaking by including system public parameters other than moving fractional encryption calculation disconnected. What's more, a public ciphertext test stage is performed before the decryption stage, which disposes of the vast majority of the calculation overhead because of ill-conceived ciphertexts. For data security, a Chameleon hash work is utilized to produce a prompt ciphertext, which will be blinded by the disconnected ciphertexts to get the last online ciphertexts.

Identity-Based Encryption (IBE), which rearranges the public key and endorsement administration at Public Key Infrastructure (PKI), is a critical option in contrast to public key encryption. In any case, one of the primary productivity downsides of IBE is the overhead calculation at Private Key Generator (PKG) amid client disavowal. Here in [6], going for handling the basic issue of identity denial, the author brings re-appropriating calculation into IBE and presents a revocable IBE conspire in the server-supported setting. This plan offloads the vast majority of the key age related activities amid key-issuing and key-refresh procedures to a Key Update Cloud Service Provider, leaving just a consistent number of basic tasks for PKG and clients to perform locally. to accomplished this objective use of a novel plot safe procedure is utilized i.e. utilizing a mixture private key for every client, in which an AND door is included to associate and bound the identity part and the time segment. According to the evaluation results, the system accomplishes consistent effectiveness for both calculation at PKG and private key size at the client. Additionally, User needs not to contact with PKG amid the key refresh, as it were, PKG is permitted to be disconnected in the wake of sending the disavowal rundown to KU-CSP. In addition, finally, no protected channel or client authentication is required amid key-refresh between client and KU-CSP.

This paper [7] endeavours to address the issue of accomplishing productive and solid key administration in secure deduplication. The system presents a gauge approach in which every client holds a free ace key for scrambling the focalized keys and redistributing them to the cloud. Nevertheless, such a gauge key administration plot produces a huge number of keys with the expanding number of clients and expects clients to dedicatedly ensure the ace keys. To this end, the author proposes Dekey, another development in which clients do not have to deal with any keys without anyone else however rather safely appropriate the focalized key offers over various servers. Security examination exhibits that Dekey is secure as far as the definitions determined in the proposed security show.

ABE gives a protected way that enables data owner to share outsourced data on untrusted storage server rather than a confided in server with a predefined gathering of clients. This preferred standpoint makes the strategy engaging in cloud storage that requires secure access control for an extensive number of clients having a place with diverse associations. By the by, one of the principle proficiency drawback of ABE is that the computational expense amid the decryption stage develops with the intricacy of the access recipe. Subsequently, before broadly sent, there is an expanding need to enhance the effectiveness of ABE. To address this issue, outsourced ABE, which gives an approach to redistribute escalated computing assignment amid decryption to CSP without uncovering data or private keys, was presented. Going for wiping out the overhead calculation at both the attribute authority and the client sides, we propose an outsourced ABE plot supporting outsourced decryption as well as empowering delegating key age. In this development [8], the author presents an insignificant arrangement controlled by a default attribute and utilize an AND door associating the inconsequential strategy and client's approach. Amid key issuing, attribute authority can re-appropriate calculation through appointing the assignment of producing a halfway private key for client's arrangement to a key age specialist co-op (KGSP) to decrease neighbourhood overhead. In addition, the outsourced decryption is acknowledged by using key blinding. All the more accurately, the client can send the blinded private key to a decryption specialist co-op (DSP) to perform fractional decryption and do the total decryption at nearby. Following our method, steady effectiveness is accomplished at the two attributes authority and client sides.

Mysterious attribute-based encryption (unknown ABE) empowers fine-grained access control over cloud storage and jelly beneficiaries' attribute privacy by concealing attribute data in ciphertexts. Nevertheless, in existing unknown ABE work, a client knows whether attributes and a concealed arrangement coordinate or not just in the wake of rehashing decryption endeavors. What's more, every decryption as a rule requires numerous pairings and the calculation overhead develops with the many-sided quality of the access recipe. Henceforth, existing plans endure an extreme proficiency downside and are not reasonable for portable cloud computing where clients might be asset compelled. In this study [9], the author proposes a novel procedure called “coordinate then-unscramble”, in which a coordinating stage is also presented before the decryption stage. This method works by computing unique segments in ciphertexts, which are utilized to play out the test that if the attribute private key matches the shrouded access strategy in ciphertexts without decryption. For quick decryption, exceptional attribute mystery key segments are created which permit accumulation of pairings amid decryption. We propose an essential mysterious ABE development and afterward get a security-improved expansion based on emphatically existentially unforgeable one-time marks. In the proposed developments, the calculation cost of an attribute coordinating test is short of what one decryption activity, which just needs a little and consistent number of pairings. Formal security investigation and execution examinations show that the proposed arrangements at the same time guarantee attribute privacy and enhance decryption proficiency for outsourced data storage in portable cloud computing.

This study [10] present a system for acknowledging complex access control of encoded data that we call Ciphertext-Policy Attribute-Based Encryption. By utilizing this strategy, scrambled data can be kept private regardless of whether the storage server is untrusted; also, this technique counters intrigue assaults. Past Attribute-based Encryption, systems utilized attributes to depict the encoded data and incorporated arrangements with client's keys; while in this system, attributes are utilized to portray a client's qualifications, and a gathering scrambling data decides an approach for who can unscramble. Pretty much this technique is adroitly nearer to customary access control strategies, for example, Role-Based Access Control (RBAC).

III. PROPOSED SYSTEM

With the quick change of adaptable cloud organizations, it ends up being dynamically defenseless to use cloud organizations to share data in a sidekick drift in the circulated registering environment. Since it is not down to earth to realize full lifecycle assurance security, get the opportunity to control transforms into a testing undertaking, especially when we share unstable data on cloud servers. Identity Based Encryption (IBE) which unravels the all-inclusive community key and assertion organization at Public Key Infrastructure (PKI) is a basic other alternative to open key encryption. Regardless, one of the major efficiency inconveniences of IBE is the overhead estimation at Private Key Generator (PKG) in the midst of customer repudiation. Beneficial denial has been all around mulled over in routine PKI setting, yet the massive organization of confirmations is certainly the weight that IBE attempts to reduce.

Public key infrastructure (PKI) is an alternate option to public key encryption whereas the Identity-Based Encryption BBE is public key and certificate management. The main disadvantage of BBE during revocation is the overhead computation at private key generator (PKG). With the rapid development of versatile cloud services, it becomes increasingly susceptible to use cloud services to share data in a friend circle in the cloud computing environment. To secure data and client Identity; Biometric Based Encryption (BBE) is an interesting option, which is proposed to streamline key administration in an authentication, based on Public Key Infrastructure (PKI) by utilizing human-coherent Identities.

Elliptical curve cryptography is a public key encryption technique which is based on the theory of elliptical curves. This encryption technique uses the properties of elliptic curve in order to generate keys instead of using the traditional methodology of generation of keys using the product of two very large prime numbers. The most important advantage of elliptical curve cryptography is the use of smaller keys providing the same level of security. ECC can provide the same security with 164-bit key that other systems provide with 1024- bit key. ECC is a public key cryptosystem which is used to generate the public key and the private key in order to encrypt and decrypt the data. It is based on the mathematical complexity of solving the elliptic curve discrete logarithm problem which deals with the problem of calculating the number of steps or hops it takes to move from one point to another point on the elliptic curve.

Elliptic curves are the binary curves and are symmetrical over x- axis. These are defined by the function:

$$y^2 = x^3 + ax + b$$

Where x and y are the standard variables that define the function while as a and b are the constant coefficients that define the curve .As the values of a and b change, elliptical curve also alters. The parameters that fully define the ECC cryptosystem are:
P: - Specification of the finite field
a, b :- Coefficients for defining curve
G: - Generator point on the curve where the operation starts
n: - Order of G
h: - Division of the total points on the curve and he order of G.

Steps Involved In ECC Algorithm:-

ECC is a public key cryptosystem where every user possesses two keys: public key and private key. Public key is used for encryption and signature verification while as private key is used for decryption and signature generation.

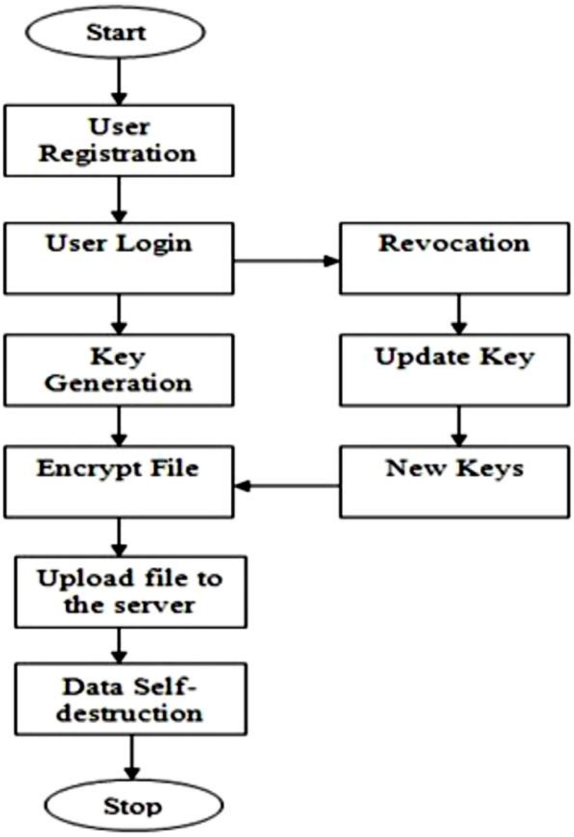

Figure 1. System Architecture

IV. CONCLUSION

Various current difficulty have appeared with the speedy enhancement of flexible cloud organizations. cloud computing is recently new technological development that has the potential to have a great impact on the world. It has many benefits that it provides to it users and businesses. We have discuss the ECC algorithm to secure privacy of the data on the cloud. A champion among the most colossal issues is the best approach to securely delete the outsourced data set away in the cloud detaches. In order to handle the issues by executing versatile fine-grained get the chance to control in the midst of the endorsement time span and time-controllable self-pulverization after near the common and outsourced data in circulated processing, this paper proposed a data self-destructing structure which can accomplish the time decided ciphertext. Moreover, a revocable outsourcing figuring into identity based encryption is familiar with beat issue of character renouncement. There is No ensured channel or customer check is required in the midst of key-revive among customer and KU-CSP, moreover with the help of KU-CSP, the structure has segments, for instance, immovable feasibility for both counts at PKG and private key size at customer.

V. REFERENCES

[1] Liehuang Zhu, Chuan Zhang, Chang Xu, Ximeng Liu, And Cheng Huang, "An Efficient and Privacy-Preserving Biometric Identification Scheme in Cloud Computing", Volume 6, IEEE Access March 2018.

[2] XialiHei, Xiaojiang Du, "Biometric-based two-level secure access control for Implantable Medical Devices during emergencies", in 2011 Proceedings IEEE INFOCOM.

[3] Mauro Barni, Tiziano Bianchi, Dario Catalano, Mario Di Raimondo, Ruggero Donida Labati, Pierluigi Failla, "Privacy-Preserving Fingercode Authentication", in Proceedings of the 12th ACM workshop on Multimedia and security, Pages 231-240 , September 2010.

[4] Yan Huang, Lior Malka, David Evans, Jonathan Katz, "Efficient Privacy-Preserving Biometric Identification", 18th Network and Distributed System Security Conference (NDSS 2011), 6-9 February 2011.

[5] Jin Li, Yinghui Zhang, Xiao Feng Chen, Yang Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing", in computers & security, Volume 72,p 1–12, Elsevier 2017

[6] Jin Li, Jingwei Li, Xiaofeng Chen, ChunfuJia, and Wenjing Lou," Identity-Based Encryption with Outsourced Revocation in Cloud Computing", IEEE Transactions on Computers, Vol. 64, NO. 2, February 2015.

[7] Jin Li, Xiaofeng Chen, Mingqiang Li, Jingwei Li, Patrick P.C. Lee, and Wenjing Lou, "Secure Deduplication with Efficient and Reliable Convergent Key Management", IEEE Transactions On Parallel And Distributed Systems, Vol. 25, NO. 6, JUNE 2014.

[8] Jin Li, Xinyi Huang, Jingwei Li, Xiaofeng Chen, and Yang Xiang, "Securely Outsourcing Attribute-Based Encryption with Checkability", IEEE Transactions On Parallel And Distributed Systems, VOL. 25, NO. 8, August 2014.

[9] Yinghui Zhang , Xiaofeng Chen, Jin Li, Duncan S. Wong, Hui Li, Ilsun You, "Ensuring Attribute Privacy Protection And Fast Decryption For Outsourced Data Security In Mobile Cloud Computing", in computers & security, Elsevier 2016.

[10] John Bethencourt, Amit Sahai, Brent Waters, "Ciphertext-Policy Attribute-Based Encryption", IEEE Symposium on Security and Privacy (SP '07), IEEE 2007.

Cite this article as :

Prof. A. V. Deorankar, Khushboo T. Khobragade, "Ensuring Better Privacy of Cloud Storage Using Elliptic Curve Cryptography", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 2, pp. 530-536, March-April 2020. Available at doi : https://doi.org/10.32628/CSEIT2062160
Journal URL : http://ijsrcseit.com/CSEIT2062160