Secured Data Outsourcing in Cloud with ECC Encryption

K.Sumathi , K.Jose Triny

Abstract: ***All sorts of external data and emerging applications as well as other existing applications are made manageable by means of implicating a well-formed methodology termed as cloud computing. Tactful statistical information or any kind resourceful information is likely to be distributed in public clouds using Attribute Based Encryption (ABE) scheme earlier. Later owing to overpriced pairing schemes accompanied with biased decryption procedures ABE has become unproductive for getting implemented to share information in an public cloud environment. In order to overcome that shortcoming for distributing information among public clouds Elliptic Curve Cryptography (ECC) Encryption scheme amalgamated with a secure auditing procedure is employed. This form of enriched security schemes proficiently suffices the original need of current cloud based networking scenario.***

Index Terms: cloud storage, key distribution center, security, Third Party Auditors (TPA).

I. INTRODUCTION

All those computing possessions contained by a network can be socialized by means of implicating cloud computing methodology in a proficient manner. Those services can be very well utilized as a service offered on demand. Thus these services offered proficiently resolves all sorts of business oriented crisis and also capably resolves those intricacies involved in storing information. Some of those publicly available computing tools found accessible in a cloud based environment are Microsoft, Google etc.These platforms possibly permit to share software, information and services as well. Devoid of acquiring a public key certificate, formerly employed ABE encrypting methodology readily permits the sender to perform encrypting operation. Hence, it becomes the root cause of some other data outsourcing problems. In order to overcome those intricacies, a proficient user access control design that relies upon an auditing control methodology amalgamated with ECC scheme is been employed in this paper. The key concept of reliability is thus highly enhanced by means of deploying TPA.

VARIED DEPLOYMENT MODELS PREVAILING IN CLOUD:

The four customized set of deployment models projected by National Institute of Standards and Technology rather than those prevailing elemental models are segregated as follows,

1. A cloud based environment that is possibly administered by an organization and is made commonly accessible to everyone gets termed as **Public Cloud.**
2. An unfailing form of privacy level is acquired by means of strengthening security measures are phrased as **Private Cloud**
3. A general infrastructure gets shared among some of those communities or organizations that do possess a similar set of vision and mission is framed as **Community Cloud.**
4. Two or more dissimilar form of cloud models are merged to create a new innovative sort of deployment model gets signified as **Hybrid Cloud**

CLOUD SECURITY:

Illegitimate activities like illegal revelation of user information as well as unlawful erasure of data should be prohibited in any of the cloud platform made available. Likewise, illicit modification of information despite of concern authority's knowledge along with prohibited information maintenance should also be prohibited. These criterions can be readily achieved on ensuring a well secured cloud platform. Hence, a well-formed framework for data security is necessitated to ensure the safe state of information residing in a cloud platform. Infrastructure that is highly demanded for any of the cloud platform is given as,

Individual accessing level for every legal user gets determined by means implicating a constrained form of mechanism verbalized as **Data Integrity.** This in turn manages the accessibility and security of the system in terms of data maintenance.

In addition to access managing strategies there exists another controlling strategy claimed as authentication. This methodology is made feasible by means of implicating **Data Confidentiality** that typically ensures security by surging cloud reliance.

A process of sharing information as well access to every individual gets managed automatically by

Revised Manuscript Received on June 11, 2019

Dr.K.Sumathi, CSE, M.Kumarasamy College Of Engineering, Karur, India.

K.Jose Triny, CSE, M.Kumarasamy College Of Engineering, Karur, India.

making sure regarding the concept of **Data Privacy**.

II. EXISTING SYSTEM

Data Owners are permitted to explore for their information that are outsourced after being encrypted using those prevailing ABE methodology within the access metrics of access control policy plotted in prior. Even though it holds for a multi-user scheme, the basic intricacy indulged in that concerned encrypting scheme is it affords a robust searching strategy only for a single keyword. Only this searching methodology holds upright for ensuring the correctness of the word being searched for. Devoid of acquiring a public key certificate, formerly employed ABE encrypting methodology readily permits the sender to perform encrypting operation. Hence, it becomes the root cause of some other data outsourcing problems. Though it is very much supportive for managing and fabricating responses of audit for Symmetric Encryption at low-level the reception of those responses becoming delayed.

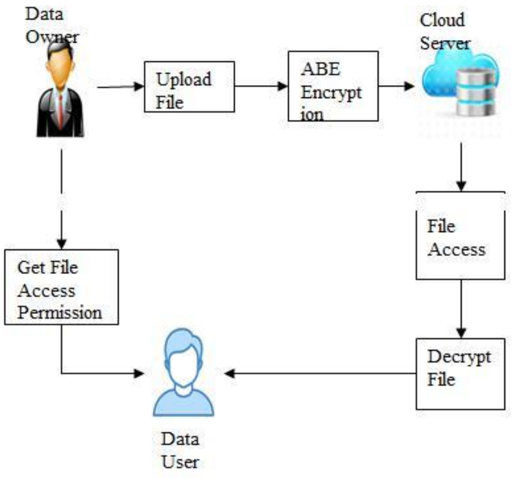

Fig.1 Existing Architecture

III. PROPOSED SYSTEM

The proposed methodology utilizes a public key encryption strategy that capably holds ECC methodology that typically utilizes the concept of elliptic curves. This strategy purposefully seeks for access permission in prior to share key with those users existing in the system. Other system is sufficient enough in providing key with 1024-bits while ECC is capable of generating key with the size of 164-bits. The auditing authority is taken over by TPA after making the most of communication channel accompanied with memory slots available. All sorts of auditing services like cross verifying of computational abilities, ability of communication channels along with public auditing is taken under the single roof of TPA. The appropriateness of information stored in cloud that is readily extracted from specifically correlated dataset is completely cross checked in Cloud Service Provider (CSP) by means of implicating TPA. This paper completely indulges in recognizing varied cryptographic procedures utilized for auditing any sort of cloud environment. The overall execution procedure of the methodology proposed gets stipulated as,

Cloud Framework

The components held by the framework are CSP, Data User and Data owner. Both services that are readily available in private as well as public cloud are offered by CSP. Amenities like software requirement as well as storage facility are also made available. The procedure of outsourcing information or files is accomplished by Data Owner which in turn also provides lawful rights to utilize every information available. The users those who are permitted to access those information or files stored are segregated as data users.

Data encryption and uploading

The Owner first encrypts the records based at the Owner's sub ACPs .The Cloud in turn encrypts the statistics based on the keys generated the use of its own Key generation set of rules. The key generation on the Cloud takes the secrets issued to Users and the sub ACPs given with the aid of the Owner into consideration to generate keys. In this encryption module, data owner upload data on cloud. After getting certificate from CA, data owner upload their files into admin system and Uploaded records are encrypted for security purpose using elliptic curve cryptography algorithm.

Encryption Algorithm of ECC

Suppose sender wants to send a message m to the receiver. Let m has any point M on the elliptic curve. Then the sender selects a random number k from [1,n-1]. Finally the cipher texts generated will be the pair of points (B1,B2) where B1= k*G B2= M + (k*G)

Decryption Algorithm of ECC

To decrypt the cipher text, the receiver computes the product of B1 and its private key. Then receiver subtracts this product from the second point B2 M = B2- (dB * B1) M is the original data sent by the sender

Authentication

User name and password is cross checked in prior for every permitted user. This holds the procedure of authentication in cloud server by those credentials being entered by the user. If the pair of credential entered by the user holds right the user concerned is authenticated or else the user concerned is left unauthenticated. Unless holding the permission for authenticity none of those user is permitted to access the file available in cloud.

Access Structure

Every authenticated user is offered with an access structure by CSP in order to define the access control for every individual user. Hence, every single registered cloud user holds a unique access structure. This procedure is taken over only after the reception of successful registration after complete authentication. Valid users alone holds their authenticity to be true for accessing files that are stored in cloud. The privilege of each and every user can be predicted by means of the access structure being plotted. This is exposed by a confined structure access labels built with logic expressions. These expressions get compressed to formulate an attribute that holds the leaf node of every access tree.

Data Auditing

All those key factors of integrity as well as confidentiality gets verified by means of ensuring the integrity of information by TPA that is found outsourced. The meta information of those information is checked over by TPA for formulating the regularizations of CSP and Data owner. This further proceeds with the procedure by analyzing those data component, random challenges found and forming the tag key for information being uploaded in cloud by data owner. This is accomplished by querying the cloud service auditor for every single user those who are searching for information.

TPA Verification

TPA verification is the process of verifying whether the TPA is valid or not to make the file verification. Before processing the request checks for authentication present with TPA. TPA should enter the shared secret key for authentication. Cloud verifies the shared secret then checks with the meta information which is received from the data owner. Auditor access the information for auditing purpose if that is authenticated, submits the access process to the data owner whenever required.

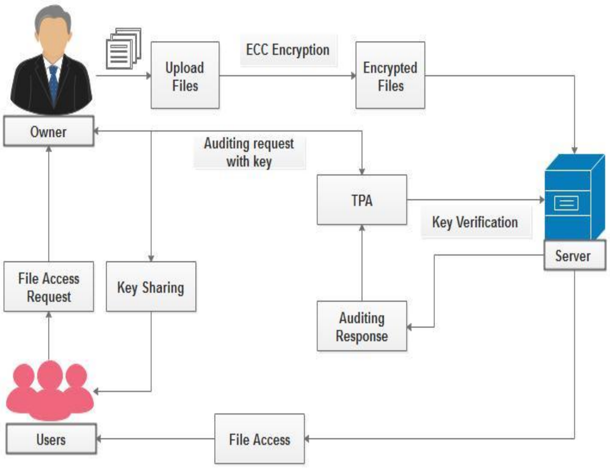

Fig.2 Proposed Architecture

IV. RESULTS AND DISCUSSION

The total amount of time acquired for execution in creating keys along with time necessitated for encrypting those messages are plotted in Figure 3. This plot typically expresses the proficiency of the proposed ECC methodology over the prevailing ABE by exhibiting a minimal time for execution. X axis holds the value of total key size taken in bits and Y axis indicates the time measured in Milliseconds (MS). Time consumed for decrypting those messages that is encrypted in prior is exposed in Figure 4.

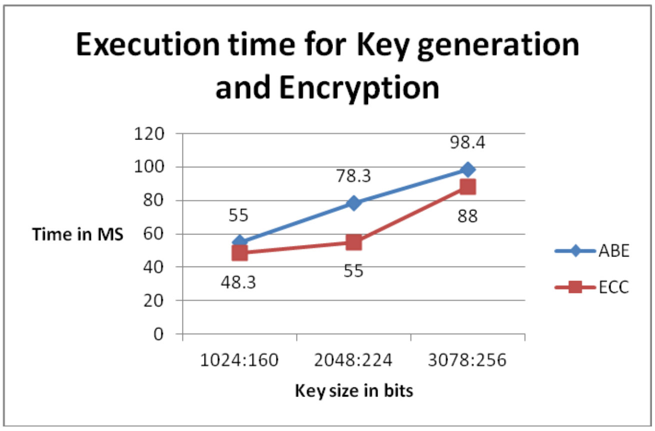

Fig3. Execution time for Key generation and Encryption

It clearly depicts the outperforming scenario of ECC over ABE by means of utilizing very little amount of time for decryption. Time graph is plotted in measure of Milliseconds for that key size taken in bits.

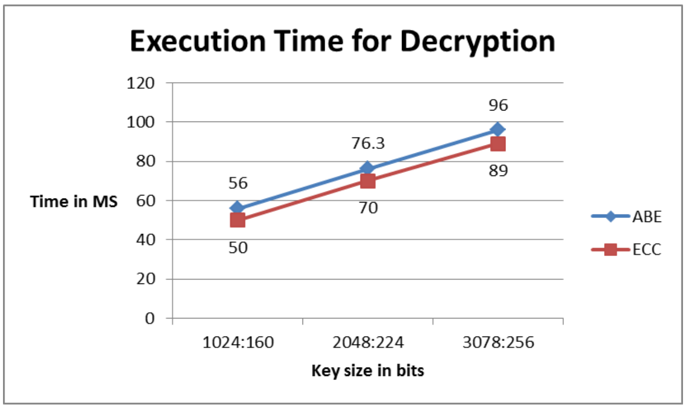

Fig4. Execution time for Decryption

V. CONCLUSION

Data security is a major issue to be dealt with from a few decades. In this paper we have reasoned the use of cryptographic techniques for securing the data. We have discussed the two efficient data security algorithms- ECC and ABE. These algorithms help in securing in transit data. Since RSA is a linear cryptographic algorithm and is slow in the encryption and decryption processes, it can put the user's security at risk. Thus ECC is the cryptographic algorithm which provides security and authentication. Authentication to the data is provided with the help of smaller keys. TPA auditing improves the security concerns in terms of confidentiality and integrity of the outsourced data. The computational cost as well as the speed of this algorithm is comparatively better. It also makes use of the good exchange protocols giving another mark to the security. The ECC key encryption time is 10.56% lower than ABE and decryption time is 7.29% lower than ABE. In future, we emphasize the use of elliptical curve cryptography for providing high data security in almost all low power devices.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

APPENDIX

S.No	Title	Author and year	Algorithm	Merit	Demerits
1	Security Concerns in Popular Cloud Storage Services	C.-K.Chu, 2013	Drop box Sharing Mechanisms	Provide secure in public data sharing	It is not widely adopted because they require complicated key management.
2	TIMER: Secure and Reliable Cloud Storage against Data Re-Outsourcing	T. Jiang,2014	Probabilistic challenge-response Scheme	Storage and computation overhead reduced.	Could not prevent a semi-trusted server from re-outsourcing clients' data
3	An Efficient Cloud-based Revocable Identity-based Proxy Re-encryption Scheme for Public Clouds	K.Liang,2014	Identity-based Proxy Re-encryption Scheme	The cost of building communication channel between the PKG and each user are both reduced	Re-encryption may be lead confusion at the time retrieving
4	A DFA-Based Functional Proxy Re-Encryption Scheme for Secure Public Cloud Data Sharing	Kaitai Liang, 2014	Deterministic Finite automata based functional PRE	Adaptively CCA secure in the standard model	Provide more number of prime order in bilinear group
5	k-times Attribute-Based Anonymous Access Control for Cloud Computing	Tsz Hon, 2015	k-times attribute-based anonymous access control	It allows k-times within a period or an event, Mean while further access will be denied	Time access control is sometimes undesirable.
6	Charm: a framework for rapidly prototyping Cryptosystems	Joseph A Akinyele,	CHARM FRAMEWORK	Provides an excellent platform for implementing techniques that automatic translation	Cannot support a high-level interpreted language
7	Outsourcing the Decryption of ABE Ciphertexts	Matthew Green, 2011	Modified Key Generation algorithm with ABE	Provide high level secure for attributes	Hardening to implement ABE in real time
8	Attribute-based encryption with verifiable outsourced decryption	Junzuo Lai,2013	ABE scheme with verifiable outsourced Decryption	Substantially reduced the computation time required for resource-limited devices to recover plaintexts	Computational overhead problems can be occurred
9	Fine-Grained Access Control System Based on Outsourced Attribute-Based Encryption	Jin Li,2013	Generic construction of attribute-based access control system	Achieves efficient key-issuing and decryption	Private information Leakage at the place of cloud service provider
10	A cipher text-policy attribute-based proxy reencryption with chosen cipher text security	Kaitai Liang, 2013	Cipher text-Policy Attribute-Based Proxy Re-Encryption (CP-ABPRE)	High level access structure model, i.e. achieving	Access structure model is complex to implement

REFERENCES

1. Jiang, Tao, Jin Li, Duncan S. Wong and Joseph Liu. "TIMER: Secure and reliable cloud storage against data re-outsourcing." In International Conference on Information Security Practice and Experience,2014,pp. 346-358.
2. Liang, Kaitai, Joseph K. Liu, Duncan S. Wong, and Willy Susilo. "An efficient cloud-based revocable identity-based proxy re-encryption scheme for public clouds data sharing." In European Symposium on Research in Computer Security,2014, pp. 257-272.
3. Yuen, Tsz Hon, Joseph K. Liu, Man Ho Au, Xinyi Huang, Willy Susilo, and Jianying Zhou. "$ k $-Times Attribute-Based Anonymous Access Control for Cloud Computing." IEEE Transactions on Computers 64, no. 9,2015,pp. 2595-2608.
4. Lai, Junzuo, Robert H. Deng, Chaowen Guan, and Jian Weng. "Attribute-based encryption with verifiable outsourced decryption." IEEE Transactions on information forensics and security 8, no. 8 2013,pp. 1343-1354.
5. Liang, Kaitai, Liming Fang, Willy Susilo, and Duncan S. Wong. "A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security." In Intelligent Networking and Collaborative Systems (INCoS), 2013, pp. 552-559.
6. Chu, Cheng-Kang, Wen-Tao Zhu, Jin Han, Joseph K. Liu, Jia Xu, and Jianying Zhou. "Security concerns in popular cloud storage services." IEEE Pervasive Computing 12, no. 4, 2013, pp. 50-57.
7. Liang, Kaitai, Man Ho Au, Joseph K. Liu, Willy Susilo, Duncan S. Wong, Guomin Yang, Tran Viet Xuan Phuong, and Qi Xie. "A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing." IEEE Transactions on Information Forensics and Security 9, no. 10,2014,pp.1667-1680.
8. Green, Matthew, Susan Hohenberger, and Brent Waters. "Outsourcing the decryption of abe ciphertexts." In USENIX Security Symposium, vol. 2011,no. 3.
9. Li, Jin, Xiaofeng Chen, Jingwei Li, Chunfu Jia, Jianfeng Ma, and Wenjing Lou. "Fine-grained access control system based on outsourced attribute-based encryption",In European Symposium on Research in Computer Security,pp.592-609.

Dr.K.Sumathi completed bachelor degree and master degree in the field of Computer Science and Engineering at Velalar College of Engineering and Technology, Thindal in the year 2005 and 2010 respectively. She received her doctoral degree from Anna University Chennai in the year 2017. She is currently working as Associate Professor of CSE department at M.Kumarasamy College of Engineering. She had published 5 different papers in reputed journals. She is life time member of ISTE. Her research area includes Networks security, Data structure and Wireless Sensor Network.

K. Jose Triny completed bachelor degree in Computer Science and Engineering at SACS M.A.V. M. M Engineering College and master degree in the field of Computer Science and Engineering at K.L.N College of Engineering and Technology, Sivagangai in the year 2012 and 2014 respectively. She is currently working as Assistant Professor of CSE department at M.Kumarasamy College of Engineering. She had published 2 different papers in reputed journals. Her research area includes Data structure and Data Mining.