International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 1 254 - 257

Securing Cloud Computing using Attribute based Signatures and Image based Key Generation

Mr. Tejas Kshirsagar, Prof. Sulabha Patil
Department of Computer Science and Engineering
Tulsiramji Gaikwad Patil college of Engineering & technology Mohgaon Nagpur

Abstract : In the realm of specialized life distributed computing has ended up basic part furthermore understanding the method for business is changing and is prone to keep changing into what's to come. Utilizing distributed storage administrations implies that you and others can get to and offer documents over a scope of gadgets and position. Records, for example, photographs and recordings can once in a while be unmanageable to email in the event that they are too enormous or you have apportion of information. You can transfer your information to a distributed storage supplier implies you can rapidly flow your information with the assistance of cloud administration and you can impart your information documents to anybody you pick. Since distributed computing shares disseminated assets by means of system in the open environment along these lines it makes less secured. Information security has turned into a noteworthy issue in information sharing on cloud. The fundamental witticism behind our framework is that it secures the information and produces the key for every exchange so every client can secure our common information by the outsider i.e. untrustworthy programmer.

Keywords: *Attribute Based Signature, Cloud Computing*

*****

I. INTRODUCTION

We focus Attribute Based Signature is an alternate primitive that customers have the capacity to sign messages with any subset of their qualities sway from a property center. In ABS, a supporter, who have an arrangement of characteristics from the force, can sign a message with a predicate that is satisfied by his traits [1] particularly, the imprint spread attributes used to satisfy the predicate and any recognizing information about the endorser (that could associate diverse imprints as being from the near guarantor). Additionally, customers can't plan to pool their attributes together. [8] The guideline hindrances with OABS is that the three substances join in OABS framework, to be specific, the quality force, customers (fuse supporters and verifiers), and S-CSP. Ordinarily, the endorsers hold their private keys from characteristic force, with which they find themselves able to sign messages a while later for any predicate satisfied by the had properties, verifiers will be induced of the way that whether an imprint is from one of the customers whose qualities satisfy the checking predicate, however remaining absolutely oblivious of the endorser's identity.

II. RELATED WORK

Jin Li1, XiaoFeng Chen2, Jingwei Li3, Chunfu Jia3, Duncan S. Wong4, WillySusilo [1]
They propose and formalize another picture called OABS, in which the computational overhead at customer side is exceptionally decreased through outsourcing such genuine estimation to an untrusted stamping cloud organization supplier (S-CSP). In addition, we apply this novel perfect model to existing ABS to decrease unconventionality and present two arrangements, i) in the first OABS arrangement, the amount of exponentiations incorporating into stamping is reduced from O(d) to O(1) (around three), where d is the upper bound of point of confinement worth portrayed in the predicate; ii) our second arrangement depends on Herranz et al's advancement with reliable size imprints.
Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou [3]
Creator propose a novel patient-driven skeleton and a suite of frameworks for data access control to PHRs set away in semi-trusted servers. To finish fine-grained and flexible data access control for PHRs, they impact property based encryption (ABE) frameworks to scramble every calm's PHR record. Special in connection to past works in secure data outsourcing, they focus on the diverse data holder circumstance, and part up the customers in the PHR structure into distinctive security spaces that colossally decreases the key organization multifaceted nature for supervisors and customers. An abnormal state of patient security is guaranteed in the meantime by manhandling multi-power ABE.Junbeom Hur [2] creator propose a novel CP-ABE plan for an information exploiting so as to share framework the normal for the framework building design. The proposed plan includes the accompanying accomplishments: 1) the key escrow issue could be tackled by sans escrow key issuing convention, which is developed utilizing the safe two-party calculation between the key era focus and the information putting away focus, and 2) fine-grained client renouncement per every characteristic should

be possible as a substitute encryption which exploits the particular property gathering key circulation on top of the ABE.

Sun Changxia Ma Wenping [5] we propose another trademark based point of confinement imprint arrangement without a trusted central force. Exactly when the quantity of customer's properties accomplishes the farthest point he can sign genuinely. Also, the central force can be addressed. We show that the arrangement is existentially unforgeable under particular properties and adaptable picked message ambush and is insurance against intrigue strike.

Zhiwei Wang∗, Ruiruixie and Shaohuiwangappl. Math. [4] They propose another thought called Attribute-Based Server-Aided Verification Signature. It is same as to common ABS arrangement, on the other hand it further enables the verifier to confirm the mark with the assistance of an outside server. In this paper, we find that there is a blemish in Wu et al's. security model against course of action strike, and diagram a bond server-helped affirmation tradition for Li et al's. attribute based imprint. We in like manner show that our tradition is insurance with self-assertive prophets.

Javier Herranz, Fabien Laguillaumie, Benoıt Libert, and Carla Rafols [6] propose the starting two trademark based imprint arranges with invariant size imprints. Their security is shown in the specific predicate and flexible message setting, in the standard model, under picked message strikes, in regards to some algorithmic suppositions related to bilinear social events. The depicted arrangements are for the case of utmost predicates, in any case they can be extended to fuse some other (more expressive) sorts of monotone predicates.

Hemanta K. Maji Manoj Prabhakaran Mike Rosulek [8] they give a general structure for creating ABS arranges, and after that exhibit a couple sensible instantiations centered around social events with bilinear mixing execution, under standard suspicions. Further, we give an improvement which is secure even against a dangerous property power; however the security for this arrangement is shown in the flat assembling model.

III. PROPOSED METHODOLOGY

A. Existing system

The proposed OABS arrangement with outsourced check decreases the preparing inconvenience at endorser side through passing on count to cloud however simply lifting two exponentiations commonly. Since the outsourcing check framework is the same as, the security can be moreover guaranteed centered on the suspicion that the third merchant does not scheme with the cloud.

Disadvantages:-

1) Our strategy gives a practical approach to understand the "piecewise key era.

2) To take into consideration high proficiency and adaptability.

B. Proposed System

In our information shared security arrangement of cloud server have four modules appeared in Fig.1. This modules give the security utilizing same kind of data and distinctive sort of yield procedure and property based encryption. The cloud server utilizes the SaaS administration to give the diverse keys to every exchange. This will help client to secure the document with respect to every exchange the cloud produces a different key for same characteristic which thusly builds the framework's security.

User Authentication

Basically whenever a user wants to use the system he/she is required to register onto the system if not registered. After registration the email is verified by sending the temporary password on mail itself. Ones the user has id and password he can login into the system and use system services.

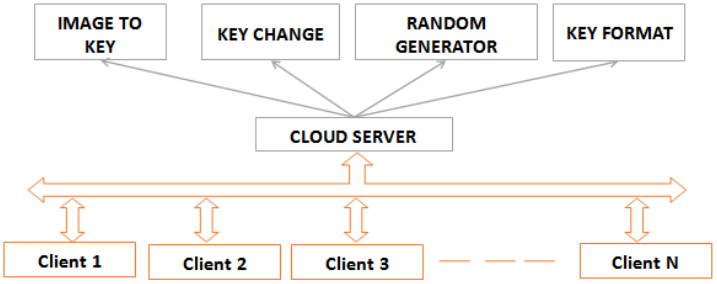

Fig.1: Proposed system architecture

The System have following four modules are as follows:

Image to Key

At whatever point a client needs to impart information to another client the first client need to transfer a key utilizing which the server will create a key. Essentially it will work for picture to key generator.

Key Change

Each time a client needs to impart information to another client the key will be changed in light of the fact that regardless of the fact that the client utilizes the same picture the server won't produce the same key.

Arbitrary Generator

Presently the inquiry emerges how the server creates various distinctive keys for the same picture. The

server utilizes an arbitrary key generator to get to the picture and add irregularity to the key era process.

Key Format

The key on server side will be produced utilizing KeyGenerator class which will take picture as a contention and will give back the key of AES calculation in object of Secret key.

SYSTEM MODEL AND DATA FLOW DIAGRAM OF SYSTEM.

Hash algorithm A hash algorithm is a function that converts a data string into a numeric string output of fixed length. The output string is generally much smaller than the original data. Hash algorithms are designed to be collision-resistant, meaning that there is a very low probability that the same string would be created for different data. Two of the most common hash algorithms are the MD5 (Message-Digest algorithm 5) and the SHA-1 (Secure Hash Algorithm). MD5 Message Digest checksums are commonly used to validate data integrity when digital files are transferred or stored.

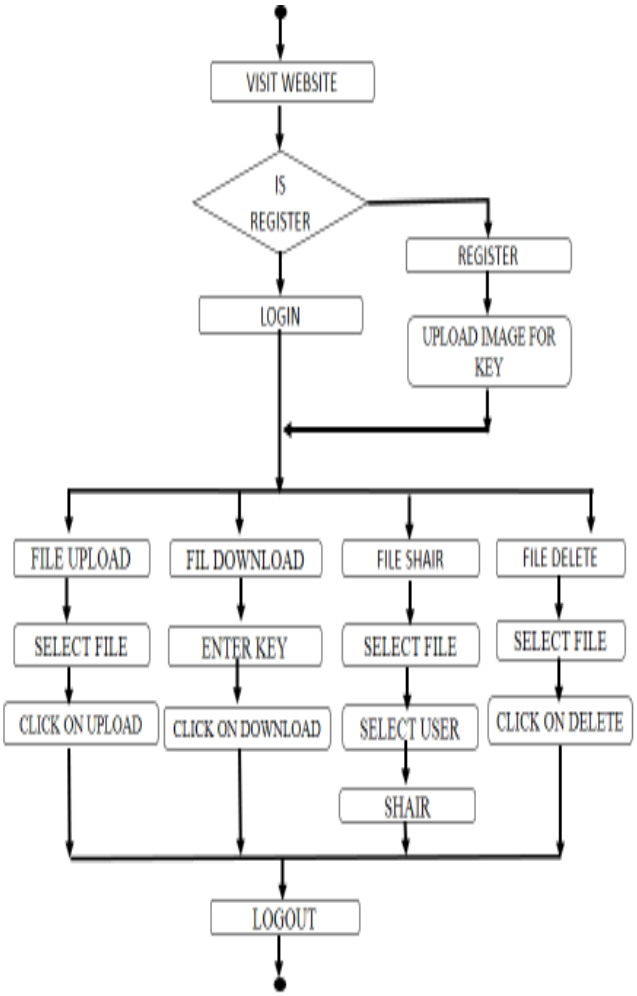

Fig. 5.2: System Model

Uploading Image as an Attribute Process

When a user uploads a file to a storage system and generate random key generation in this System, he has to upload the image as an attribute, for uploading the file procedure. After uploading image key will be generated by using hash Algorithms with addition of systems nano time. The key generation procedure uses a common Hash algorithm with system nano time to avoid same key generation.

Random Key Generation Using Attribute Based Signature

Random key generation is a mechanism that provide the security to the data and generates the key for each transaction so every user can secure our shared data by the third party i.e. unethical hacker by using hash algorithm with adding system nano time we generate the random key to provide security using same input multiple output methodology and attribute based encryption. System provide file sharing in many to many fashion and also provide data security using ABE and AES Encryption.

UPLOADING FILE PROCESS

User can upload the data for the purpose of storing and sharing any type of data to many to many or one to many fashion. Under the security of random key generation technique.

DELETE FILE

If user don't want to share the file which he upload then user can also delete this file by using delete option in system.

SHARING FILE PROCESS

After completing the process of uploading the data user can shared the any type of file to many to many or one to one fashion.

DOWNLOADING FILE PROCESS

Any user who has relevant permission can download data stored in the cloud. For downloading the user have to enter the key he got at the time of registration.

IV. CONCLUSION

The Proposed system provides security in cloud environment with the help of Attribute Based Signature (ABS) in the system the user signature (image uploaded by user) it outsourced to the cloud and key is generated by the same. The system proposed consist of the key generation logic for cloud server which helps random key generation security for ABS. The proposed system provides data security using random key generation in each transaction. The form of data that will be encrypted for sharing will be text and image.

REFERENCES

[1] Secure Outsourced Attribute Based Signature IEEE Transactions on Parallel and Distributed Systems, (Volume: PP, Issue: 99) 2014

[2] Improving Security and Efficiency in Attribute-Based Data Sharing JunbeomHur IEEE Transactions on Knowledge and Data Engineering Vol: 25 No: 10 2013

[3] Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou, IEEE Transactions On Parallel And Distributed Systems Vol. Xx, No. Xx, Xx 2012

[4] Attribute-based Server-Aided Verification Signature Zhiwei Wang∗, RuiruiXie and ShaohuiWangAppl. Math. Inf. Sci. 8, No. 6, 3183-3190 (2014)

[5] Secure Attribute-based Threshold Signature without a Trusted Central Authority Sun Changxia Ma Wenping Journal of Computers, Vol. 7, No. 12, December 2012

[6] Short Attribute-Based Signatures for Threshold Predicates Javier Herranz, Fabien Laguillaumie, Benoıt Libert, and Carla Rafols "RSA Conference 2012, San Francisco : United States (2012)"

[7] Improving Revocation Scheme to Enhance the Performance in Multi-Authority ABE Shraddha U. Rasal Bharat TidkeInternational Journal of Computer Applications (0975 – 8887) Volume 90 – No 18, March 2014

[8] Attribute-Based Signatures Hemanta K. MajiManojPrabhakaran Mike Rosulek November 22, 2010

[9] Provable Secure Multi-Authority Attribute Based Signatures Yanli Chen, JunjunChen,GengYang Journal of Convergence Information Technology(JCIT) Volume 8, Number 2,Jan 2013

[10] R. L. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. In C. Boyd, editor, ASIACRYPT,volume 2248 of Lecture Notes in Computer Science, pages 552–565. Springer, 2001

[11] D. Chaum and E. van Heyst. Group signatures. In EUROCRYPT, pages 257–265, 1991

[12] X. Boyen. Mesh signatures. In M. Naor, editor, EUROCRYPT, volume 4515 of Lecture Notes in Computer Science, pages 210–227. Springer, 2007.

[13] Dynamic Credentials and Ciphertext Delegation for Attribute-Based Encryption Amit SahaiUCLA HakanSeyalioglu†, UCLA Brent Waters‡, University of Texas at AustinAugust 1, 2012