Enhancing Security by Implementing Image based Encryption in Cloud Environment

[1] Tejas Kshirsagar, [2] Prof. Sulabha Patil

Tulsiramji Gaikwad Patil College of Engineering 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 liable to keep changing into what's to come. Utilizing distributed storage administrations implies that you and others can get to and share documents over a scope of gadgets and position. Records, for example, photographs and recordings can some of the time be unmanageable to email in the event that they are too huge or you have apportion of information. You can transfer your information to a distributed storage supplier implies you can expediently flow your information with the assistance of cloud administration and you can impart your information records to anybody you pick. Since distributed computing offers circulated assets by means of system in the open environment in this manner it makes less secured. Information security has turned into a noteworthy issue in information sharing on cloud. The primary aphorism behind our framework is that it secures the information and creates the key for every exchange so every client can secure our common information by the outsider i.e. dishonest programmer.

Individual information put away in the Cloud may contain account numbers, passwords, notes, and other imperative data that could be utilized and abused by a scalawag, a contender, or an official courtroom. These information are stored, replicated, and documented by Cloud Service Providers, regularly without client's approval and control. The framework proposed comprise of the key era rationale for cloud server which helps irregular key era security for ABS. What's more, our framework secures the information and produces the key for every exchange by utilizing property based mark.

Keywords*: Cloud Computing, ABS , AES.*

*****

I. Introduction

Distributed computing is mostly used to tackle the capacity and support issue. Distributed storage offers online capacity and gets to it from anyplace and whenever. Few of the administrations in cloud render by administration suppliers. In private cloud they have their own particular stockpiling zone. Record lost issue is explained by the document reinforcement process in distributed framework. In the conveyed framework chronicled, stored, duplicates of the record is accessible at numerous associates. Any of the companions can go about as a server to the administration suppliers. So the duplicates are accessible perpetually after downloaded the required secret document. The duplicates lives in the companion are in clear frame. Here, constrained the extreme sum or replication is required. Clients are unconscious of those duplicates accessible at the reserve memory of the administration suppliers. They can't have control over the information. Such duplicates of the document are kept up by the administration supplier against unplanned, legitimate and malignant assaults. In P2P framework mystery key is put away with dispersed hash table (DHT). In appropriated hash table it must be guarantee that key really stores the information connected with the key in every hub. Steering assaults, stockpiling and recovery assaults damages information security in DHT. Sybil assaults make the fake substances and additions notoriety from the legit elements. For sharing the documents and ensuring security the idea called vanish is presented.

Objectives of characteristic based mark (ABS), clients sign messages with any predicate of their traits issued from a quality power. Under this thought, a mark bears witness to not to the character of the person who marked a message, yet a case in regards to the properties the basic underwriter has. In ABS, clients can't manufacture marks with characteristics they don't have even through intriguing. Then again, a true blue underwriter stays mysterious without the apprehension of renouncement and is unclear among every one of the clients whose properties fulfilling the predicate indicated in the mark. ABS is valuable in numerous critical applications, for example, unknown verification and characteristic based informing frameworks. In this paper, we propose two proficient ABS developments supporting adaptable limit predicate by investigating another method for mark marking. Contrasted and existed plans, the new developments give better effectiveness as far as both the computational expense and mark size. The principal new development is provably secure in the irregular prophet model, while the second development does not depend on

the arbitrary prophet supposition. To advance decrease the trust on trait power, we additionally demonstrate an ABS development with different quality powers. It is significant that the security of all the proposed developments is not depending on non specific gathering. As an illustrative application, we develop an effective non-transferable access control framework from ABS.

Quality Based Signature is an alternate primitive that customers can sign messages with any subset of their attributes sway from a property center. In ABS, a guarantor, 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 cover the credits used to satisfy the predicate and any recognizing information about the endorser (that could interface diverse imprints as being from the relative financier). In addition, customers can't plan to pool their qualities together. [2] The guideline impediments with OABS is that the three substances consolidate in OABS framework, in particular, the quality force, customers (join guarantors and verifiers), and S-CSP. Typically, the endorsers hold their private keys from characteristic force, with which they can 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 unaware of the identity of the endorser.

II. Related Work

Jin Li1, XiaoFeng Chen2, Jingwei Li3, Chunfu Jia3, Duncan S. Wong4, WillySusilo [1]Author propose and formalize another photo called OABS, in which the computational overhead at customer side is uncommonly decreased through outsourcing such genuine count to an untrusted stamping cloud organization supplier (S-CSP). Moreover, we apply this novel perfect model to existing ABS to decrease eccentrics and present two arrangements, i) in the principal 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 breaking point worth portrayed in the predicate; ii) our second arrangement depends on Herranz et al's advancement with steady size imprints.

Zhiwei Wang, Ruiruixie and Shaohuiwangappl. Math. [2] Author propose another idea called Attribute-Based Server-Aided Verification Signature. It is same as to common ABS arrangement, in any case it further engages the verifier to attest the mark with the assistance of an outside server. In this paper, we find that there is a defect in Wu et al's. security model against course of action attack, and framework a concrete 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.

R. Brindha, R. Rajagopal [3] creator proposed quality based encryption (ABE) is an open key based one-to-various encryption that licenses customers to scramble and unscramble data centered around customer attributes. An ensuring use of ABE is versatile access control of encoded data set away in the cloud, using access polices and credited qualities associated with private keys and Cipher works. One of the key adequacy drawbacks of the current ABE arrangements is that unscrambling incorporates expensive mixing operations and the amount of such operations creates with the many-sided nature of the privilege to get access approach. In ABE system, a customer gives an untrusted server, say a cloud organization supplier, with a change key that allows the cloud to decipher any ABE ciphertext satisfied by that customer's attributes or get to technique into a fundamental figure substance, and it just gains somewhat computational overhead for the customer to recover the plaintext from the changed ciphertext. Then again, it doesn't guarantee the precision of the change done by the cloud. In the present structure, another need of ABE with outsourced unscrambling: certainty. Coolly, sureness guarantees that a customer can capably check if the change is done adequately. In the proposed Categorical Heuristics on Attribute-based Encryption (CHAE) is a conformity of Attribute Based Encryption (ABE) for the reasons of giving affirmations towards the provenance of the checked data, furthermore towards the anonymity of the financier. Finally, exhibit a use of our arrangement and result of execution estimations, which demonstrates an enormous diminishment on enrolling resources constrained on customers.

Shraddha U. Rasal, Bharat Tidke [4] creator proposed Conventional structure in cryptography allows essentially bestowing of keys between the sender and recipient, for such a strategy simply the imprint stockpiling is obliged the customer's open key. In any case as the amount of customers constructs, it's transformed into a testing occupation to have such an affirmation stockpiling furthermore key movement, to thrashing this Identity Based Encryption (IBE) was proposed, once more it had made the dull environment as it was supporting just to composed correspondence. After IBE Attribute Based encryption (ABE) made likelihood to give multicast correspondence between customers anyway it was obliged to simply key methodology based encryption and also couldn't give the denial sensation to keys. So this paper intends to make a present structure using MAMM (Multiple Authority Multiple Mediator) with the usage of dispersed CP-ABE (Cipher Policy ABE) which overhauls the repudiation and upgrades the execution.

III. Proposed System

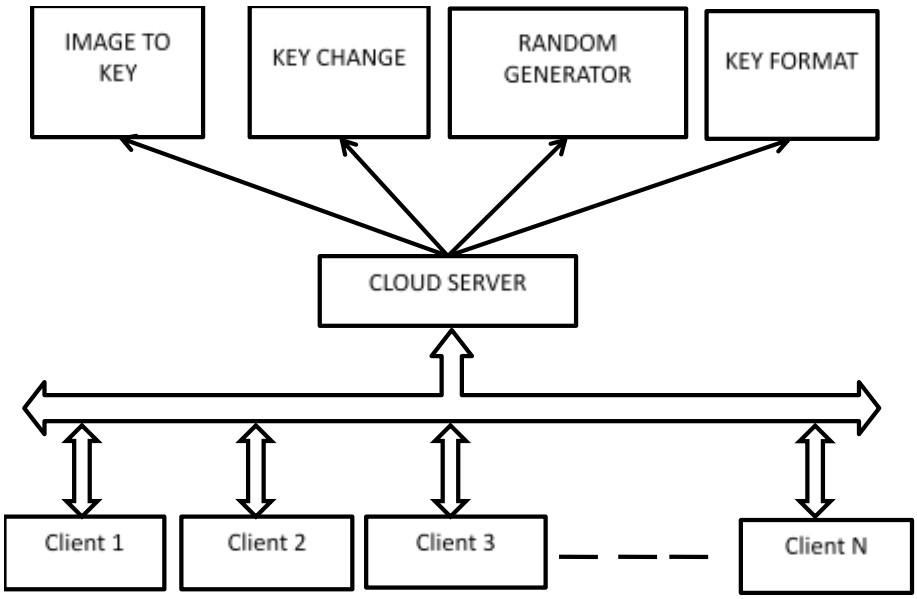

Fig: Proposed Architecture

The System have following four modules are as follows:

IMAGE TO KEY:-

Whenever a user wants to share data with another user the first user need to upload a key using which the server will generate a key. Basically it will work for image to key generator.

KEY CHANGE:-

Every time a user wants to share data with another user the key will be changed because even if the user uses the same image the server won't generate the same key.

RANDOM GENERATOR:-

Now the question arises how the server generates multiple different keys for the same image. The server uses a random key generator to access the image and add randomness to the key generation process.

KEY FORMAT:-

The key on server side will be generated using Key Generator class which will take image as an argument and will return the key of AES algorithm in object of Secret key.

USER AUTHENTICATION

A new user has to first create a profile. This is done by registration. A user id and password are submitted by the user. The user can login successfully only if user id and password are entered correctly. The login is a failure if the incorrect user id or wrong password is entered by the user. This helps in preventing unauthorized access.

Fig.6.1: User Login Form

UPLOADING IMAGE AS AN ATTRIBUTE

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.

Fig.6.2: uploading Image.

RANDOM KEY GENERATION

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.

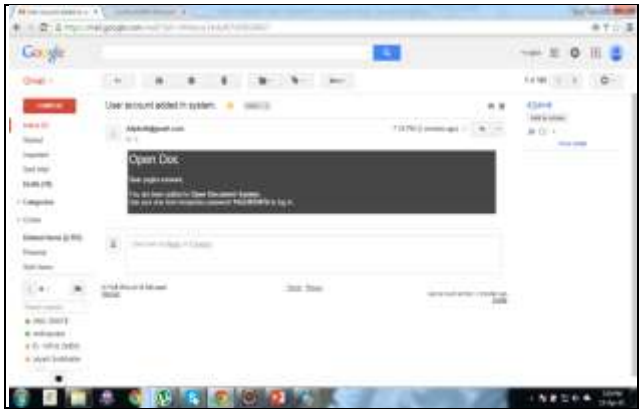

Fig. 6.3: KEY GENERATION

UPLOADING DATA

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.

FIG.6.4: DATA UPLOADING

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.

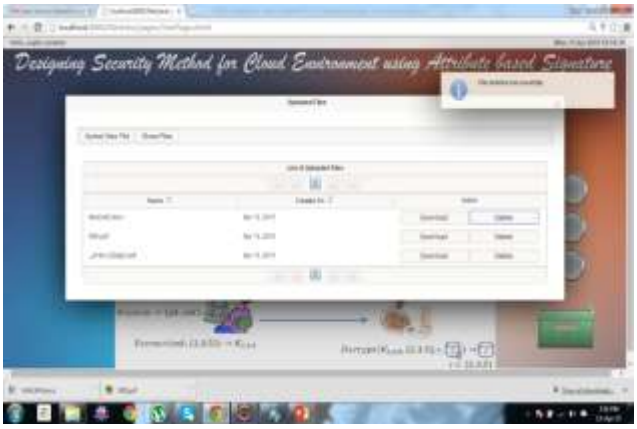

FIG.6.5: DELETE FILE

SHARING DATA

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.

FIG.6.6: SHARING DATA

DOWNLOADING FILE

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.

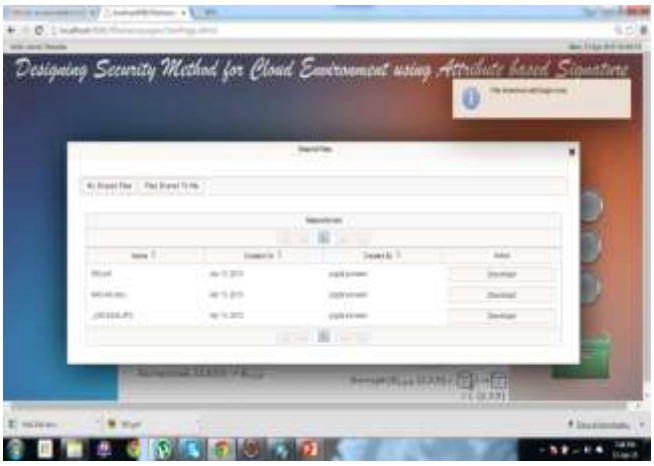

Fig.6.7: DOWNLOADING FILE

IV. Conclusion

The proposed system provides security using ABE and AES encryption algorithm. This project servers an alternative to digital signature. The security provided is improvise using a image to key based random key generator which provides different key form same image using a random function. The proposed system can be used in any application which includes data sharing between users (either one to one or many to many) approach.

V. Future Scope

In future we can extend following functionalities in this project:

- Use of multiple encryption algorithms for better security.
- Extending project to multi-cloud.
- Real time data sharing like audio and video conferencing.
- Strong Compression algorithm for less cloud data storage.

Making it more user friendly.

References

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

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

[3] Categorical Heuristic for Attribute Based Encryption in the Cloud Server R. Brindha, R. Rajagopal International Journal of Computer Trends and Technology (IJCTT) – volume 9 number 2– Mar 2014.

[4] 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

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

[6] Hierarchical Attribute-Based Secure Outsourcing for Malleable Access in Cloud Computing S. Usha, Dr. A. Tamilarasi, K. Mahalakshmi International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 6- June 2013.

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

[8] Label-Embedding for Attribute-Based Classification ZeynepAkataa,b, FlorentPerronnina, Zaid Harchaouib and CordeliaSchmidb Ieee Conference On Computer Vision And Pattern Recognition Year 2013.

[9] 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

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

[11] Dynamic Credentials and Cipher text Delegation for Attribute-Based Encryption Amit Sahai UCLAHakanSeyalioglu†, UCLA Brent Watersffi, University of Texas at AustinAugust 1, 2012

[12] Decentralized Attribute-Based Signatures Tatsuaki Okamoto and Katsuyuki Takashima July 27, 2012

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

[14] An Expressive Attribute-based Signature Scheme without Random Oracles Dan. Tianzuo Wang Xiaofeng Wang, Jinshu Su the 2nd International Conference on Computer Application and System Modeling (2012)

[15] Efficient And Expressive Fully Secure Attribute-Based Signature In The Standard Model Piyi Yang, Tanveer A Zia, Zhenfu Cao and Xiaolei Dong 2011.

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

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

[18] 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

[19] Revocable Attribute-Based Signatures with Adaptive Security in the Standard Model Alex Escala, Javier Herranz, and Paz MorilloDecember 2001

[20] Attribute Based Group Signatures Dalia Khader University of BathVolume 4 Issue 4 December 2000

[21] A New Approach to Threshold Attribute Based Signatures S Sharmila Deva Selvi, SubhashiniVenugopalan, C. PanduRanganVol. 7, No. 12, 2000

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