Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 9; April-June, 2015 pp. 16-20
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/acsit.html

Result Paper on–"Designing Security Method for Cloud Environment using Attribute Based Signature

Yogita R. Sunwani[1] and Amit Welekar[2]

[1]Department of Wireless Communication and Computing TGPCET, RTM Nagpur University, Nagpur, Maharashtra India
[2]Department of Information Technology TGPCET, RTM Nagpur University, Nagpur, Maharashtra, India
E-mail: [1]yogita.sunwani@gmail.com, [2]welekar.amit@gmail.com

Abstract—*In the world of technical life cloud computing has become integral part and also understanding the way of business is changing and is likely to continue changing into the future. Using cloud storage services means that you and others can access and share files across a range of devices and position. Files such as photos and videos can sometimes be unmanageable to email if they are too big or you have allot of data. You can upload your data to a cloud storage provider means you can speedily circulate your data with the help of cloud service and you can share your data files with anyone you choose. Since cloud computing shares distributed resources via network in the open environment thus it makes less secured. Data security has become a major issue in data sharing on cloud. The main motto behind our system is that it secures 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.*

Keywords*: Attribute Based Signature, Cloud Computing*

1. INTRODUCTION

1.1 Overview

We determine Attribute Based Signature is a different primitive that clients are able to sign messages with any subset of their characteristics impact from a property focus. In ABS, an underwriter, who have a set of qualities from the power, can sign a message with a predicate that is fulfilled by his attributes [1] specifically, the mark cover the ascribes used to fulfill the predicate and any distinguishing data about the endorser (that could connect different marks as being from the comparative underwriter). Moreover, clients can't conspire to pool their characteristics together. [2] The principle disadvantages with OABS is that the three substances incorporate in OABS system, namely, the quality power, clients (incorporate underwriters and verifiers), and S-CSP. Normally, the endorsers hold their private keys from trait power, with which they are able to sign messages a while later for any predicate fulfilled by the had attributes, verifiers will be persuaded of the way that whether a mark is from one of the clients whose qualities fulfill the marking predicate, however remaining totally insensible of the personality of the endorser.

Propelled by the late improvements in secure outsourced trait based signature, in this paper, we introduce new information imparting securing on cloud utilizing quality based mark. Whatever is left of this paper is sorted out as takes after.

1.2 Problem Definition

To develop a system that provides security in cloud based environment using attribute based encryption and random key generation using image to key and provide file hosting services to users.

1.3 Objectives

- To design a website that will provide proper authentication services.
- To provide file upload and download facility to user.
- To provide file sharing in many to many fashion
- To provide data security using ABE and AES Encryption.
- To provide random key generation for key management.

2. LITERATURE SURVEY AND REVIEW

Jin Li1, XiaoFeng Chen2, Jingwei Li3, Chunfu Jia3, Duncan S. Wong4, WillySusilo [1]Author propose and formalize another picture called OABS, in which the computational overhead at client side is extraordinarily diminished through outsourcing such serious calculation to an untrusted marking cloud administration supplier (S-CSP). Besides, we apply this novel ideal model to existing ABS to lessen unpredictability and present two plans, i) in the first OABS plan, the quantity of exponentiations including in marking is diminished from O(d) to O(1) (about three), where d is the upper bound of limit worth characterized in the predicate; ii) our second plan is based on Herranz et al's development with consistent size marks.

Zhiwei Wang, Ruiruixie and Shaohuiwangappl. Math. [2] Author propose another thought called Attribute-Based Server-Aided Verification Signature. It is same as to typical ABS plan, however it further empowers the verifier to affirm the signature with the help of an outside server. In this paper, we find that there is a flaw in Wu et al's. security model against arrangement assault, and outline a cement server-helped confirmation convention for Li et al's. trait based mark. We likewise demonstrate that our convention is guarantee with arbitrary prophets.

R. Brindha, R. Rajagopal [3] author proposed attribute based encryption (ABE) is an open key based one-to-numerous encryption that permits clients to scramble and unscramble information focused around client traits. A guaranteeing application of ABE is adaptable access control of encoded information put away in the cloud, utilizing access polices and attributed traits connected with private keys and Cipher writings. One of the fundamental effectiveness downsides of the current ABE plans is that unscrambling includes costly blending operations and the quantity of such operations develops with the intricacy of the right to gain entrance approach. In ABE framework, a client gives an untrusted server, say a cloud administration supplier, with a change key that permits the cloud to interpret any ABE ciphertext fulfilled by that client's characteristics or access strategy into a basic Fig. content, and it just acquires a little computational overhead for the client to recoup the plaintext from the changed ciphertext. On the other hand, it doesn't promise the accuracy of the change done by the cloud. In the current framework, another necessity of ABE with outsourced unscrambling: irrefutability. Casually, certainty ensures that a client can proficiently check if the change is carried out effectively. In the proposed Categorical Heuristics on Attribute-based Encryption (CHAE) is an adjustment of Attribute Based Encryption (ABE) for the reasons of giving assurances towards the provenance of the marked information, and also towards the namelessness of the underwriter. At long last, demonstrate a usage of our plan and consequence of execution estimations, which shows a huge diminishment on registering assets forced on clients.

Shraddha U. Rasal, Bharat Tidke [4] author proposed Conventional framework in cryptography permits simply imparting of keys between the sender and beneficiary, for such a method just the mark stockpiling is accommodated the client's open key. Anyhow as the quantity of clients builds, it's turned into a testing occupation to have such a declaration stockpiling and also key conveyance, to defeat this Identity Based Encryption (IBE) was proposed, yet again it had made the tedious environment as it was supporting just to coordinated correspondence. After IBE Attribute Based encryption (ABE) made probability to give multicast correspondence between clients however it was constrained to just key approach based encryption and additionally couldn't give the repudiation sensation to keys. So this paper means to create a current framework utilizing MAMM (Multiple Authority Multiple Mediator) with the utilization of disseminated CP-ABE (Cipher Policy ABE) which upgrades the disavowal and enhances the execution.

Sun Changxia Ma Wenping [5] Author propose another characteristic based limit mark plan without a trusted focal power. At the point when the number of client's properties achieves the limit he can sign truly. Moreover, the focal power can be questioned. We demonstrate that the plan is existentially unforgeable under specific properties and versatile picked message assault and is guarantee against connivance assault.

S. Usha, Dr. A. Tamilarasi, K. Mahalakshmi [6] author proposed endeavor to give an upgraded information stockpiling security show in Cloud Computing and making a trust environment in distributed computing. There are a ton of convincing explanations behind organizations to send cloud-based capacity. For another business, start-up expenses are essentially decreased on the grounds that there is no compelling reason to contribute capital in advance for an inward IT framework to backing the business. By a wide margin, the most obvious inquiry customers considering a move to distributed storage ask is whether their information will be secure. Putting away information offsite doesn't change information security necessities; they are the same as those confronting information put away on location. Security ought to be focused around business necessities for particular applications and information sets, regardless of where the information is put away. We accept that information stockpiling security in Cloud Computing, a zone brimming with difficulties and of central significance, is still in its outset now, and numerous exploration issues are yet to be recognized. In this paper, we researched the issue of information security in cloud information stockpiling, to guarantee the rightness of customers' information in cloud information stockpiling. We proposed a Hierarchical Attribute-Based Secure Outsourcing for mallable Access in Cloud registering which likewise guarantees information stockpiling security and survivability consequently giving trust environment to the customers. To battle against unapproved data spillage, delicate information must be scrambled before outsourcing to give end-to-end information secrecy affirmation in the cloud and past. We have lessened the calculation time because of key size by executing ECDSA calculation for Cryptographical operations. Additionally we utilize push mail calculation for key trade in the middle of holder and customer. It upgrades the security in the proposed model adequately.

3. METHODOLOGY

3.1 Block Diagram

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.

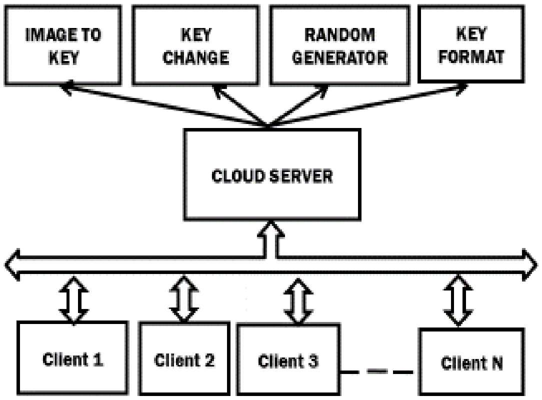

Fig. 1: Proposed system architecture

The System have following four modules are as follows:

Image to Key

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.

3.2 Flow Chart

The flowchart given in the following Figure.2 describes the working principle of how random key generate from attribute based signature.

- User wants to use the system he/she is required to register onto the system.
- Upload Image For key.
- User can Upload,Delete,Shair,Download file by clicking on button vice versa.

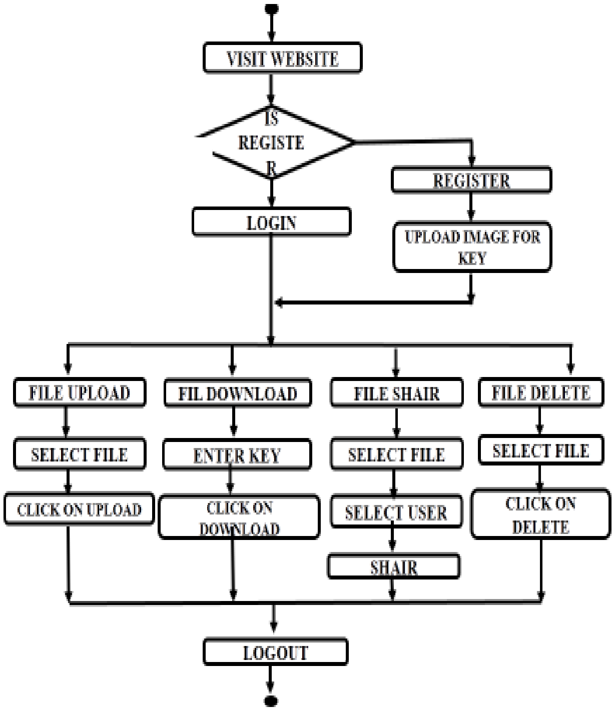

Fig. 2: Flow Chart of Random key generator from ABS

4. DESIGN/ IMPLEMENTATION

4.1 AES Algorithm

- **AES (Advanced Encryption Standard)**

AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

AES operates on a 4×4 column-major order matrix of bytes, termed the state, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field.

The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. The numbers of cycles of repetition are as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

High-level description of the algorithm

Key Expansion—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.

SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

ShiftRows—a transposition step where each row of the state is shifted cyclically a certain number of steps.

MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

AddRoundKey
Final Round (no MixColumns)

SubBytes

ShiftRows

AddRoundKey.

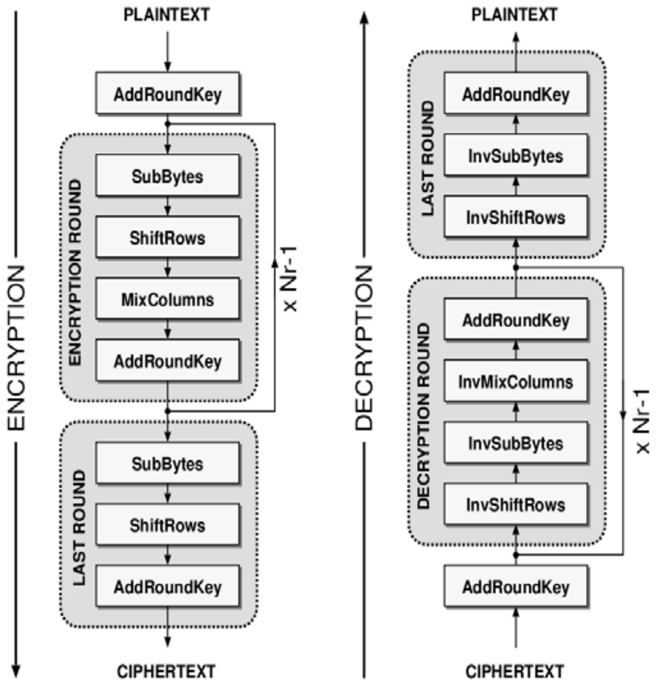

Fig. 3: Working of AES Algorithm

5. EXPERIMENTAL RESULTS

The proposed system is developed in J2EE java based technology. The proposed system provides better security in cloud environment using image based key generation with random approach. In proposed system the key generation logic generates a new key every time a user wants to share file with another user. The key is generated using image attribute and random number fusion. The key generated is used for AES encryption with key size f 256 key size. Using such strong encryption will avoid any general security breaches and random key for harder key guessing.

6. 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

7. APPLICATION AND FUTURE SCOPE

The proposed system will provide security in any cloud based environment websites that provide data sharing within users. Some of the basic examples can be Gmail, facebook and other social networking sites. In future we plan to provide better security using multiple security algorithms and multimedia based attribute signatures.

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 CordeliaSchmidbIeee 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, KuiRen, 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 UCLA HakanSeyalioglu†, UCLA Brent Waters‡, 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 Morillo December 2001

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

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

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