International Journal of Engineering Research and General Science Volume 3, Issue 2, March-April, 2015
ISSN 2091-2730

Designing Security Method for Cloud Environment Using Attribute Based Signature

[1]Yogita R. Sunwani
TGPCET, RTM Nagpur University,
Nagpur, Maharashtra, India
Yogita.sunwani@gmail.com
[2] Prof. Amit Welekar
TGPCET, RTM Nagpur University,
Nagpur, Maharashtra, India
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

INTRODUCTION

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. We audit the related work in Section II. We depict the proposed approach in Section III. Furthermore we finish up this paper in Section IV

PROPOSED SYSTEM

In this paper we are proposing a system to provide security using same input, multiple output methodology and attribute based encryption. We will use cloud SaaS to generate key and send to multiple users. It provides data sharing services between multiple clients.

LITERATURE SURVEY

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 figure 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.

ZeynepAkataa,b, FlorentPerronnina, Zaid Harchaouib and CordeliaSchmidb [8]author proposed attributes are a halfway representation, which enables parameter offering between classes, an absolute necessity when preparing information is rare. We propose to view trait based picture classification as an issue inserting issue: each one class is implanted in the space of property vectors. We present a capacity which measures the similarity be- tween a picture and a mark installing. The parameters of this capacity are adapted on a preparation set of named samples to guarantee that, given a picture, the right classes rank higher than the wrong ones. Comes about on the Animals With Attributes and Caltech-UCSD-Birds datasets demonstrate that the proposed structure beats the standard Direct At- tribute Prediction benchmark in a zero-shot learning situation. The name inserting system offers different focal points, for example, the capacity to power option wellsprings of information notwithstanding properties (e.g. class chains of command) or to move easily from zero-shot figuring out how to learning with substantial amounts of information.

Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou [9]Author propose a novel patient-driven skeleton and a suite of systems for information access control to PHRs put away in semi-trusted servers. To accomplish fine-grained and versatile information access control for PHRs, they influence property based encryption (ABE) systems to scramble each quiet's PHR document. Unique in relation to past works in secure information outsourcing, they concentrate on the different information holder

situation, and part up the clients in the PHR framework into different security spaces that enormously lessens the key administration multifaceted nature for managers and clients. A high level of patient security is ensured at the same time by abusing multi-power ABE.

Amit Sahai, UCLA HakanSeyalioglu [11]author Inspired by the inquiry of access control in distributed storage, we consider the issue utilizing Attribute-Based Encryption (ABE) in a setting where clients' certifications may change and figure writings may be put away by an outsider. Author find that an extensive answer for our issue should all the while take into consideration the denial of ABE private keys and also consider the capacity to upgrade cipher texts to reflect the latest upgrades. Our principle result is acquired via blending two commitments.

Tatsuaki Okamoto and Katsuyuki Takashima2[12] Author exhibit the first decentralized multi-power quality based mark (DMA-ABS) plan, in which no focal power and no trusted setup are needed. The proposed DMA- ABS plan for general (non-monotone) predicates is completely secure (versatile predicate unforgeable and flawless private) under a standard presumption, the decisional straight (DLIN) supposition, in the irregular prophet model.

Javier Herranz, Fabien Laguillaumie, Benoıt Libert, and Carla Rafols [13]Author propose the initial two characteristic based mark plans with invariant size marks. Their security is demonstrated in the particular predicate and versatile message setting, in the standard model, under picked message assaults, regarding some algorithmic suppositions identified with bilinear gatherings. The portrayed plans are for the instance of limit predicates, however they can be protracted to incorporate some other (more expressive) sorts of monotone predicates.

Dan. Tianzuo Wang ,Xiaofeng Wang, Jinshu Su [14]author proposed attribute based marks (ABS) is another cryptographic primitive and can assume an incredible part in attribute based access control frameworks. In ABS, an endorser can pick its qualities fulfilling an arrangement of a verifier to create a substantial signature without uncover its character or traits, while the mark guarantees that the message is embraced by an individual owning characteristics the approach needing. Nonetheless, most existing works of ABS need irregular prophets, which is strange and brings about the reliance of security on hash capacities. In this paper, we allude to the experienced systems utilized as a part of character based encryption (IBE) to propose an ABS plan without arbitrary prophets. Our plan help any expressive strategy comprising of AND, OR, limit doors, which offers extraordinary adaptability to the usage of access control.

A Zia, Zhenfu Cao and Xiaolei Dong [15] Author Outlining a completely secure (versatile predicate unforgeable and consummately private) trait based mark (ABS), which permits an endorser to pick a set of traits rather of a solitary string speaking to the underwriter's personality, under standard cryptographic suspicion in the standard model is a testing issue. Existing plans are either excessively entangled or just demonstrated in the non-exclusive gathering model. In this paper, we display an effective completely secure ABS conspire in the standard model focused around q-parallel BDHE suspicion which is more pragmatic than the bland gathering model utilized as a part of the past plan. To the best of our insight, our plan is the most proficient one among all the past ABS conspires in the standard model. Additionally, our proposed plan is exceedingly expressive since it permits any endorser to tag case predicates regarding any predicate comprises of AND, OR, and Threshold entryways over the traits in the framework. ABS has discovered numerous essential applications in secure correspondences, for example, unknown validation framework and property based informing framework.

Hemanta K. Maji Manoj Prabhakaran Mike Rosulek [16] Author give a general structure for developing ABS plans, and after that demonstrate a few down to earth instantiations focused around gatherings with bilinear blending execution, under standard suspicions. Further, we give a development which is secure even against a malignant property power; however the security for this plan is demonstrated in the bland gathering model. We depict a few pragmatic issues that persuaded this work, and how ABS can be utilized to settle them. Additionally, we demonstrate how our systems permit us to extend Groth-Sahai NIZK evidences to be recreation extractable and character based with down overheard.

Alex Escala, Javier Herranz, and Paz Morillo[19]Author proposed an attribute based signature regarding a marking arrangement, picked impromptu by the underwriter, persuades the verifier that the endorser holds a subset of characteristics fulfilling that marking approach. In a perfect world, the verifier must acquire no other data about the personality of the endorser or the properties he holds. This primitive has numerous applications in true situations obliging both confirmation and namelessness/security fitting ties. We propose in this paper the first property based mark plan fulfilling in the meantime the accompanying properties: (1) it concedes general marking strategies, (2) it is demonstrated secure against completely versatile foes, in the standard model, and (3) the quantity of components in a mark depends just on the measure of the marking arrangement. Besides, our plan en- delights the extra property of revocability: an outside judge can break the secrecy of a mark, when important. This property may be exceptionally fascinating in genuine applications where powers are unwilling to permit full secrecy.

Dalia Khader University of Bath [20] Author proposed an Attribute Based Group Signature (ABGS) permits a verifier to demand a signature from a part of a gathering who has notable qualities. Hence, a mark ought to validate an individual in a gathering and

demonstrate responsibility for properties. The significant distinction between our plan and past gathering marks, is that the verifier can focus the part of the genuine endorser inside the gathering. In this paper we define the first ABGS plan, and security thoughts, for example, secrecy and traceability. We then build the plan and demonstrate it.

S Sharmila Deva Selvi, SubhashiniVenugopalan, C. PanduRangan [21] author proposed Enlivened by advancements in characteristic based encryption and marks, there has as of late been a spurt of advancement toward limit property based marks (t-ABS). In this work we propose a novel methodology to develop edge quality based marks motivated by ring marks. Edge trait based marks, defined by a (t,n∗) limit predicate, guarantee that the underwriter holds at least out of a specified set of n∗ credits to pass the verification. An alternate approach to take a gander at this would be that, the underwriter has at least 1 out of the blend of quality sets. In this manner, another methodology to t-ABS would be to let the endorser pick some n0 sets of t traits each, from the n∗ t conceivable sets, and demonstrate that (s)he has at least one of the n0 sets in his/her ownership. In this work, we give a flexible edge ABS conspire that understands this methodology.

PROPOSED METHOOLOGY

I. Existing system

1) The proposed OABS plan with outsourced check diminishes the processing trouble at endorser side through conveying calculation to cloud however just lifting two exponentiations provincially. Since the outsourcing check system is the same as, the security can be additionally ensured focused around the suspicion that the third vendor does not connive 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.

II. Proposed System

In our data shared security system of cloud server have four modules shown in Fig.1. This modules provide the security using same type of input and different type of output methodology and attribute based encryption. The cloud server uses the SaaS service to provide the different keys for each transaction. This will help user to secure the file as for each transaction the cloud generates a separate key for same attribute which in turn increases the security of the system.

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

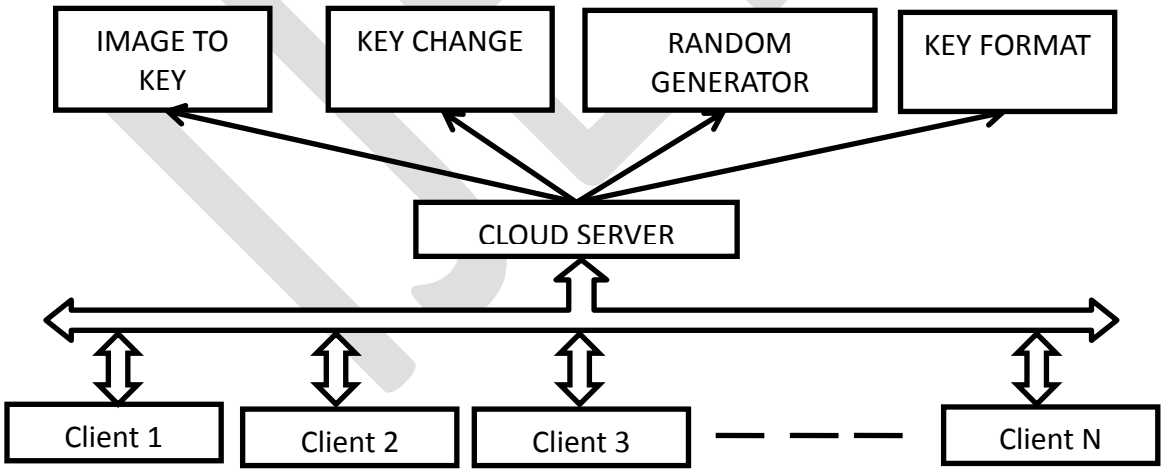

Fig.1: Proposed system architecture

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.

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] 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 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