ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

Authentic Verification through Fine Grained Policies & Device based Security for Applications in Cloud Computing Services

Pranita Kalokhe [1], Dr.Poorna shankar [2]

P.G. Student, Department of Computer Engineering, Indira College Engg & Mgmt, Pune, Maharashtra, India[1]

Head, Department of Computer Engineering, Indira College Engg & Mgmt, Pune, Maharashtra, India [2]

ABSTRACT: A new authentication framework is introduced for fine-grained three-factor authentication (3FA) access control system get to control for web-based distributed computing services. Specially, in our proposed three-factor authentication (3FA) three layer mechanism is implemented. It includes attribute level where depending upon user's attribute roles are assigned to the user, and the access privilege may be different by using access control privileges. Policy level enables fine grained access control over encrypted data using different access policies according to users attributes. Security device level in which security device is initialized by the trustee in Device Initialization. It concentrates on attribute-based access control mechanism with the necessity of a user secret key and a lightweight security device (application).A user is not able to access the system's data if he/she do not hold both, the mechanism will enhance the security of the system, especially in those situations wherever no of users access the same computer system for web-based cloud services. Attribute-based control in the system enables the cloud server to restrict the access to those users which have similar set of attributes while preserving user privacy, i.e. the cloud server is only aware of that the user fulfils the desired predicate, but doesn't have any idea about exact identity of the user. Finally, we carry out the simulation to demonstrate the practicability of our proposed three-factor authentication (3FA) system.

KEYWORDS: Attribute-based, Fine-grained, Three-factor, Web services, Access control.

I. INTRODUCTION

Cloud computing is a service oriented architecture which provides the services to the end user through client server model. It is a virtual host computing system that allows enterprises to sell, buy, lease or distribute software and different digital resources over the web as an on-demand service. There are many applications of cloud computing, such as data storage, medical information system, big data management, data sharing etc. There are many benefits of web-based cloud services, which include the reduced costs and capital expenditures, scalability, ease of accessibility, increased operational efficiencies, flexibility and immediate time to market.

Although the new paradigm of cloud computing provides multiple benefits, there are mean while additionally considerations relating to security and privacy particularly for web based mostly cloud services. Information security, as it exists in several different applications, is among these challenges that will raise great issues from users after they store sensitive data on cloud servers. As sensitive information could also be keep within the cloud for sharing purpose or convenient access; and eligible users may additionally access the cloud system for varied applications and services, user authentication has become a crucial element for any cloud system. However, it's well acknowledged that privacy is an important feature that has to be thought of in cloud computing systems. Second, it's common to share a laptop among completely different folks. It perhaps simple for hackers to put in some spyware to find out the login password from the web-browser.

A recently proposed access control model known as attribute-based access control could be a smart candidate to tackle the first drawback. It not solely provides anonymous authentication however additionally further defines access control policies supported totally different attributes of the requester, setting, or the data object. In an attribute-based access control system, 1 every user incorporates a user secret key issued by the authority. In observe, the user

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

secret key is hold on within the private pc. After we think about the higher than mentioned second drawback on web-based services, it's common that computers could also be shared by several users particularly in some large enterprises or organizations. These considerations originate from the fact that cloud servers are typically operated by business suppliers that are very likely to be outside of the trustworthy domain of users.
In these cases, user secret keys might be simply stolen or utilized by an unauthorized party. Even if the pc could also be secured by a password, it will still be possibly guessed or stolen by undetected malware's. A cloud system may have many cloud service providers (CSPs) to improve the performance of said system. Based on availability and work load, the system selects a CSP for the client accessing it. Hundreds or thousands of clients may access the system simultaneously; hence the availability is a major problem. It can be improved by CSPs with data replication. The data owners may want to set some restrictions to clients who are trying to access the data. In this scenario, the distributed data should keep all details about the different access control policies set to data. But again the authorized clients should be categorized according to permission; it will be a problem in a distributed system with many clients.

II. RELATED WORK

Sometimes an image may contain text embedded on to it. Detecting and recognizing these characters can be very important, and removing these is important in the context of removing indirect advertisements, and for aesthetic reasons.
In several distributed systems a user can able to access data if a user posses a certain set of credentials or attributes. Presently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server stores the data, which is compromised, then the confidentiality of the data will be compromised. In this paper, author present a process for realizing complex access control on encrypted data that author said Cipher text-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted;[2]moreover, our systems are secure against collusion attacks. Previous Attribute Based Encryption systems used attributes to explain the encrypted data and built policies into users keys; while in our system attributes are used to explain a users credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our systems are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, author ensure an implementation of our system and give performance measurements [1].
An attribute based encryption scheme capable of handling multiple authorities were recently proposed by Chase. The scheme is built upon a single-authority attribute based encryption technique presented earlier by Sahai and Waters. [6]-[9] Chases construction uses a trusted central authority that is inherently able to do decrypting arbitrary cipher texts created within the system. We present a multi-authority attribute based encryption technique in which only the set of recipients defined by the encrypting party can decrypt a corresponding cipher text [5]. The central authority is shown as honest-but-curious: on the one hand it honestly follows the protocol, and on the other it is curious to decrypt arbitrary cipher texts thus violating the intent of the encrypting party. The advance scheme, which like its predecessors relies on the Bilinear DiffieHellman assumption, has a complexity comparable to that of Chases technique. We prove that our scheme is secure in the selective ID model and can tolerate an honest-but-curious central authority. Building on the proposal for multi authority based attribute based encryption from; author constructed a scheme where thecentralauthorityisnolongercapableofdecryptingarbitraryciphertextscreated within the system. In addition to viewing security in the selective ID model, author showed that the proposed system can able to tolerate an honest-but-curious central authority[7]. Since both Chases scheme and the proposed scheme rely on the same hardness assumption, and have a comparable complexity, the new scheme seems a viable alternative to Chases construction. However, since the proposed method is capable of handling a curious yet honest central authority, the proposed scheme is suggested in applications where security against such a central authority is required[2].
Securing data stored in clouds using privacy preserving authenticated access control. Authors proposed a privacy preserving access control scheme for data storage, which supports anonymous authentication and performs decentralized key management. In the proposed scheme ,the cloud adopts an access control policy and attributes hiding strategy to enhance security[4].
As a sophisticated mechanism for secure well-grained access control, cipher text policy attribute-based encryption (CPABE) is a highly promising solution for commercial applications like cloud computing. But there still exists one major issue awaiting to be solved, that is, the prevention of key abuse. The existing CP-ABE

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

Systems missed this critical functionality, hindering the wide utilization and commercial application of CP-ABE systems to date. Here we address two practical problems about the key abuse of CP-ABE: The key escrow problem of the half-trusted authority; and, The malicious key delegation problem of the users. For the semi trusted authority, its misconduct (i.e., illegal key (re-)distribution) should be caught and prosecuted. And for a user, his/her malicious conduct (i.e., illegal key sharing) need be traced. We affirmatively solve these two key abuse issues by proposing the first accountable authority CP-ABE with white box traceability that supports policies expressed in any monotone access structures. And we provide an audit or to judge publicly when the rasp acted serisguiltyor is framed by the authority[8]. In this process, we addressed two practical problems about the key abuse of CP-ABE in the cloud, and have presented an accountable authority CP-ABE technique supporting white box traceability and public auditing. Specifically, the proposed system could trace the spiteful users for illegal key sharing. And for the half trusted authority, its illegal key (re-)distributing misconduct could be caught and prosecuted. Furthermore, we have provided an audit or to judge whether a malicious us Eris naive or framed by the authority. As far as we know, this is the first CP-ABE technique that simultaneously encourages white-box traceability, accountable authority, public auditing. We have also proved that the new system is total protection in the standard model. Note that there exists a stronger notion for traceability called black-box traceability. In black box scenario, the malicious user can hide the decryption algorithm by tweaking it, as well as the decryption key. And in this case, the advanced system with white box traceability in this paper will fail since both the decryption key and decryption algorithm are not good. In our future work, we will focus on constructing an accountable authority CP-ABE technique which is black-box traceability and public auditing [3]. Attribute-based encryption module is using for each and every node encrypt data store. After encrypted data and again the re encrypted the same data is using for fine-grain concept using user data uploaded. The attribute-based encryption have been proposed to secure the cloud storage. Attribute-Based Encryption (ABE). In such encryption scheme, an identity is viewed as a set of descriptive attributes, and decryption is possible if a decrypters identity has some overlaps with the one specified in the ciphertext.

III. OBJECTIVE

-To improve new Fine-grained three-factor authentication (3FA) access control method for cloud based portals.
-To generate 3FA access control method involves, an attribute, Policy and device based security mechanism is carried out to generate secret key and a lightweight protection mechanism.
-To remove dependency on a server or a number of machines that physically exists, as it is a virtual system. User authentication has become important component for any cloud system.
- To solve security problem in sharing where the number of resources get shared across multiple users.
- To overcome traditional account password based authentication as it not privacy preserving, the new authentication system is introduced.
- To generate user level policies for access control.
- To develop an mobile application to implement security.
- To ensure to resist unauthenticated user.

IV. PROBLEM STATEMENT

Cloud storage permits a large number of users having different roles and access permissions to share and store their data. In a distributed environment multiple copies of data is there to improve availability. Hence the integrity and access control are major concerns, with respect to data accessibility to users. The normal account/password authentication just isn't privateness retaining. However, it's well stated that privateness is an primary function that need to be regarded in cloud computing systems.

- User level The users role may be different, and the access privilege may be different by using access control.
- Policy level This enables fine grained access control over encrypted data using access policies.
- Security device level The security device is initialized by the trustee in Device Initialization.

Finally the attribute issuing authority generates the user attribute secretkey according to the users attribute in AttrGen.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

V. RESEARCH TECHNIQUE

1. User Key Generation Phase:

The user key generation process consists of three parts.

- First, the user generates his secret and public key in USetup.
- Then the security device is initialized by the trustee in Device Initialization. All the public parameters generated are used during the authentication process.
- Finally the attribute issuing authority generates the user attribute secret key according to the users attribute in AttrGen. The secret generated by the attribute issuing authority determines which all data the user can access and this key is stored in the user computer. The user has to use his own computer and the USB key storage each time for accessing the cloud. Additional recovery options are also provided.

2. Access Authentication Phase:

The access authentication process is an interactive protocol between the user and the cloud service provider. It requires the user to have his partial secret key, attribute secret key , Policy details and the security device each time the user is accessing the cloud. When the server wants the user authenticate to it towards the server, it must respond appropriately to unauthenticated requests. When the user wants to send the server authentication credentials it might use the Authorization. HTTP doesn't offer a technique for an internet server to instruct the consumer to "log out" the user. However, there is variety of strategies to clear cached credentials in sure internet browsers. One among them is redirecting the user to a universal resource locator (URL) on identical domain containing credentials that are by design incorrect. The interactive authentication protocol takes as input TPK, APK and a claim-predicate. User has some additional inputs having an attribute secret key SKX, Y for attribute A, USK = y and the security device.

3. Security Mediator :

In a SMC system, a user contains a secret key, public key and an identity. In the signing or decryption algorithm, it needs the secret key and therefore the SEM along. Within the signature verication or encryption algorithmic program, it needs the user public key and therefore the corresponding identity. Since the SEM is controlled by associate degree authority that is employed to handle user revocation, the authority refuses to supply any cooperation for any revoked user. Therefore revoked users cannot generate signature or decrypt ciphertext. SMC is completely different from our conception. The most purpose of SMC is to unravel the revocation downside. Therefore the SME is controlled by the authority. In different words, the authority has to be on-line for each signature language and ciphertext cryptography. The user isn't anonymous in SMC. Whereas in our system, the safety device is controlled by the user.

VI. IMPLEMENTATION

First the user secret key (which is usually stored inside the computer) is required. In addition, the security device should be also connected to the computer (e.g. through Android Device) in order to authenticate the user for accessing the cloud using QR Code. The user can be granted access only if he has both items. Furthermore, the user cannot use his secret key with another device belonging to others for the access. Our protocol supports fine-grained attribute-based access which provides a great flexibility for the system to set different access policies according to different scenarios. At the same time, the privacy of the user is preserved. The cloud system only knows that the user possesses some required attribute, but not the real identity of the user. To show the practicality of our system, we simulate the prototype of the protocol. Device Authentication using QRCODE and Android App: IMAGE(image url, alternate text[height, width]): Is a function to show image with giving data 2.1 chs: Height and width of QR Code 2.2 cht: Chart Type. We need to put qr for QR code 2.3 chl: QR Code will generate this Device and data accessing Key. Simple Password Exponential Key Exchange(SPEKE) Simple Password Exponential Key Exchange SPEKE makes only one small

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

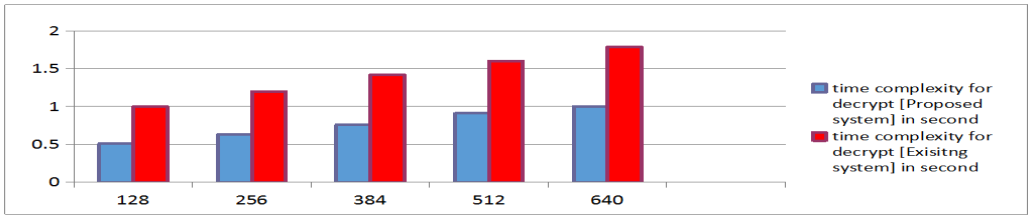
Vol. 6, Issue 7, July 2017

change to the Diffie-Hellman Key Exchange. Rather than agreeing on a shared generator, each party will compute a generator (G;Step2) by squaring the hash of some shared password. Because the generator (G) is now derived from a password, it is private.. Hence, if only Alice and Bob know the shared password, then this algorithm is safe from a Met attack. And since the generator(G) is private, no offline dictionary attack is possible. Note well, however, that no validation of K has occurred. So while Alice knows that data encrypted with K can not be read by any one but Bob, she's till doesn't know whether the person on the other end of the exchange is, in fact, Bob. If it isnt Bob on the other end, K will contain an on sensual value and any data encrypted by it will be irretrievable.
In our system we tend to proposed a RC6 (Rivest cipher 6) algorithm to boost the security. RC6 includes a easy structure and outline relative to the opposite proposed block ciphers. RC6 was one among ve analysts for the Advanced encryption standard. It consists of 2 Feistel networks whose information are mixed via information dependent rotations. The operations in one round of RC6 are the following: two applications of the squaring function f (x) = x (2x + 1) mod 232, two xed 32-bit rotations, two data- dependent 32-bit rotations, two exclusive ors and two additions modulo 232.A version of the RC6 is additional accurately specied as RC6w/r/b wherever the word size is w bits, coding consists of a non-negative range of rounds r, and b denotes the length of the coding key in bytes. RC6 formula receives 3 parameters RC6-w/r/b wherever the word size is w bits, coding consists of a non-negative range of rounds r, and b denotes the length of the coding key in bytes.We additionally projected SPEKE(Simple Arcanum Exponential Key Exchange) algorithmic program for key generation. it's Associate in Nursing older and well-known protocols within the comparatively new field of password authenticated key exchange. We use adventurer algorithmic program as a result of it prevents off-line wordbook attack on tiny passwords. It Survive on-line wordbook attack. It Provides mutual authentication.

VII. RESULT ANALYSIS

Result For Data Processing :
Differentiate output results of enc-dec (Base 64, Hexadecimal) results are given in Fig. for Exisiting and Proposed System, Fig. shows the results at base 64 encoding while It gives the results of hexadecimal base encoding. We can notice that there is significant difference at both system. The same method is applied for encryption with multiple sample; we can recognize that the two bars given in image.

Data in KB	time complexity for Decrypt[Proposed system] in second RC6	time complexity for Decrypt[Existing system] in second AES
128	0.51	1
256	0.63	1.2
384	0.76	1.42
512	0.91	1.6
640	1	1.79



VIII. CONCLUSION

The model proposed in this paper gives power to the data owner to implement the security process attrubute, policy and device mechanism, and hence retain the control over the data. The model also proposed the combination of cryptography and access control to keep the data safe from vulnerabilities. A multi factor authentication approach is employed for the authentication and authorization of the client, which increase the confidentiality and integrity of the data, which guarantee the isolation and safe execution of the cloud environment.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

REFERENCES

[1] L. Vaquero, L. Rodero-Merino, J. Caceres and M. Lindner, A break in the clouds: towards a cloud denition, ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, (2008), pp. 50-55.
[2] S. Ullah and Z. Xuefeng, Cloud Computing Research Challenges, In Proceedings of 5th IEEE International Conference on Biomedical Engineering and Informatics, (2012), pp. 1397-1401.
[3] S. Yu, C. Wang, K. Ren and W. Lou, Achieving secure, scalable, and ne grained data access control in cloud computing, In INFOCOM, 2010 Proceedings IEEE, IEEE, (2010), pp. 1-9.
[4] L. Yousef, M. Butrico and D. Da Silva, Toward a Unied Ontology of Cloud Computing, Grid Computing Environments Workshop, GCE 08, (2008), pp. 1-10.
[5] Z. Shen and Q. Tong, The Security of Cloud Computing System enabled by Trusted Computing Technology, In Proceedings of 2nd International Conference on Signal Processing Systems, (2010), pp. 11- 15.
[6] R. L. Grossman, The Case for Cloud Computing, IT Professional, vol. 11, no. 2, (2009), pp. 23-27.
[7] S. Ullah, Z. Xuefeng and Z. Feng, TCloud: Challenges and Best Practices for Cloud Computing, International Journal of Engineering Research and Technology, vol. 1, no. 9, (2012), pp. 01-05.
[8] S. Subashini and V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, vol. 34, no. 1, (2011), pp. 1-11.
[9] Di Vimercati, S. De Capitani, S. Foresti, S. Jajodia, S. Paraboschi and P. Samarati, A data outsourcing architecture combining cryptography and access control, In Proceedings of the 2007 ACM workshop on Computer security architecture, ACM, (2007), pp. 63-69.
[10] W. Wang, L. Zhiwei, R. Owens and B. Bhargava, Secure and efcient access to outsourced data, In Proceedings of the 2009 ACM workshop on Cloud computing security, ACM, (2009), pp. 55-66.