ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 2, Issue 8, August 2017

Modified Two Factor Authentication Control For Web Based Cloud Computing Services

[1] R.Raj Priya, [2] R.Karthikeyan, [3] D.Shakilakumari
[1] Research Scholar, Department of Computer Science, Bharath University, Chennai.
[1] Head, Department of MCA, Bharath University, Chennai.
[2] Asst. Professor, Dept. of Computer Science, Pachaiyappa's College for men, Kanchipuram.
[3] Asst. Professor, Dept. of Computer Science, Pachaiyappa's College for men, Kanchipuram.

Abstract: ***Cloud computing web services are the most current and improving technology. In this paper we have two-factor authentication access control system for cloud computing services based on web. In our proposed two factor authentication control system, an attribute-based access control mechanism is implemented with the necessity of a user secret key and an OTP (One Time Password). A user can access the system only if they hold the two factors as mentioned above, this solution can improve the security of the system specifically in times of problem where many users share the same computer for web-based cloud services. Because we are using attribute-based authentication control which is one of our important factor in the system that enables the cloud server to restrict the access to those users with the same set of attributes while preserving user privacy. We use the most improvised algorithm which is a combination of ABE (Attribute Based Encryption) and ABC (Attribute Based Credentials) called ABKE (Attribute Based Key Exchange) which is provided by a certificate authority. We test our system and see the practicability of our proposed three factor authentication system.***

Keywords- ***authentication, ABKE, Secret key, OTP***

I. INTRODUCTION

Cloud computing is an alternate to traditional information technology due to its many advantageous characteristics. Users enjoy the on-demand high-quality applications and services from the shared pool of computing resources by using cloud storage. Cloud Computing is a virtual host computer system which helps users to buy, lease, sell, or distribute software and other digital resources over the internet as an on demand service. Users need not depend on a server or a number of physical machines, as it is a virtual system.

As there are many advantages equally there are many disadvantages in using cloud computing specially for web based cloud services. One of the main disadvantages is hacking the password which leads to many problems like stealing confidential information, uploading dangerous information, altering information to wrong updates etc. There are many more problems but handling authentication is very important factor in cloud web services. In our daily life everyone uses email web service which is an example of web based cloud services. Currently we all are using login id and password which is not privacy preserving neither highly secured solution. Not all our mails are confidential but some are which might be sometimes highly secret too, so preserving confidential matters in web based cloud services are the biggest task and challenge.

In our existing system they use a light weight device and a secret key. The secret key is computed using the attribute based encryption (ABE) method which is issued by attribute issuing authority. The light weight device is issued by a trustee which is a small device which generates numbers through built in hash function and displays it. The device is issued by trustee upon registration of the user. But the disadvantage is that they assume that the light weight device is unbreakable which cannot hold true all times. Also if it is stolen then everything goes wrong.

In our proposed system we use modified two factor authentication control. The first factor is a secret key which is a concept same as in existing system but with a small change which incurs big difference. The change is the algorithm used to generate secret key. In our existing system also they generated the key using attribute based encryption but we use the Attribute based key Exchange algorithm which is the combination of Attribute based encryption and attribute based credentials. Also along with secret key we use a OTP (One Time Password) which is generated using random oracle generator. Even though it is a simple factor it reduces the burden of user to carry a physical device called light weight device present in the existing system.

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 2, Issue 8, August 2017

II. PROBLEM STATEMENT

2.1 System Model:

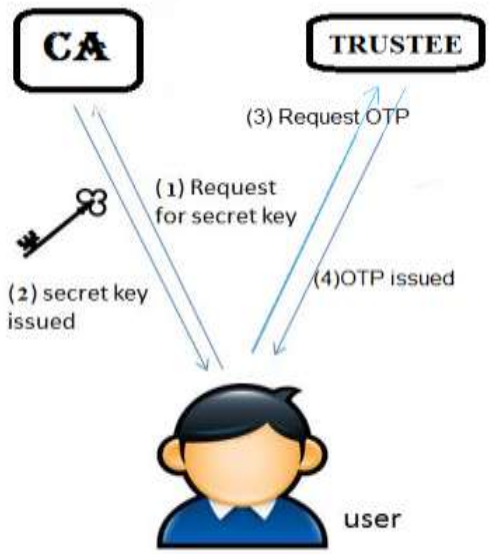

Figure 1 User secret key and OTP generation process

The proposed system consists of four modules and people involved. The data owner also called as user, the cloud server, the certificate authority also called as CA, and the trustee. The user is one who wants to secure his or her own data from stranger which is stored at cloud server. The cloud server is where all the user data are stored and maintained. The CA is one who provides secret key upon registration. It's a shared key which is provided to cloud once it is sent to user. The CA generates the secret key using Attribute based key exchange (ABKE) algorithm which is a combination of attribute based encryption (ABE) and attribute based credentials (ABC). The trustee is one who generates and provides OTP each time when there is a need for access to cloud by user. This happens when the user requests OTP during each access. . The OTP is of four digits which are generated by trustee using random generator. The sent OTP is also shared to the Cloud for verification. The cloud grants user the permission to access if and only if it provides the correct OTP and the correct secret key which matches the attributes of the user and also checks to that whether it was the correct shared key provided by the CA. Like secret key it also checks to that it was the correct shared OTP. The OTP can be generated by the cloud but in this system there are many chances both for the cloud and the user to misbehave. Both are considered to be dishonest. Therefore we engage CA and trustee. Also there are no chances that none of the four knows the two factor at a time which reduces is the chance of all problems and thus increases the

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 2, Issue 8, August 2017

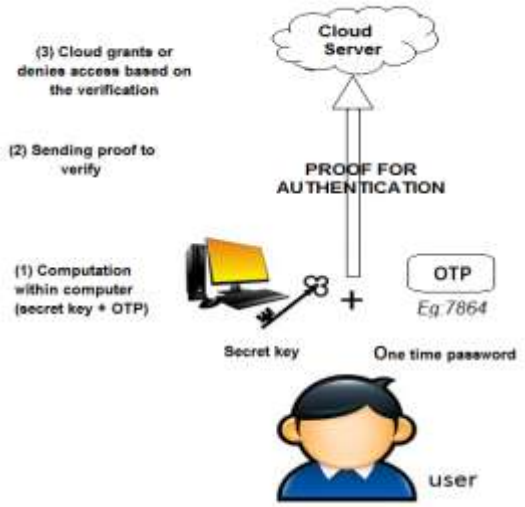

Figure 2 Authentication process

There are two figures shown above in this system. The figure1 shows how the first phase, user secret key and OTP generation process works. In this phase the user receives a secret key and OTP from the CA and the trustee upon requests. The figure2 shows how the second phase, the authentication process works. Here the cloud verifies the user by the authentication factors he or she has provided. And then grants or denies access to data present on cloud.

2.2 Threat Model:

i) Threats caused during authentication:

A user might try to provide wrong attribute and try to access beyond his privileges gathering information from around.

ii) Threats caused by accessing without secret key:

There are chances for a user to misbehave by trying to access without secret key either by loosing or trying to access others accounts.

iii) Threats caused by accessing without OTP:

A user might try to access without OTP because he is trying to access others data.

iv) Threats caused by others:

Since there are chances for multiple people to share same system there are many chances to hack and steal confidential data.

III. ATTRIBUTE BASED KEY ENCRYPTION (ABKE) ALGORITHM:

Attribute Based Encryption (ABE):

ABE is an algorithm which is based upon public key cryptography. Let's see the basic public key cryptography where the data is encrypted using the receiver's public key and sent to the receiver. After public key cryptography came the Identity Based Encryption (IDE). In IDE they used one of the receiver's attribute for encryption, example the email address, DOB etc.

We should see that in IDE only one identical attribute is used for encryption. Then after IDE comes the advance concept in encryption called ABE .It combines a set of attributes of receiver or user and encrypt the messages that is the data to be passed. There are two types of ABE. Cipher Text Policy Attribute Based Encryption (CP ABE) and Key Policy Attribute Based Encryption (KP ABE).The term or rule is, someone can only be able to decrypt a cipher text if only if the person hold the matching attributes where user keys are always issued by trusted party like Certificate Authority used in this paper. In our proposed system we use CP ABE type of ABE algorithm and below is the explanation.

The Cipher text Policy ABE uses user's private key related with a set of attributes and it also specifies an access policy over a defined universe of attributes within the system. A user to decrypt the cipher text should specify the attributes that satisfy the policy of respective cipher text. Policies are defined using conjunction, disjunction over attributes and (k,n)- Threshold gates. That is k out n attributes have to be present. For example, let us assume that the universe of attribute is defined to be {A, B, C, D} and user 1 receives a Key to attributes {A, B} and user 2 to attribute {D}. If cipher text is encrypted with respect to the policy (A ∧ B) v D then user 2 will be able to decrypt, while user 1 will not be able to decrypt. In the example as per given policy A^B the user 1 should have both attributes A and C simply because the policy states but since it has A and B, it cannot decrypt. User 1 can decrypt since it has attribute D as stated in policy that the user must have either attribute D or attribute A, C. So the authorization is included within the encrypted data that is cipher text and only the user who satisfies the related policy will be able to decrypt the cipher text. So only the authenticated user will be able to decrypt since the policy is designed with such a condition.

Attribute Based Credential (ABC):

Attribute Based Credential algorithm is used by cloud server who provide web services. The cloud server authenticates web service users by providing high security and privacy. The users obtain a certificate which is issued by the CA derived upon attributes which is shown to service provider for authentication. ABC supports multiple communications with same server by one or more users that cannot be linked together. In general they call this as unlinkability.

Attribute Based Key Exchange (ABKE):

ABKE is an algorithm which is actually formed by combining two algorithms. They are Attribute Based Encryption (ABE) and Attribute Based Credential (ABC) algorithms. In the ABE algorithm the user one who decrypts will stay passive and therefore it is called non-interactive. To avoid this from being happening we use the key point called unlinkability present in ABC algorithm. The condition states that the different or multiple users of the system cannot pass the policy combining all their attributes into single for verification that neither could have individually passed. In this paper we aim to obtain an interactive solution that involves a user who holds a certificate issued by CA, claiming for its attributes and a server that consists of a policy that is computable on the certificate (that is set of attributes). The main goal of the server is to establish a shared key with the user, if and only if user's certificate satisfies the policy.

IV. RELATED WORKS

4.1 Scalable secure file sharing on untrusted storage

In this paper the authors M.Kallahalla, E.Riedel, R.Swaminathan, Q.Wang, and K.Fu explains about the cryptographic file system to secure file storage on untrusted servers. Here they group a set of files with similar sharing attributes as file group and associates each file group with a symmetric lockbox key. Each file is encrypted using a unique file block key which is further encrypted with lock box key. But the disadvantage is that the complexity of key management is proportional to the total number of file groups. So it is not suitable for huge file groups.

4.2 On defining proofs of knowledge

The authors of this paper are M. Bellare and

o. Goldreich. They give us a complete explanation about proofs of knowledge in this paper. Intuitively, a two-party protocol constitutes a system for proofs of knowledge if one party (called the verifier) is convinced that the other party (called the prover) indeed knows some "knowledge. A proof of knowledge is a two-party protocol with the following properties. At first the completeness, if $(x, y) \in R$, the honest prover who knows witness y for x succeeds in convincing the honest verifier of his knowledge. Then soundness, if $(x, y) /\in R$, no cheating prover can convince the honest verifier that $(x, y) \in R$, except with some small probability. It can be captured by the existence of a *knowledge extractor E* to extract the witness y: given oracle access to a cheating prover P, the probability that E outputs y must be at least as high as the success probability of P in convincing the verifier. For a zero-knowledge proof of knowledge, it has the extra property of Zero-knowledge, no cheating verifier learns anything other than $(x, y) \in R$. It is formalized by showing that

every cheating verifier has some simulator that can produce a transcript that is indistinguishable with an interaction between the honest prover and the cheating (or honest) verifier.

4.3 Achieving secure scalable and fine grained data acces control in cloud computing

The authors of this paper are Shucheng yu, Cong Wang, Kui Ren, and Wenjing Lou. This paper addresses two challenging open issues. One by defining and enforcing access policies based on data attributes and on other hand allowing the data owner to delegate most of the computation tasks involved in fine grained data access control to untrusted servers without disclosing the underlying data contents.

4.4 Fine grained two factor access control for web based cloud computing services

Joseph K. Liu, Man Ho Au and Xinyi Huang are the authors of this paper. In this paper they introduce two factors one is a secret key based on attributes using ABE algorithm. The other factor is a light weight security device that computes numbers using built in hash function. This is our existing system. The disadvantage is the security device which might be broken, stolen, lost or forgotten to be carried by the user.

V. CONCLUSION

The aim of this paper is to provide high security for web based cloud services. To do so the user's data are protected by restricting the access of wrong users during the authentication process itself. Thereby we have provided secure two factor authentication control for web based cloud services. The two factors are the secret key and the OTP. The secret key is modified concept in which the most secured algorithm ABKE is used. The second factor, one time password which is simple but widely used is combined with secret key. Also we should note that none the people in the model knows the two factor before the authentication process which guarantees the complete security.

VI. REFERENCES

[1] Joseph K. Liu, Man Ho Au and Xinyi Huang,
"Fine grained two factor access control for web based cloud computing services," in *ieee transactions on information forensics and security*,vol. 11, no. 3, march 2016
[2] M. H. Au, A. Kapadia, and W. Susilo, BLACR: TTP-free blacklistable anonymous redentials with reputation," in *Proc. 19th NDSS*, 2012, pp. 1–17.
[3] M. H. Au, W. Susilo, and Y. Mu, "Constant-size dynamic *k*-TAA," in *Proc. 5th Int. Conf. SCN*, 2006, pp. 111–125.
[4] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang, "A secure cloud computing based framework for big data information management of smart grid," *IEEE Trans. Cloud Comput.*, vol. 3, no. 2, pp. 233–244,
Apr./Jun. 2015.
[5] M. Bellare and O. Goldreich, "On defining proofs of knowledge," in
Proc. 12th Annu. Int. CRYPTO, 1992, pp. 390–420.
[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in
Proc. IEEE Symp. Secur. Privacy, May 2007, pp. 321–334.
[7] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures,"in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 2004, pp. 41–55.
[8] D. Boneh, X. Ding, and G. Tsudik, "Fine-grained control of security capabilities," *ACM Trans. Internet Technol.*, vol. 4, no. 1, pp. 60–82,
2004.
[9] Shucheng Yu, Cong Wang, Kui Ren , and Wenjing LouAchieving," Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing" in IEEE telecom 2010
[10] J. Camenisch, M. Dubovitskaya, and G. Neven, "Oblivious transfer with access control," in *Proc. 16th ACM Conf. Comput. Commun.*
Secur. (CCS), Chicago, IL, USA, Nov. 2009, pp. 131–140.
[11] J. Camenisch and A. Lysyanskaya, "A signature scheme with efficient protocols," in *Proc. 3rd Int. Conf. Secur. Commun. Netw. (SCN)*, Amalfi, Italy, Sep. 2002, pp. 268–289.
[12] J. Camenisch and A. Lysyanskaya, "Signature schemes and anonymous credentials from bilinear maps," in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 2004, pp. 56–72.

[13] Y. Chen, Z. L. Jiang, S. M. Yiu, J. K. Liu, M. H. Au, and X. Wang, "Fully secure ciphertext-policy attribute based encryption with security mediator," in *Proc. ICICS*, 2014, pp. 274–289.
[14] S. S. M. Chow, C. Boyd, and J. M. G. Nieto, "Security-mediated certificateless cryptography," in *Public Key Cryptography* (Lecture Notes in Computer Science), vol. 3958. Berlin, Germany: Springer-Verlag, 2006, pp. 508–524.
[15] C.-K. Chu, W.-T. Zhu, J. Han, J.-K. Liu, J. Xu, and J. Zhou, "Security concerns in popular cloud storage services," *IEEE Pervasive Comput.*, vol. 12, no. 4, pp. 50–57, Oct./Dec. 2013.
[16] R. Cramer, I. Damgård, and P. D. MacKenzie, "Efficient zero-knowledge proofs of knowledge without intractability assumptions," in *Public Key Cryptography* (Lecture Notes in Computer Science), vol. 1751, H. Imai and Y. Zheng, Eds. Berlin, Germany: Springer-Verlag, 2000, pp. 354–373.
[17] Y. Dodis, J. Katz, S. Xu, and M. Yung, "Key-insulated public key cryptosystems," in *Proc. EUROCRYPT*, 2002, pp. 65–82.
[18] Y. Dodis and A. Yampolskiy, "A verifiable random function with short proofs and keys," in *Public Key Cryptography* (Lecture Notes in Computer Science), vol. 3386, S. Vaudenay, Ed. Berlin, Germany: Springer-Verlag, 2005, pp. 416–431.
[19] Vladimir kolesnikov, Hugo Kraweczk, Yhuda lindell and Tal Rabin", Attribute-based Key Exchange with General Policies", URL:https://eprint.iacr.org/2016/518 presented at ACM CCS 2016.