



Two Factor Authentication And Access Control For Cloud Computing Services

¹Amal.M.R, ²Jisha P Abraham
M. Tech Computer Science and Engineering
M.A. College of Engineering, Kothamangalam-686666
Ernakulam, Kerala, India

Abstract: Cloud computing is a virtual host computer system that enables enterprises to buy, lease, sell, or distribute software and other digital resources over the internet as an on-demand service. Though the new paradigm of cloud computing provides great advantages, there are meanwhile also concerns about security and privacy especially for web based cloud services. A two-factor authentication (2FA) and access control system for web-based cloud computing services is developed. Specifically, in the proposed 2FA access control system, an attribute-based access control mechanism is implemented with the necessity of both user secret key and a lightweight security device. As a user cannot access the system if s/he does not hold both, the mechanism can enhance the security of the system, especially in those scenarios where many users share the same computer for web-based cloud services. In addition, attribute-based control in the system also enables the cloud server to restrict the access to those users with the same set of attributes while preserving user privacy, i.e., the cloud server only knows that the user fulfills the required predicate, but has no idea on the exact identity of the user.

Keywords: Cloud Computing, Security, Authentication, Access Control, USB Storage Key

I. Introduction

Cloud computing is a virtual host computer system that enables enterprises to buy, lease, sell, or distribute software and other digital resources over the internet as an on-demand service. It no longer depends on a server or a number of machines that physically exist, as it is a virtual system. User authentication has become a critical component for any cloud system. A user is required to login before using the cloud services or accessing the sensitive data stored in the cloud. There are two problems for the traditional account/password based system. First, the traditional account/password based authentication is not privacy-preserving. However, it is well acknowledged that privacy is an essential feature that must be considered in cloud computing systems. Second, it is common to share a computer among different people. It may be easy for hackers to install some spyware to learn the login password from the web-browser. A recently proposed access control model called attribute-based access control is a good candidate to tackle the first problem. It not only provides anonymous authentication but also further defines access control policies based on different attributes of the requester, environment, or the data object. In an attribute-based access control system, each user has a user secret key issued by the authority. In practice, the user secret key is stored inside the personal computer. While considering the above mentioned second problem on web-based services, it is common that computers may be shared by many users especially in some large enterprises or organizations.

In this paper, it is intended to develop a high end security system for providing authentication and access control mechanism which is very fast and accurate in computation as well as limited usage of storage server.

II. Two Factor Access Control

The system setup process consists of two parts. The first part TSetup is run by a trustee to generate public parameters. The second part ASetup is run by the attribute issuing authority to generate its master secret key and public key. The process of authenticating the user and access control mechanism consist of mainly two steps.

A. 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 user's 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.

B. 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 and the security device each time the user is accessing the cloud.

The interactive authentication protocol takes as input TPK, APK and a claim-predicate. The user has some additional inputs including an attribute secret key $SK_{x,y}$ for attribute A, $USK = y$ and the security device. Parse $sk_{A,y}$ as (A, e, s, x^A) .

III. Problem statement

A. Two Factor Authentication:-

The main task is to analyze and identify the identity of the user. Who is the user and what the role of that user is. Various two factor authentication mechanisms such as OTP passwords, etc. can be used for this purpose. Such authentication mechanism can validate the user credentials.

S

B. Two Factor Access Control

According to cloud based applications and services the important task is access control. Which all data a genuine user can access with his role. The user's role may be different, and the access privilege may be different by using two factor access control the user can access the data according to his role without use of storage server access. In this paper a new method which can be used for implementing both this access control and authentication is described.

IV. Solution

A. Attribute-Based Cryptosystem :-

ABE enables fine grained access control over encrypted data using access policies and associates attributes with private keys and cipher texts. Within this context, cipher text-policy ABE (CP-ABE) allows a scalable way of data encryption such that the encrypter defines the access policy that the decrypter (and his/her attributes set) needs to satisfy to decrypt the cipher text. Thus, different users are allowed to decrypt different pieces of data with respect to the pre-defined policy. This can eliminate the trust on the storage server to prevent unauthorized data access. Besides dealing with authenticated access on encrypted data in cloud storage service, ABE can also be used for access control to cloud computing service, in a similar way as an encryption scheme can be used for authentication purpose: The cloud server may encrypt a random message using the access policy and ask the user to decrypt. If the user can successfully decrypt the cipher text (which means the user's attributes set satisfies the prescribed policy), then it is allowed to access the cloud computing service.

B. Mediated cryptography:-

Mediated cryptography was first introduced in as a method to allow immediate revocation of public keys. The basic idea of mediated cryptography is to use an on-line mediator for every transaction. This on-line mediator is referred to a SEM (Security Mediator) since it provides a control of security capabilities. If the SEM does not cooperate then no transactions with the public key are possible any longer.

C. Key-Insulated Cryptosystem:-

The general idea of key-insulated security was to store long-term keys in a physically-secure but computationally-limited device. Short-term secret keys are kept by users on a powerful but insecure device where cryptographic computations take place. Short term secrets are then refreshed at discrete time periods via interaction between the user and the base while the public key remains unchanged throughout the lifetime of the system. At the beginning of each time period, the user obtains a partial secret key from the device. By combining this partial secret key with the secret key for the previous period, the user renews the secret key for the current time period. Different from the proposed concept, key-insulated cryptosystem requires all users to update their keys in every time period. The key update process requires the security device. Once the key has been updated, the signing or decryption algorithm does not require the device anymore within the same time period. While the proposed concept does require the security device every time the user tries to access the system. Furthermore, there is no key updating required in the system.

C. Monotone span program:-

The proposed access control mechanism depends on expressing the attribute predicate as a monotone span program, which is defined as a monotone Boolean function as follows

$$\Upsilon : \{0, 1\}^n \rightarrow \{0, 1\}$$

$$\Upsilon(x_1, \dots, x_n) = 1 \iff \exists \vec{v} \in \mathbb{F}^{1 \times \ell} : \vec{v}\mathbf{M} = [1, 0, 0, \dots, 0]$$

$$\text{and } (\forall i : x_{\rho(i)} = 0 \Rightarrow v_i = 0).$$

D. BBS+ signatures:-

A signature scheme called BBS+ is used. It belongs to a class of signature schemes, commonly known as CL-signatures. CL-signatures are useful in certifying credentials since their structures allows a signer to create a signature on committed values; and a signer holder to prove to any third party that he/ she is in possession of a signature from the signer in zero knowledge. Let the public parameters are

$$(p, \mathbb{G}, \mathbb{G}, \mathbb{G}_T, \hat{e}) \leftarrow \mathcal{G}(1^\lambda)$$

The generators of the cyclic group are

$$\hat{g}, h, h_0, h_1, \dots, h_n \in \mathbb{G}$$

Compute the following, thus signature A is generated

$$A = (hh_0^{x_0} h_1^{x_1} \dots h_n^{x_n} \hat{g}^s)^{\frac{1}{\gamma+e}}$$

Evaluated during authentication as follows

$$\hat{e}(A, wh^e) = \hat{e}(hh_0^{x_0} h_1^{x_1} \dots h_n^{x_n} \hat{g}^s, h)$$

E. Proof of knowledge protocol:-

A proof of knowledge is a two-party protocol with the properties such as completeness and soundness. Completeness in the sense if x and y belongs to R the honest prover who knows witness y for x succeeds in convincing the honest verifier of his knowledge. Soundness is if x and y is not belonging to R no cheating prover can convince the honest verifier that x and y belongs to 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 and y belongs to 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.

V. Schema Description

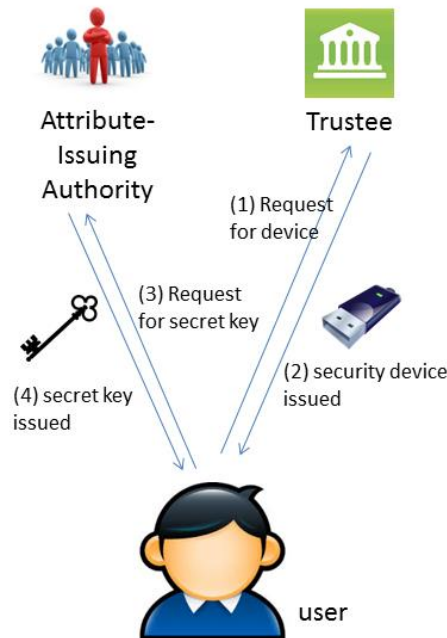


Figure 1 User Key Generation Process

The security device employed in the system satisfies the following requirements. The security key used is tamper resistant and it is capable of evaluation of a hash function. In addition, it can generate random numbers and compute exponentiations of a cyclic group defined over a finite field. Let A be the desired universe of attributes. For simplicity, assuming that $A = [1, n]$ for some natural number n . We will use a vector x belongs to $\{0, n\}$ n to represent the user's attribute set. Let vector $x = (x_1, \dots, x_n)$ belongs to $\{0,1\}^n$. If the user is in possession of

attribute i , $x_i = 1$. Otherwise, $x_i = 0$. The system setup process consists of two parts. The first part TSetup is run by a trustee to generate public parameters. The second part ASetup is run by the attribute issuing authority to generate its master secret key and public key. 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. Finally the attribute issuing authority generates the user attribute secret key according to the user's attribute in AttrGen.

Figure 2 shows the access authentication process, which 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 and the security device. The interactive authentication protocol takes as input TPK, APK and a claim-predicate. The user has some additional inputs including an attribute secret key $SK_{X,Y}$ for attribute A, $USK = y$ and the security device. Parse $sk_{A,Y}$ as $(A, e, s, x^\wedge)$.



Figure 2 User Access Authentication Process

- 1) The authentication server picks at random a challenge R belongs to Z_p and sends R to the user
- 2) The user computes $C = e^\wedge(g, h_0^{1/(y+R)})$ and submits (C, y, R) to his /her security device
- 3) The security device validates $C^{(y+R)} = TG$ and $TG^y = TY$.
- 4) Upon successful validation, the security device picks a random r belongs to Z_p , computes $C_R = H(TGr \parallel R \parallel C)$ and $Z_R = r - CR^{tsk}$. It returns (C_R, Z_R) to the user.
- 5) The user converts claim predicate value to its corresponding monotone span program $M = (M_i, j)$ belongs to $Z_p^{1^*m}$, with row labeling.
- 6) For $i = 1$ to l , the user randomly picks a_i ; t_i belongs to Z_p and computes $C_i = g^{vi} h^{ti}$
- 8) Then engage in zero-knowledge protocol, all the parameters are given to the protocol for validation process.

A. Input Design:-

This is a process of converting user inputs into computer based formats. The data is fed into system using simple interactive forms. The forms have been supplied with messages so that user data is read without facing any difficulty. The data is validated wherever it requires in the project. This ensures that only the correct data have been incorporated into the system. It also includes determining the recording media methods of input, speed of capture and entry into the system.

B. Output Design:-

A quality output is one, which meets the requirements of the end user and presents the information clearly. In the output design, it is determined how the information is to be displayed for immediate need and also the hard copy output. The output design should be understandable to the user and it must offer great convenience. The output of the proposed software tool is designed as opening the text file containing the translated code.

The main objectives that guide the output design is that the user must be informed with proper messages and access permissions in case of any un usual key input or in case of the right key validation.

VI. Experiment Analysis

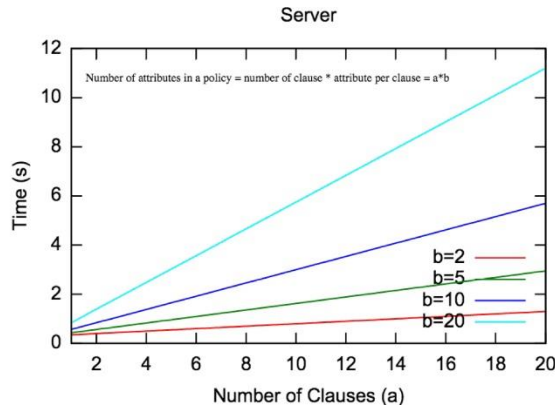


Figure 3 Running time of the Authentication protocol (Server side)

The system is analyzed for evaluating the performance for further development. Fig. 3 shows the time cost of the server to authenticate a single user. For a relatively simple policy, say, consisting of 2 clauses with 2 attributes per clause for a total of 4 attributes, the time is less than 0.3 seconds. For a policy of 10 clauses with 10 attributes per clause, the time is around 3 seconds. While the asymptotic complexity at the user is similar to that of the server, the time cost for a user is about five times slower due to the use of a less powerful computing device. One should note that the security device is not the bottleneck as it only accounts for a constant time cost of 0.6 seconds.

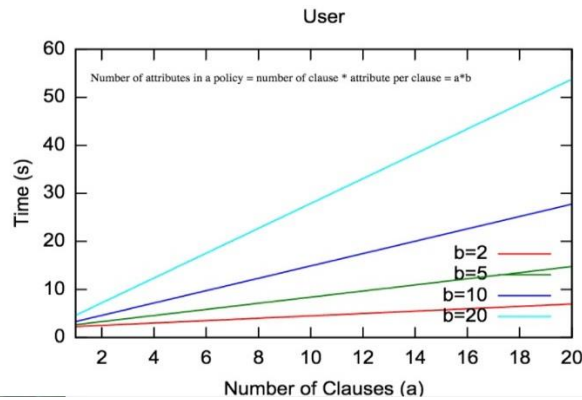


Figure 4 Running time of the Authentication protocol (User side)

The communication cost of our protocol is depicted in Fig. 9. In particular, for a policy of 100 attributes, the total bandwidth requirement is around 45 KB, which is acceptable for today's network. One could conclude that our protocol is plausible for very simple policy and is still not practical yet for policy of medium size.

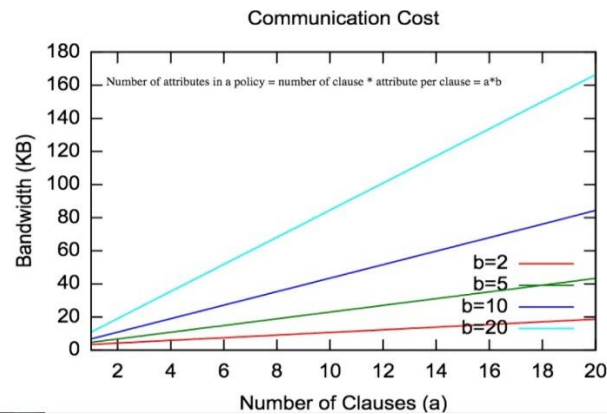


Figure 5 Communication cost of the Authentication protocol (KB)

VII. Conclusion

A new 2FA (including both user secret key and a lightweight security device) authentication and access control system for web-based cloud computing services has been developed. Based on the attribute-based access control mechanism, the proposed 2FA access control system has been identified to not only enable the cloud server to restrict the access to those users with the same set of attributes but also preserve user privacy. Detailed security analysis shows that the proposed 2FA access control system achieves the desired security requirements. Through performance evaluation, it is demonstrated that the construction is “feasible”. In future work the efficiency has to be improved while keeping all nice features of the system.

VIII. Future Scope

This paper has a vast future scope of work. It is highly extensible. The security issues are increasing day by day. Since the technologies and its secure use is an important concern we use different and secure access control and authentication mechanism. The major concern is more user friendly and highly secure measures must be developed and implemented. So the future work has a scope on this area where more user friendly security measures has to be concentrated.

References

- [1] M. H. Au and A. Kapadia. PERM: practical reputation-based blacklisting without TTPS. In T. Yu, G. Danezis, and V. D. Gligor, editors, the ACM Conference on Computer and Communications Security, CCS'12, Raleigh, NC, USA, October 16-18, 2012, pages 929–940. ACM, 2012.
- [2] M. H. Au, A. Kapadia, and W. Susilo. Blacr: Ttp-free blacklistable anonymous credentials with reputation. In NDSS. The Internet Society, 2012.
- [3] M. H. Au, W. Susilo, and Y. Mu. Constant-Size Dynamic k-TAA. In SCN, volume 4116 of Lecture Notes in Computer Science, pages 111–125. Springer, 2006.
- [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 T. Cloud Computing, 3(2):233–244, 2015.
- [5] M. Bellare and O. Goldreich. On defining proofs of knowledge. In CRYPTO, volume 740 of Lecture Notes in Computer Science, pages 390–420. Springer, 1992.
- [6] J. Bethencourt, A. Sahai, and B. Waters. Cipher text-policy attribute-based encryption. In IEEE Symposium on Security and Privacy, pages 321–334. IEEE Computer Society, 2007.
- [7] D. Boneh, X. Boyen, and H. Shacham. Short Group Signatures. In Franklin [19], pages 41–55.
- [8] D. Boneh, X. Ding, and G. Tsudik. Fine-grained control of security capabilities. ACM Trans. Internet Techn., 4(1):60–82, 2004.
- [9] J. Camenisch. Group Signature Schemes and Payment Systems Based on the Discrete Logarithm Problem. PhD thesis, ETH Zurich, 1998. Reprint as vol. 2 of ETH Series in Information Security and Cryptography, ISBN 3-89649-286-1, Hartung-Gorre Verlag, Konstanz, 1998.
- [10] J. Camenisch, M. Dubovitskaya, and G. Neven. Oblivious transfer with access control. In E. Al-Shaer, S. Jha, and A. D. Keromytis, editors, Proceedings of the 2009 ACM Conference on Computer and Communications Security, CCS 2009, Chicago, Illinois, USA, November 9-13, 2009, pages 131–140. ACM, 2009.
- [11] J. Camenisch and A. Lysyanskaya. A signature scheme with efficient protocols. In S. Cimato, C. Galdi, and G. Persiano, editors, Security in Communication Networks, Third International Conference, SCN 2002, Amalfi, Italy, September 11-13, 2002. Revised Papers, volume 2576 of Lecture Notes in Computer Science, pages 268–289. Springer, 2002.
- [12] J. Camenisch and A. Lysyanskaya. Signature Schemes and Anonymous Credentials from Bilinear Maps. In Franklin [19], pages 56–72.
- [13] Y. Chen, Z. L. Jiang, S. Yiu, J. K. Liu, M. H. Au, and X. Wang. Fully secure ciphertext-policy attribute based encryption with security mediator. In ICICS '14, volume 8958 of Lecture Notes in Computer Science, pages 274–289. Springer, 2014.
- [14] S. S. M. Chow, C. Boyd, and J. M. G. Nieto. Security-mediated certificate less cryptography. In Public Key Cryptography, volume 3958 of Lecture Notes in Computer Science, pages 508–524. Springer, 2006.
- [15] C. Chu, W. T. Zhu, J. Han, J. K. Liu, J. Xu, and J. Zhou. Security concerns in popular cloud storage services. IEEE Pervasive Computing, 12(4):50–57, 2013.
- [16] R. Cramer, I. Damgård, and P. D. MacKenzie. Efficient zero knowledge proofs of knowledge without intractability assumptions. In H. Imai and Y. Zheng, editors, Public Key Cryptography, volume 1751 of Lecture Notes in Computer Science, pages 354–373. Springer, 2000.
- [17] Y. Dodis, J. Katz, S. Xu, and M. Yung. Key-insulated public key cryptosystems. In EUROCRYPT, volume 2332 of Lecture Notes in Computer Science, pages 65–82. Springer, 2002.
- [18] Y. Dodis and A. Yampolskiy. A verifiable random function with short proofs and keys. In S. Vaudenay, editor, Public Key Cryptography, volume 3386 of Lecture Notes in Computer Science, pages 416–431. Springer, 2005.