Asia-pacific Journal of Convergent Research Interchange
Vol.2, No.2, June 30 (2016), pp. 43-50
http://dx.doi.org/10.21742/apjcri.2016.06.06

Enhanced Filter based access control for web based cloud

A. Narendra Babu[1)]

Abstract

In this paper, we present a new fine-grained two-factor authentication (2FA) get to control system for electronic distributed computing administrations. In particular, in our proposed 2FA get to control framework, a property based get to control component is executed with the need of both a client mystery key and a lightweight security gadget. As a client can't get to the system on the off chance that they don't hold both, the component can upgrade the security of the system, particularly in those situations where numerous clients have a similar PC for online cloud administrations. What's more, characteristic based control in the system additionally empowers the cloud server to limit the entrance to those clients with a similar arrangement of traits while safeguarding client protection, i.e., the cloud server just realizes that the client satisfies the required predicate, yet has no clue on the exact identity of the client. At last, we additionally do a reenactment to show the practicability of our proposed 2FA system.

Keywords : Fine-grained, two-factor, access control, Web services.

1. Introduction

CLOUD computing is a virtual host computer system that empowers ventures to purchase, rent, offer, or distribute software and other digital resources over the web as an ondemand benefit. It no longer relies on upon a server or various machines that physically exist, as it is a virtual framework. There are many applications of cloud computing, for example, information sharing[1-4], information stockpiling [5-8] medical information administration[9-11], therapeutic data framework[12-15] and so forth. End clients get to cloud-based applications through a web program, thin customer or versatile application while the business programming and client's information are put away on servers at a remote area. The advantages of web-based cloud computing administrations are tremendous, which incorporate the simplicity of availability, decreased expenses and capital uses, expanded operational efficiencies, versatility, adaptability

Received(April 14, 2016), Review Result(1st: April 29, 2016, 2nd: May 30, 2016), Accepted(June 10, 2016)

[1](Corresponding Author) Department of Computer Science and Engineering, KL University, Vaddeswaram, Guntur Dist., A.P., India. 522502
email: Aannam.psp@gmail.com

and quick time to showcase[16-19].

Despite the fact that the new worldview of distributed computing gives awesome focal points, there are then additionally worries about security and protection particularly for web-based cloud administrations. As touchy information might be put away in the cloud for sharing reason or helpful get to; and qualified clients may likewise get to the cloud system for different applications and administrations, client confirmation has turned into a basic part for any cloud system[20]. A client is required to login before utilizing the cloud benefits or getting to the touchy information put away in the cloud[21-25]. There are two issues for the conventional account/password-based framework. To begin with, the conventional record/secret key based confirmation is not protection saving. Notwithstanding, it is very much recognized that protection is a fundamental component that must be considered in cloud computing systems[26-29]. Second, it is basic to share a PC among various individuals. It perhaps simple for programmers to introduce some spyware to take in the login secret word from the web-program. An as of late proposed get to control demonstrate called characteristic based get to control is a decent possibility to handle the primary issue. It gives mysterious validation as well as further characterizes get to control strategies in light of various properties of the requester, environment, or the information question. In a quality based get to control system,1 every client has a client mystery key issued by the expert. Practically speaking, the client mystery key is put away inside the PC. When we consider the previously mentioned second issue on electronic administrations, it is basic that PCs might be shared by numerous clients particularly in some huge undertakings or associations.

2. Proposed System

2.1 Related Work

We review some related works including attribute-basedcryptosystems and access control with security device in this section.

2.1.1 Attribute-Based Cryptosystem

Attribute-based encryption (ABE) [20] is the foundation of attribute-based cryptosystem. ABE empowers fine-grained get to control over scrambled information utilizing access arrangements and partners traits with private keys and ciphertexts. Inside this unique circumstance, ciphertext-policy ABE (CP-ABE) [6] permits an adaptable method for information encryption to such an extent that the encryptor characterizes the get to arrangement that the decryptor (and his/her qualities set) needs to fulfill to decode the ciphertext. In this manner, diverse clients are permitted to decode distinctive bits of information concerning the pre-characterized strategy. This can wipe out the trust on the capacity server to forestall unapproved information get to.

Other than dealing with authenticated access on encrypted information in cloud storage service[13-18], ABE can likewise be utilized for get to control to distributed computing administration, correspondingly as an encryption plan can be utilized for verification reason: The cloud server may encode an irregular message utilizing the get to strategy and request that the client unscramble. On the off chance that the client can effectively unscramble the ciphertext (which implies the client's characteristics set fulfills the endorsed strategy), then it is permitted to get to the distributed computing administration.

2.1.2 Access Control With Security Device

1) Security Mediated Cryptosystem: Mediated cryptography was initially presented in [8] as a technique to permit quick repudiation of open keys. The fundamental thought of interceded cryptography is to utilize an on-line go between for each exchange. This on-line arbiter is alluded to a SEM (SEcurity Mediator) since it gives a control of security capacities. On the off chance that the SEM does not participate then no exchanges with the general population key are conceivable any more. Recently, an attribute-based version of SEM was proposed in [13].

The notion of SEM cryptography was further changed as security intervenedcertificateless (SMC) cryptography [14]. In a SMC framework, a client has a mystery key, open key and a personality. In the marking or decoding calculation, it requires the mystery key and the SEM together. In the mark confirmation or encryption algorithm, it requires the client open key and the comparing character. Since the SEM is controlled by an expert which is utilized to handle client renouncement, the specialist declines to give any collaboration to any denied client. In this manner denied clients can't produce signature or decode ciphertext. Take note of that SMC is not quite the same as our idea. The primary motivation behind SMC is to take care of the disavowal issue. In this way the SME is controlled by the expert. As such, the specialist should be online for each mark marking and ciphertext unscrambling. The client is not unknown in SMC. While in our system, the security device is controlled by the client. Namelessness is likewise saved.

2) Key-Insulated Cryptosystem: The paradigm of keyinsulated cryptography was presented in [17]. The general thought of key-protected security was to store long haul enters in a physically-secure however computationally-restricted gadget. Transient mystery keys are kept by clients on an intense yet shaky gadget where cryptographic computations happen. Transient privileged insights are then revived at discrete eras by means of collaboration between the client and the base while people in general key stays unaltered all through the lifetime of the framework. Toward the start of every day and age, the client acquires an incomplete mystery key from the gadget. By consolidating this fractional mystery key with the mystery key for the past period, the client recharges the mystery key for the present day and age.

Different from our concept, key-insulated cryptosystem requires all clients to overhaul their keys in each era. The key redesign handle requires the security gadget. Once the key has been upgraded, the marking or unscrambling calculation does not require the gadget any longer inside a similar era. While our idea requires the security device each time the client tries to get to the system. Moreover, there is no key updating required in our system.

2.2. Existing System

Though the new paradigm of cloud computing gives incredible advantages, there are in the interim likewise concerns about security and protection particularly for web-based cloud administrations. As touchy information might be put away in the cloud for sharing reason or helpful get to; and qualified clients may likewise get to the cloud system for different applications and administrations, client authentication has turned into a basic segment for any cloud system. A client is required to login before utilizing the cloud benefits or getting to the delicate information put away in the cloud. There are two issues for the conventional account/password based system.

2.2.1 Disadvantage of Existing 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.

In existing, Even though the computer may be locked by a password, it can still be possibly

http://dx.doi.org/10.21742/apjcri.2016.06.06

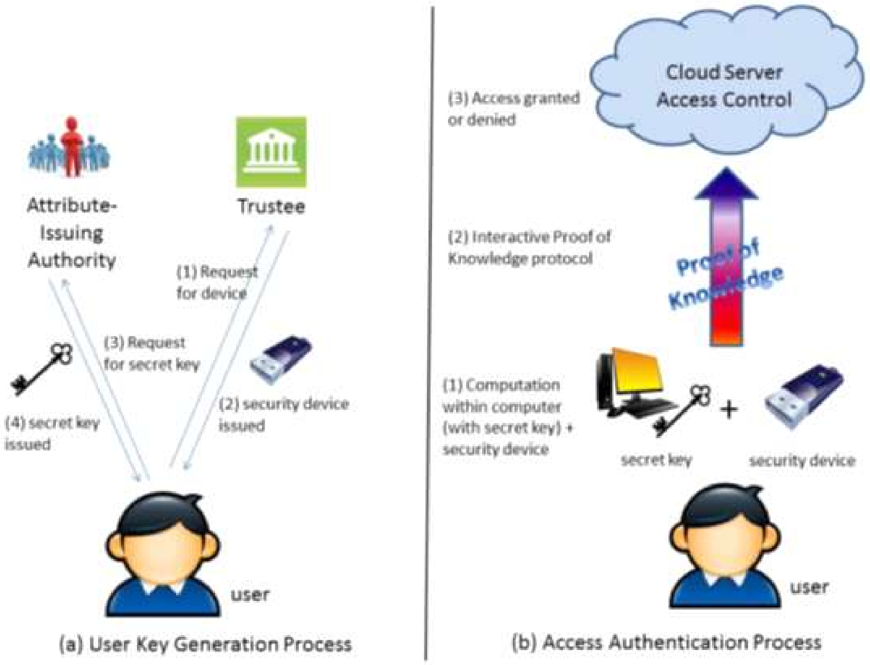
guessed or stolen by undetected malwares.

2.3 Proposed System

In this paper, we propose a fine-grained two-figure get to control convention for web-based cloud computing administrations, utilizing a lightweight security device. The device has the accompanying properties: (1) it can compute some lightweight algorithms, e.g. hashing and exponentiation; and (2) it is tamper resistant, i.e., it is accepted that nobody can break into it to get the mystery data stored inside.

2.3.1 Advantages of Proposed System

Our protocol provides a 2FA security. 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 also preserved.


Attribute-Issuing Authority
Trustee
(1) Request for device
(3) Request for secret key
(2) security device issued
(4) secret key issued
user
(a) User Key Generation Process
Cloud Server Access Control
(3) Access granted or denied
(2) Interactive Proof of Knowledge protocol
Proof of Knowledge
(1) Computation within computer (with secret key) + security device
+
secret key
security device
user
(b) Access Authentication Process

[Fig 1] System Architecture

2.4 Modules

In this implementation we have 4 Modules,

1. Trustee Module
2. Attribute-Issuing Authority Module
3. User Module
4. Cloud Service Provider Module

2.4.1 Module Description

Trustee: It is responsible for generating all system parameters and initializes the security device.

Attribute-issuing Authority: It is responsible to generate user secret key for each user according to their attributes.

User: It is the player that makes authentication with the cloud server. Each user has a secret key issued by the attribute-issuing authority and a security device initialized by the trustee.

Cloud Service Provider: It provides services to anonymous authorized users. It interacts with the user during the authentication process.

3. Conclusion

In this paper, we have introduced a new 2FA (including both user secret key and a lightweight security device) get to control system for web-based cloud computing administrations. In light of the quality based get to control instrument, the proposed 2FA get to control system has been distinguished to not just empower the cloud server to limit the entrance to those clients with a similar arrangement of properties additionally protect client security. Point by point security investigation demonstrates that the proposed 2FA get to control system accomplishes the craved security necessities. Through performance assessment, we showed that the development is "feasible". We leave as future work to additionally enhance the proficiency while keeping all nice features of the system.

References

[1] M. H. Au and A. Kapadia, PERM: Practical reputation-based blacklisting without TTPS, Proc. ACM Conf.

Comput. Commun.Secur. (CCS), **(2012)**, Oct pp.929-940; Raleigh, NC, USA

[2] M. H. Au, A. Kapadia and W. Susilo, BLACR: TTP-free blacklistable anonymous credentials with reputation in Proc. 19th NDSS, **(2012)**, pp.1-17.

[3] M. H. Au, W. Susilo and Y. Mu, Constant-size dynamic k-TAA, 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., **(2015)**, Vol.3, No. 2, pp.233-244.

[5] M. Bellare and O. Goldreich, On defining proofs of knowledge, Proc. 12th Annu. Int. CRYPTO, **(1992)**, pp.390-420.

[6] J. Bethencourt, A. Sahai and B. Waters, Ciphertext-policy attribute based encryption, Proc. IEEE Symp.Secur. Privacy, **(2007)**, May, 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., **(2004)**, Vol.4, No.1, pp.60-82.

[9] J. Camenisch, Group signature schemes and payment systems based on the discrete logarithm problem, Ph.D. dissertation, ETH Zurich, **(1998)**, Zürich, Switzerland,

[10] J. Camenisch, M. Dubovitskaya and G. Neven, Oblivious transfer with access control, Proc. 16th ACM Conf. Comput.Commun.Secur. (CCS), **(2009)**, Nov., pp.131-140; Chicago, IL, USA

[11] J. Camenisch and A. Lysyanskaya, A signature scheme with efficient protocols, Proc. 3rd Int. Conf. Secur.Commun.Netw. (SCN), **(2002)**, Sept., pp.268-289; Amalfi, Italy

[12] J. Camenisch and A. Lysyanskaya, Signature schemes and anonymous credentials from bilinear maps in Advances in Cryptology, Springer-Verlag, **(2004)**, pp.56-72; Berlin, Germany

[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, Proc. ICICS, **(2014)**, pp.274-289.

[14] S. S. M. Chow, C. Boyd and J. M. G. Nieto, Security-mediated certificateless cryptography, Public Key Cryptography (Lecture Notesin Computer Science), **(2006)**, Vol.3958, Springer-Verlag, pp.508-524; Berlin, Germany

[15] C. K. Chu, W. T .Zhu, J. Han, J. K. Liu, J. Xu and J. Zhou, Securityconcerns in popular cloud storage services IEEE Pervasive Comput., **(2013)**, Vol.12, No.4, pp.50-57.

[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), **(2000)**, Vol.1751, H. Imai and Y. Zheng, Eds., Springer-Verlag, pp.354-373; Berlin, Germany.

[17] Y. Dodis, J. Katz, S. Xu and M. Yung, Key-insulated public keycrypto systems 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 Notesin Computer Science), **(2005)**, Vol.3386, S. Vaudenay, Ed, Springer-Verlag,

pp.416-431; Berlin, Germany

[19] V. Goyal, O. Pandey, A. Sahai and B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, Proc. 13th ACM Conf. Comput. Commun. Secur., **(2006)**, pp.89-98.

[20] J. Han, W. Susilo, Y. Mu and J. Yan, Privacy-preserving decentralized key-policy attribute-based encryption IEEE Trans. Parallel Distrib. Syst., **(2012)**, Vol.23, No.11, pp.2150-2162.

[21] X. Huang, J. K. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu and J. Zhou, Cost-effective authentic and anonymous data sharing with forward security, IEEE Trans. Comput., **(2015)**, Vol.64, No.4, pp.971-983.

[22] J. Hur, Attribute-based secure data sharing with hidden policies, smartgrid IEEE Trans. Parallel Distrib. Syst., **(2013)**, Vol.24, No.11, pp.2171-2180.

[23] J. Hur, Improving security and efficiency in attribute-based data sharing, IEEE Trans. Knowl. Data Eng., **(2013)**, Vol.25, No.10, pp.2271-2282.

[24] T. Jiang, X. Chen, J. Li, D. S. Wong, J. Ma and J. Liu, TIMER: Secureand reliable cloud storage against data re-outsourcing, Proc. 10th Int. Conf. ISPEC, **(2014)**, pp.346-358.

[25] A. Juels, D. Catalano and M. Jakobsson, Coercion-resistant electronic elections, Proc. WPES, **(2005)**, pp. 61-70.

[26] J. Lai, R. H. Deng, C. Guan and J. Weng, Attribute-based encryption with verifiable outsourced decryption, IEEE Trans. Inf. ForensicsSecurity, **(2013)**, Vol.8, No.8, pp.1343-1354.

[27] M. Li, X. Huang, J. K. Liu and L. Xu, GO-ABE: Group oriented attribute-based encryption, Proc. 8th Int. Conf. NSS, **(2014)**, pp.260-270.

[28] M. Li, S. Yu, Y. Zheng, K. Ren and W. Lou, Scalable and secure sharing of personal health records in cloud computing using attribute based encryption, IEEE Trans. Parallel Distrib. Syst., **(2013)**, Vol.24, No.1, pp.131-143.

[29] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, T. V. X. Phuong and Q. Xie, A DFA-Based Functional Proxy Re-Encryption Scheme for Secure Public Cloud Data Sharing, IEEE Trans. Inf. Forensics Security, **(2014)**, Vol.9, No.10, pp.1667-1680.