Control of Two Accessories Concentrated For Administrations Based on the Web of Computing in the Cloud

Valavoju Mounika
Department of Computer Science, AVN Institute of Engineering & Technology, Ranga Reddy, Telangana, India.

V. Sridhar Reddy
Associate Professor, Department of CSE, AVN Institute of Engineering & Technology, Ranga Reddy, Telangana, India.

Dr. Shaik Abdul Nabi
Professor, Head of CSE Department, AVN Institute of Engineering & Technology, Ranga Reddy, Telangana, India.

Abstract – In this paper, we present another fine-grained two-factor verification (2FA) get to control framework for electronic distributed computing administrations. In particular, in our proposed 2FA access control framework, a characteristic based access control instrument is actualized with the need of both a client mystery key and a lightweight security. As a client can't get to the framework on the off chance that they don't hold both, the instrument can improve the security of the framework, particularly in those situations where numerous clients share a similar record for electronic cloud administrations. Moreover, characteristic based control in the framework additionally empowers the cloud server to limit the entrance to those clients with a similar arrangement of properties while protecting client security, i.e., the cloud server just realizes that the client satisfies the required predicate, yet has no clue on the correct personality of the client. At long last, we additionally do a reenactment to exhibit the practicability of our proposed 2FA framework.

Index Terms – Fine-grained, Two-Factor, Access Control, Web Services.

1. INTRODUCTION

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 [2],[3],[4] at a remote area. The benefits of electronic distributed computing administrations are immense, which incorporate the simplicity of openness, diminished expenses and capital consumptions, expanded operational efficiencies, versatility, flexibility and prompt time to advertise.

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 customary record/password [3],[5],[6],[8] based framework. Initially, the customary record password based [6],[8] verification isn't security safeguarding. In any case, it is well recognize that protection is a fundamental element that must be considered in distributed computing frameworks. Second, it is normal to share a PC among various individuals [8],[9],[10]. It possibly simple for programmers to introduce some spyware to take in the login watchword from the web-program.

The cloud server may encode an arbitrary message utilizing the entrance arrangement and request that the client unscrambles. On the off chance that the client can effectively decode the figure content (which implies the client's characteristics set fulfills the endorsed approach), [2],[3],[6],[8] at that point it is permitted to get to the distributed computing administration. Notwithstanding ABE, another cryptographic primitive in characteristic based cryptosystem is property based mark (ABS). An ABS conspire empowers a client to sign a message with fine-grained control over recognizing data. In particular, in an ABS plot, clients get their property private keys from a quality expert. At that point they can later sign messages [13],[15],[16],[17] for any predicate fulfilled by their traits. A verifier will be persuaded of the way that the endorser's qualities fulfill the marking predicate if the mark is legitimate. In the meantime, the character of endorser stays covered up. In this way it can accomplish mysterious trait based access control effectively. As of late, Yuen et al. proposed a characteristic based access control system, which can be viewed as the intuitive type of ABS.

2. RELATED WORK

Attribute-Based Cryptosystem Attribute-based encryption (ABE) is the cornerstone of attribute-based cryptosystem. ABE enables finegrained access control over encrypted [15],[20],[21] data using access policies and associates attributes with private keys and ciphertexts. 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 unauthorised [7],[8] 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 [8],[9]. 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 ciphertext (which means the user's attributes set satisfies the prescribed policy), [12],[13],[14] then it is allowed to access the cloud computing service.

Access Control with Security Device Security Mediated Cryptosystem Mediated cryptography was first introduced [6],[8] 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. Recently, an attribute-based version of SEM was proposed [3],[5],[6],[8]. Thus revoked users cannot generate signature or decrypt ciphertext. The main purpose of SMC is to solve the revocation problem. Thus the SME is controlled by the authority. In other words, the authority needs to be online for every signature signing and ciphertext decryption. The user is not anonymous in SMC. While in our system, the security device is controlled by the user.

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 [13],[14],[18] where cryptographic computations take place. 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 our concept, key-insulated cryptosystem [21],[22] 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 [23],[25] does not require the device any more with in the same time period. While our concept does require the security device every time the user tries to access the system. Furthermore, there is no key updating required in our system.

3. SYSTEM DESIGN

We specifically design our system in another manner. We do not split the secret key into two parts. Instead, we introduce some additional unique information stored in the security [9],[10],[11] device. The authentication [20] process requires this piece of information together with the user secret key. It is guaranteed that missing either part cannot let the authentication pass. There is also a linking relationship between the user's device and the secret key so that the user cannot use another [23] user's device for the authentication. The communication overhead is minimal and the computation required in the device is just some lightweight algorithms[25]. All the heavy computations such as pairing are done on the computer.

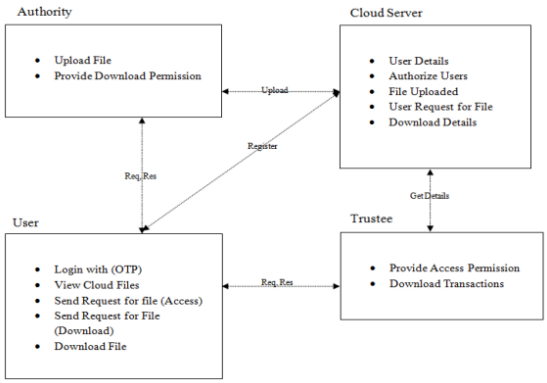

Fig. 1: Architecture Diagram

A naive thought to achieve our goal is to use a normal ABS and simply divide the secret key of the user into two parts. The user saves a part (stored in the computer) while another part is initialized in the security device. Particular attention should be paid to the process since normal ABS does not guarantee that the loss of a secret key portion does not affect the schema security, while in two 2FAs, the author of the attack[13],[14],[16],[18], [1],[20],[21] may have been compromised by one of the factors. In addition, the division must be performed so that most of the computing load must be with the user's computer, as it is assumed that the security device is not powerful [23],[25]. Specifically, we design our system in another way. We do not divide the secret key into two parts. Instead, we present unique [1],[5],[9] additional information stored in the security device. The authentication process requires this information along with the user's secret key. It is guaranteed that no missing part can pass authentication. There is also a link between the user device and the secret key [16],[17]so that the user can not use another user's device for authentication.

THREAT MODEL

In this paper, we consider the following threats:

1) Authentication: The adversary tries to access the system beyond its privileges. For example, a user with attributes {Student,Physics} may try to access the system with policy "Staff" AND "Physics". To do so, he may collude with other users.

2) Access without Security Device: The adversary tries to access the system (within its privileges) without the security device, or using another security device belonging to others.

3) Access without Secret Key: The adversary tries to access the system (within its privileges) without any secret key. It can have its own security device.

4) Privacy: The adversary acts as the role of the cloud server and tries to find out the identity of the user it is interacting with.

4. PROSPECTIVE IMPROVEMENT

- An unequivocal security [23],[25],[26] examination demonstrates that the 2FA access control structure has finished the required security basics. Through the execution assessment we have demonstrated that change is "doable".
- We leave as future work to moreover enhance practicality while [25] keeping up all the immaculate highlights of the structure**.**
- We leave as future work to furthermore improve viability while keeping up all the flawless features of the structure.

5. CONCLUSION

In this paper, we displayed another 2FA access control structure (which merges both a confound key client and a lightweight security gadget) for electronic spread figuring associations. In light of the property based access control fragment, the 2FA access control framework has been organized to permit not just the cloud server to compel access to those clients with a tantamount trademark set, yet also to save client confirmation.

REFERENCES

[1] M. H. Au and A. Kapadia, "PERM: Down to earth reputation based boycotting without TTPS," in Proc. ACM Conf. Comput. Commun. Secur. (CCS), Raleigh, NC, USA, Oct. 2012, pp. 929– 940.
[2] M. H. Au, A. Kapadia, and W. Susilo, "BLACR: without ttp blacklistable baffling capabilities with reputation," in Proc. nineteenth NDSS, 2012, pp. 1– 17.
[3] M. H. Au, W. Susilo, and Y. Mu, "Reliable size dynamic k-TAA," in Proc. fifth Int. Conf. SCN, 2006, pp. 111– 125.
[4] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang, "An ensured conveyed registering based framework for colossal data information organization of splendid system," IEEE Trans. Cloud Comput., vol. 3, no. 2, pp. 233– 244, Apr./Jun. 2015.
[5] M. Bellare and O. Goldreich, "On describing confirmations of data," in Proc. twelfth Annu. Int. CRYPTO, 1992, pp. 390– 420.
[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-plan attributebased encryption," in Proc. IEEE Symp. Secur. Insurance, May 2007, pp. 321–334.
[7] D. Boneh, X. Boyen, and H. Shacham, "Short assembling marks," 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 limits," ACM Trans. Web Technol., vol. 4, no. 1, pp. 60– 82, 2004.
[9] J. Camenisch, "Social occasion check designs and portion systems in perspective of the discrete logarithm issue," Ph.D. piece, ETH Zurich, Zürich, Switzerland, 1998.
[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th ACM Conf. Comput. Commun. Secur., 2006, pp. 89–98.
[11] J. Han, W. Susilo, Y. Mu, and J. Yan, "Privacy-preserving decentralized key-policy attribute-based encryption," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 11, pp. 2150–2162, Nov. 2012.
[12] X. Huang et al., "Cost-effective authentic and anonymous data sharing with forward security," IEEE Trans. Comput., vol. 64, no. 4, pp. 971–983, Apr. 2015.
[13] J. Hur, "Attribute-based secure data sharing with hidden policies in smart grid," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 11, pp. 2171–2180, Nov. 2013.
[14] J. Hur, "Improving security and efficiency in attribute-based data sharing," IEEE Trans. Knowl. Data Eng., vol. 25, no. 10, pp. 2271–2282, Oct. 2013.
[15] T. Jiang, X. Chen, J. Li, D. S. Wong, J. Ma, and J. Liu, "TIMER: Secure and reliable cloud storage against data re-outsourcing," in Proc. 10th Int. Conf. ISPEC, 2014, pp. 346–358.
[16] A. Juels, D. Catalano, and M. Jakobsson, "Coercion-resistant electronic elections," in Proc. WPES, 2005, pp. 61–70.
[17] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 1343–1354, Aug. 2013.
[18] M. Li, X. Huang, J. K. Liu, and L. Xu, "GO-ABE: Grouporiented attribute-based encryption," in Proc. 8th Int. Conf. NSS, 2014, pp. 260–270.
[19] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attributebased encryption," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013.
[20] K. Liang et al., "A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing," IEEE Trans. Inf. Forensics Security, vol. 9, no. 10, pp. 1667–1680, Oct. 2014.
[21] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloud-based revocable identity-based proxy re-encryption scheme for public clouds data sharing," in Proc. 19th ESORICS, 2014, pp. 257–272.
[22] K. Liang, W. Susilo, and J. K. Liu, "Privacy-preserving ciphertext multisharing control for big data storage," IEEE Trans. Inf. Forensics Security, vol. 10, no. 8, pp. 1578–1589, Aug. 2015.
[23] J. K. Liu, M. H. Au, W. Susilo, K. Liang, R. Lu, and B. Srinivasan, "Secure sharing and searching for real-time video data in mobile cloud," IEEE Netw., vol. 29, no. 2, pp. 46–50, Mar./Apr. 2015.
[24] J. K. Liu, M. H. Au, W. Susilo, and J. Zhou, "Enhancing location privacy for electric vehicles (at the right time)," in Proc. 17th Eur. Symp. Res. Comput. Secur., Pisa, Italy, Sep. 2012, pp. 397–414.
[25] H. K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures," in Topics in Cryptology, vol. 6558. Berlin, Germany: Springer-Verlag, 2011, pp. 376–392.
[26] M. Nabeel, N. Shang, and E. Bertino, "Privacy preserving policy-based content sharing in public clouds," IEEE Trans. Knowl. Data Eng., vol. 25, no. 11, pp. 2602–2614, Nov. 2013.

Authors

Valavoju Mounika, B.tech, is currently pursuing M.tech in the stream of Computer Science and Engineering, in AVN Institute Of Engineering & Technology, Ibrahimpatnam, Hyderabad, Telangana state, India. She has attended workshops on CLOUD COMPUTING in association with Scient Institute Of Engineering And Technology. Ibrahimpatnam, Hyderabad. Organized the event SAMVIGYAN 2K-13 in Scient Institute Of Engineering And Technology. Her areas of interest are oops, java, oracle and cloud computing.

V.Sridhar Reddy, B.Tech, M.Tech is having 12+ years of relevant work experience in Academics and Teaching. At present, he is working as Associate Professor in CSE department, AVN Institute of Engineering & Technology, Ibrahimpatnam, Hyderabad, TS, India.

He has attended workshops and International conferences on NS-3, Big data. His areas of interest are Big data, Computer Graphics, Software Engineering and Cloud computing.

Dr. ShaikAbdul Nabi is working as professor &Head of the Dept. of CSE, & vice principal in AVN Inst. Of Engg. & Tech, Hyderabad, T.S, India. He completed his B.E (Computer Science & engineering) from Osmania University, Hyderabad. He has completed his M.Tech. from JNTU Hyderabad campus and he received Doctor of Philosophy (Ph.D) in the area of Web Mining from Acharya Nagarjuna University, Guntur, AP, India. He is a certified professional by Microsoft.

He is having 17 years of Teaching Experience in various Engineering Colleges. He has published 18 publications in International / National Journals and presented 10 papers in National / International conferences. His expertise areas are Data warehousing and Data Mining, Data Structures & UNIX Networking Programming, Cloud Computing and Mobile Computing.