International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 07 | July -2017 www.irjet.net p-ISSN: 2395-0072

Fine Grained Two Factor Access Control Using Secured Device for Web Based Cloud Computing

Sameer[1], Naveen Kumar B[2]

[1] PG Student, University BDT college of Engineering, Visveswaraya Technological University, Hadadi Road, Davangere, Karnataka, India
[2]Assistant Professor Dept CS &E, University BDT college of Engineering, Hadadi Road, Davangere, Karnataka,India

---

Abstract - we present another fine-grained two-factor verification (2FA) get to control framework for electronic distributed computing administrations. In particular, in our proposed 2FA get to control framework, a quality based get to control component is actualized with the need of both a client mystery key and a lightweight security gadget. As a client can't get to the framework on the off chance that they don't hold both, the component can upgrade the security of the framework, particularly in those situations where numerous clients share a similar PC for online cloud administrations. What's more, property based control in the framework likewise empowers the cloud server to limit the entrance to those clients with a similar arrangement of properties while saving 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 show the practicability of our proposed 2FA framework.

Key Words: Two Factor Access Control(2FA)

1. INTRODUCTION

Dispersed processing is a virtual host PC structure that enables dares to buy, lease, offer, or pass on programming and other automated resources over the web as an on-ask for advantage. It never again depends on upon a server or different machines that physically exist, as it is a virtual structure. There are various uses of disseminated registering, for instance, data sharing data stockpiling colossal data organization, therapeutic information structure et cetera. End customers get the chance to cloud-based applications through a web program, thin client or adaptable application while the business programming and customer's data are secured on servers at a remote range. The upsides of online circulated processing organizations are enormous, which fuse the straightforwardness of receptiveness, diminished costs and capital utilizations, extended operational efficiencies, versatility, flexibility and provoke time to grandstand.

Notwithstanding the way that the new perspective of appropriated processing gives mind boggling inclinations, there are meanwhile also stresses over security and insurance especially for online cloud organizations. As sensitive data may be secured in the cloud for sharing reason or accommodating get to and qualified customers may in like manner get to the cloud system for various applications and organizations, customer approval has transformed into an essential portion for any cloud structure. A customer is required to login before using the cloud benefits or getting to the fragile data set away in the cloud. There are two issues for the standard record/mystery word based system. In any case, the standard record/mystery key based check is not security ensuring.

2. Literature Survey

[4] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang. A protected distributed computing based system for enormous information data administration of keen matrix. IEEE T. distributed computing, 3(2):233–244, 2015.

Sharp systems are persistently supplanting traditional power networks in view of extended viability, trustworthiness, economy, and criticalness of energy organizations. Taking after the achievement of ENEL Telegestore which yielded a yearly venture assets of 500 million Euros, other sharp cross section exercises, for instance, Hydro One expect in Canada, the Evora InovGrid stretch out in Portugal, and the Modellstadt Mannheim (Moma) reach out in Germany have run with a similar example. Due to prerequisites in getting colossal measure of information from a far reaching number of front-end sharp devices, clever cross sections couldn't be passed on at a tremendous scale (e.g., in the whole country). To refer to a case, the measure of data required to handle trades of two million customers at a particular utility accomplished 22 gigabytes for consistently. In this way, the assurance, plan, checking and examination of such gigantic sharp system data is not a straightforward errand. Further, steady information get ready is regularly required in the canny grid. Any deferral may realize a veritable result in the whole structure. To stroll over these difficulties, conveyed figuring has been used in light of its flexibility, adaptability, deftness, imperativeness capability, and cost saving properties.

[6] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-arrangement trait based encryption. In IEEE Symposium on Security and Privacy, pages 321–334. IEEE Computer Society, 2007.

Generally speaking, when a customer scrambles delicate data, it is essential that she set up a specific get the chance to control technique on who can unscramble this data. For example, accept that the FBI open degradation of-fices in Knoxville and San Francisco are analyzing a confirmation of pay off including a San Francisco lobbyist and a Tennessee congressman. The head FBI authority may need to encode a sensitive update with the goal that solitary work constrain that have certain capabilities or at-tributes can get to it. For instance, the head expert may demonstrate the going with get to structure for getting to this information: (("Public Corruption Office" AND ("Knoxville" OR "San Francisco")) OR (organization level > 5) OR "Name: Charlie Eppes").

By this, the head master could suggest that the refresh should simply be seen by administrators who work at general society pollution work environments at Knoxville or San Francisco, FBI specialists high up in the organization chain, and a specialist named Charlie Eppes.

As appeared by this case, it can be important that the individual having the puzzle data have the ability to pick a get to plan in light of specific learning of the major data. In addition, this individual may not know the right identities of every single other person who should have the ability to get to the data, yet rather she may simply have a way to deal with depict them in regards to unmistakable qualities or affirmations.

3 System Design

It can be portrayed as a move from customer's point of view to programming designers or database person's viewpoint. The arrangement organize goes about as an expansion between the required specific and the execution arrange.

The setup arrange incorporates two phases specifically:

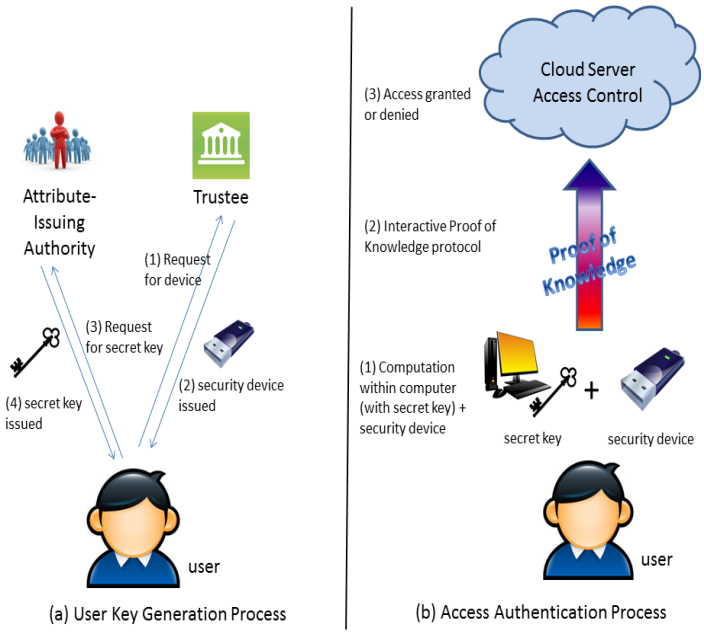
- Top - Level Design

Top Level Design

The inspiration driving this stage is to orchestrate a response for the issue dictated by the need record. This stage basically moves from issue space to the plan space. The setup of the structure is the most essential variable impacting the way of the item. Here we amass the Block Diagram that will be valuable to grasp the lead of the system.

3.1 Detailed Design

The engineering is one of the portrayal of the hypothetical framework that characterizes the structure, conduct alongside more details about the framework. It shows the principal association of the framework that portrays different parts in it and their association with each other.



Our system consists of the following entities:
- Trustee: It is responsible for generating all system parameters and initialized 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.

4 Existing Framework

Only user name and password is not authenticate to provide security. Hackers can easily hack the system

Inconveniences of Existing Framework:

1. In this user provide password as his name or surname or some numbers there might be chance to get a password by hackers.

2. In cyber that is common to share computers among users by using browsing history hackers can get users confidential information.

3. In existing, Even however the PC might be bolted by a secret word, it can in any case be conceivably speculated or stolen by undetected malwares.

4.1 Propsed Framework:

Points of interest of Proposed System:

1. Our convention gives a 2FA security

2. Our convention bolsters fine-grained characteristic based get to which gives an incredible adaptability to the framework to set diverse get to arrangements as indicated by various situations. In the meantime, the protection of the client is additionally safeguarded.

5. CONCLUSION

In this project, we have presented a new 2FA (including both user secret key and a lightweight security device) access control system for web-based cloud computing services. 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, we demonstrated that the construction is feasible. Weleave as future work to further improve the efficiency while keeping all nice features of the system.

6 REFERENCES

[1] M. H. Au and A. Kapadia, "PERM: Practical reputation-based blacklisting without TTPS," in Proc. ACM Conf. Comput. Commun. Secur. (CCS), Raleigh, NC, USA, Oct. 2012, pp. 929–940. Volume: 1 Issue: 4 December 16 3

[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," 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, "Ciphertextpolicy attributebased encryption," in Proc. IEEE Symp. Secure. 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] J. Camenisch, "Group signature schemes and payment systems based on the discrete logarithm problem," Ph.D. dissertation, ETH Zurich, Zürich, Switzerland, 1998.

[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.