

Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Service

¹V. Vijay Kumar and ²R. Bala Dhankar,

¹PG Student, ²Assistant Professor,

^{1,2}Department of computer Applications, Godavari Institute of Engineering and Technology, Rajahmundry, India

Abstract-- In this paper, we have a tendency to present a Two-factor confirmation (2FA) get to framework for electronic distributed computing administrations. In particular, in our arranged 2FA access framework, quality based access administration system is upheld with the need of each a client mystery key and a light-weight security gadget. As a client can't get to the framework in the event that they are doing not hold each, the component will improve the security of the framework, especially in those outcomes wherever a few clients share a proportionate workstation for electronic cloud administrations. furthermore, quality based administration inside the framework moreover enables the cloud server to confine the entrance to those clients with an equal arrangement of traits while monitoring client security, i.e., the cloud server exclusively knows about that the client satisfies the coveted predicate, however has no arrangement on the exact personality of the client.

Keywords-- two-factor, access control, web services

I. INTRODUCTION

Cloud computing is a progressive figuring strategy, by which processing assets are given powerfully by means of Internet and the information stockpiling and calculation are outsourced to somebody or some gathering in a cloud. It extraordinarily draws in consideration and enthusiasm from both scholarly world and industry because of the benefit, however it likewise has no less than three difficulties that must be dealt with before going to our genuine to the best of our insight.

Above all else, information privacy ought to be ensured. The information security isn't just about the information substance. Since the most appealing piece of the cloud processing is the calculation outsourcing, it is a long way sufficiently past to simply direct an entrance control. More probable, clients need to control the benefits of information control over different clients or cloud servers.

This is on account of when touchy data or calculation is outsourced to the cloud servers or another client, which is out of users' control in most cases, security dangers would rise significantly in light of the fact that the servers may unlawfully assess users' information and access touchy data, or different clients may have the capacity to construe delicate data from the outsourced calculation.

In this manner, the entrance as well as the operation ought to be controlled. Also, individual data (characterized by each user's qualities set) is in danger since one's personality is confirmed in light of his data with the end goal of access control (or benefit control in this paper). As individuals are winding up more worried about their character protection these days, the character security additionally should be ensured before the cloud enters our life. Ideally, any specialist or server alone ought not know any customer's close to home data. To wrap things up, the distributed computing framework ought to be flexible on account of security break in which some piece of

the framework is bargained by assailants. They are partners to each other as in the choice of encryption arrangement (who can or can't unscramble the content). In the KP-ABE, a figure content is related with an arrangement of properties, and a private key is related with a monotonic structure like a tree, which portrays this user's personality (e.g. IIT AND (Ph.D. Or then again Master)). A client can unscramble the figure content if and just if the entrance tree in his private key is fulfilled by the characteristics in the figure content.

Be that as it may, the encryption approach is depicted in the keys, so the encoded does not have whole control over the encryption arrangement. He needs to assume that the key generators issue keys with revise structures to rectify clients. Besides, when arencryption happens, the greater part of the clients in a similar framework must have their private keys re-issued in order to access there-encoded records, and this procedure causes impressive issues in execution. Then again, those issues and overhead are altogether tackled in the CP-ABE. In the CP-ABE, figure writings are made with an entrance structure, which determines the encryption strategy, and private keys are produced by users' characteristics. A client can decode the figure content if and just if his qualities in the private key fulfill the entrance tree determined in the figure content. Thusly, the encoded holds a definitive specialist about the encryption approach. Likewise, the as of now issued private keys will never be adjusted unless the entire framework reboots.

II. RELATED WORK

In this section, the reference are collected from all conferences, sites, articles, books from the internet which helps to implement the project. For good understanding of the advanced authentication system there are some work on the IEEE international journal that have been referenced:

(a) Boyang Wang, Student Member, IEEE, Baochun Li, Senior Member, IEEE, and Hui Li, Member, IEEE has proposed a paper on "Public Auditing for Shared Data with Efficient User Revocation in the Cloud". Where it gives information of Shared data with efficient user revocation in the cloud. The cloud can improve the efficiency of user revocation. But it has disadvantage as "Network Connections Dependency. Cost is more"

(b) Cheng-Kang Chu, Sherman S.M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H Deng proposed a paper on "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage". More flexible than hierarchical key assignment which can only save spaces if all key-holders share a similar set of privileges. Allows efficient and flexible

key delegation. "Network Connections Dependency. here also has disadvantage that Cost is more and algorithm used are Key Aggregate Encryption, Decryption.

(c) Seung-Hyun Seo, Member, IEEE, Mohamed Nabeel, Member, IEEE, Xiaoyu Ding, Student Member, IEEE, and

Elisa Bertino, Fellow, IEEE" proposed a paper on "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds". Securely share sensitive data in public clouds. Improve efficiency. here also has disadvantage that Network Connections Dependency and Cost is more" algorithm used are public key encryption algorithms.

(d) Mohamed Nabeel and Elisa Bertino, Fellow, IEEE proposed a paper on "Privacy Preserving Delegated Access Control in Public Clouds". Decomposition ACPs used to privacy preserving fine-grained delegated access control to data in public clouds. The Owner has to handle a minimum number of attribute conditions while hiding the content from the cloud here also has disadvantage that "Network Connections Dependency. Cost is more" algorithm used are optimization algorithms, gen graph, random cover, policy decomposition.

(e) Kaitai Liang, Man Ho Au, Member, IEEE, Joseph K. Liu, Willy Susilo, Senior Member, IEEE, Duncan S. Wong" proposed a paper on "A DFA-Based Functional Proxy Re-Encryption Scheme for Secure Public Cloud Data Sharing". here also has disadvantage that "Network Connections Dependency. Cost is more" algorithm used are DFA-based functional proxy re-encryption.

(f) Kaiping Xue, Member, IEEE and Peilin Hong, Member, IEEE proposed a paper on "A Dynamic Secure Group Sharing Framework in Public Cloud Computing". "Dynamic secure group sharing framework in public cloud computing environment The sharing files are secured stored in cloud servers and all the session key are protected in the digital Envelopes. here also has disadvantage that "Network Connections Dependency. Cost is more" algorithm used are Proxy signature algorithm. Diffie-Hellman.

(g) Tao Jiang, Xiaofeng Chen, and Jianfeng Ma IEEE. proposed a paper on "Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation". it has Secure data integrity auditing for share dynamic data. Provide data confidentiality for group users. here also has disadvantage that "Network Connections Dependency. Cost is more" algorithm used are Randomized Key generation, RSA, SHA.

(h) Jiawei Yuan and Shucheng Yu, Member, IEEE proposed a paper on "Public Integrity Auditing for Dynamic Data Sharing With Multiuser Modification". "Efficient data user authentication protocol, which not only prevents attackers from eavesdropping secret keys and pretending to be illegal data users performing searches, but also enables data user authentication and revocation. -Systematically construct a novel secure search protocol, which not only enables the cloud server to perform secure ranked keyword search without knowing the actual data of both keywords and trapdoors, but also allows data owners to encrypt keywords with self-chosen keys and allows authenticated data users to query without knowing these keys. -Additive Order and Privacy Preserving Function family (AOPPF) which allows data owners to protect the privacy of relevance scores using different functions according to their preference, while still permitting the cloud server to rank the data files accurately. here also has disadvantage that "Network Connections Dependency. Cost is more" algorithm used are Randomize Key generation, AES 128.

III. EXISTING SYSTEM

As touchy information might be put away in the cloud for sharing reason or advantageous access; and qualified clients may likewise get to the cloud framework for different

applications and administrations, client confirmation has turned into a basic segment for any cloud framework. 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 record/secret key based existing framework. To begin with, the conventional account/secret word based confirmation isn't security safeguarding. Nonetheless, it is all around recognized that protection is an fundamental element that must be considered in distributed computing frameworks. Second, it is regular to share a PC among diverse individuals. It might be simple for programmers to introduce some spyware to take in the login secret word from the web-program. Along these lines such frameworks are not completely secured.

Disadvantages

1. The customary record/secret word based validation isn't protection safeguarding.
2. Common to share a PC among various individuals. It might be simple for programmers to introduce some spyware to take in the login watchword from the web-program.
3. Existing framework isn't completely secured.

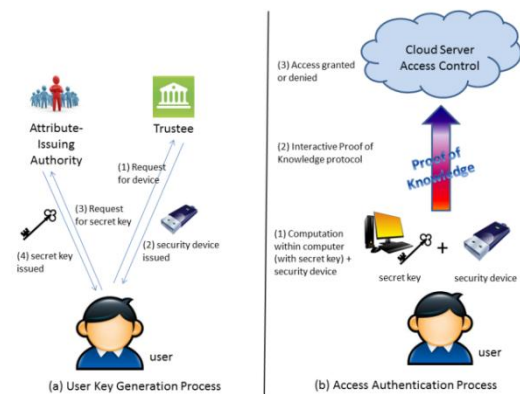


Figure 1: Overview idea of our system

IV. PROPOSED SYSTEM

In this Paper, we propose a fine-grained two factor get to control convention for electronic distributed computing administrations, utilizing a lightweight security gadget. The gadget has the accompanying properties: (1) It can figure some lightweight calculations, e.g. hashing and exponentiation and (2) it is alter safe, i.e., it is assume that nobody can break into it to get the mystery data put away inside. With this gadget, our convention gives a 2FA security. In the first place the client mystery key (which is typically put away inside the PC) is required. Furthermore, the security gadget ought to be additionally joined to the PC (e.g. through USB) with a specific end goal to validate the client for getting to the cloud. The client can be allowed get to just in the event that he has the two things. Nonetheless, the client can't utilize his mystery key with another gadget having a place with others for the entrance.

A. Advantages

1. Our Protocol underpins fine-grained quality based access which gives an awesome adaptability to the framework to set distinctive access approaches as per diverse scenarios.
2. In the meantime, the protection of the client is likewise saved.
3. The cloud framework just realizes that the client forms some required quality, yet not the genuine character of the client.

4. To demonstrate the reasonableness of our framework, we mimic the model of the convention.

V. RESULTS

This project is developed by using NET Beans 8.0.2 & JDK 1.8 with My Sql as database. The proposed system shows the performance of the security in this paper.

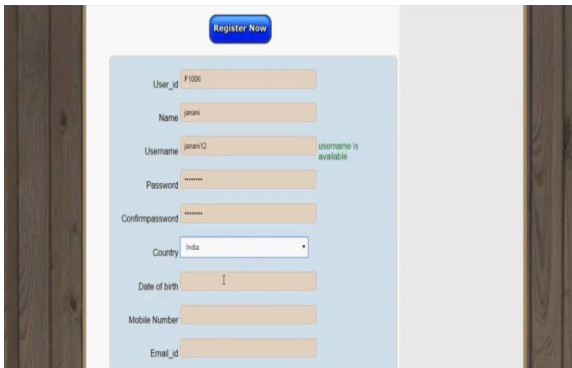


Figure 2: Show the Registration of the User.

CONCLUSION

In this paper, we've given a brand new 2FA (including both user secret key and a light-weight security device) access control system for web-based cloud computing services. Based on the attribute-based access management mechanism, the projected 2FA access system has been known to not solely enable the cloud server to limit the access to those users with an equivalent set of attributes however additionally preserve

user privacy. Detailed security analysis shows that the projected 2FA access control system achieves the required security needs. Through performance analysis, we have a tendency to incontestable that the construction is "feasible". we have a tendency to leave as future work to additional improve the potency whereas keeping all nice options of the system.

References

- [1] 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.
- [2] 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.
- [3] Joseph K. Liu, Tsz Hon Yuen, Man Ho Au, Xinyi Huang, Willy Susilo, and Jianying Zhou, "k-times attribute-based anonymous access control for cloud computing", IEEE Transactions on Computers, 64 (9), 2595-2608.
- [4] 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.
- [5] 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.