IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue-14, May 2019 E-ISSN: 2347-2693

Multi-Factor Authentication

S. Mayur[1], M. Harish[2], R.Tejesh[3], Vishal Umrao[4], Shalini Tiwari[5*]

[1,2,3,4,5]School of Computing and Information Technology, Reva University, Bangalore, India

[*]*Corresponding Author: shalinitiwari@reva.edu.in, Tel.: 9606205729*

DOI: https://doi.org/10.26438/ijcse/v7si14.509511 | Available online at: www.ijcseonline.org

Abstract- In this paper, we introduce a multi-factor authentication forverification (2FA) get to control framework for online distributed computing administrations. In particular, in our proposed 2FA access control framework, a characteristic based access 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 improve the security of the framework, particularly in those situations where numerous clients share a similar PC for electronic cloud administrations. Likewise, trait based control in the framework additionally empowers the cloud server to limit the entrance to those clients with a similar arrangement of qualities while safeguarding client protection, i.e., the cloud server just realizes that the client satisfies the required predicate, however has no clue on the accurate personality of the client.

Keywords—Cipher text, Encryption, Distributed storage structures, Security, Cloud computing, Access Control, SEM

I. INTRODUCTION

Distributed computing is a virtual host PC framework that empowers ventures to purchase, rent, sell, or convey programming and other computerized assets over the web as an on-request administration. It never again relies upon a server or a number of machines that physically exist, as it is a virtual framework. There are numerous utilizations of distributed computing, for example, information sharing information storage [1], huge information management [2] medicinal data framework and so forth. End clients get to cloud-based applications through an internet browser, slim customer or versatile application while the business programming and client's information are put away on servers at a remote area. The advantages of online distributed computing administrations are immense, which incorporate the simplicity of openness, diminished expenses and capital uses, expanded operational efficiencies, versatility, adaptability and quick time to advertise.

In spite of the fact that the new worldview of distributed computing gives incredible focal points, there are in the meantime likewise worries about Security and protection particularly for electronic cloud administrations. 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 what's more, administrations, client confirmation has turned into a basic part for any cloud framework. A client is required to login before utilizing the cloud benefits or getting to the touchy information put away in the cloud. There are two issues for the customary record/secret phrase based framework. Initially, the conventional record/secret key based confirmation isn't protection saving. Nonetheless, it is very much recognized that security is a fundamental component and that must be considered here in the distributed computing frameworks. Second, usually to share a PC among various individuals.

It might be simple for programmers to introduce some spyware to take in the login secret key from the internet browser. An as of late proposed get to control show called property based access control is a decent contender to handle the principal issue. It provides mysterious verification as well as further characterizes get to control strategies dependent on various raits of the requester, condition, or the information object. In a property based access control system1, every client has a client mystery key issued by the expert. By and by, the client mystery key is put away inside the PC.

When we consider the previously mentioned second issue on online administrations, usually PCs may be shared by numerous clients particularly in some extensive undertakings or associations. For instance, let us consider the Following two situations:

• In a medical clinic, PCs are shared by various staff. Dr. Alice utilizes the PC in room A when she is on obligation in the daytime, while Dr.Weave utilizes a similar PC in a similar room when he is on obligation around evening time.

• In a college, PCs in the undergrad lab are generally shared by various understudies. In these cases, client mystery keys could be effectively stolen or utilized by an unapproved party. Despite the fact that the PC might be bolted by a secret key, it can in any case be potentially speculated or stolen by

undetected malwares. An increasingly secure route is to utilize two-factor confirmation (2FA). 2FA is basic among online e-banking administrations. Notwithstanding a username/secret word, the client is likewise required to have a gadget to show a onetime secret phrase. A few frameworks may require the client to have a cell phone while the one-time secret phrase will be sent to the cell phone through SMS amid the login procedure. By utilizing 2FA, clients will have more certainty to utilize shared PCs to login for electronic e-banking administrations. For a similar reason, it will be smarter to have a 2FA framework for clients in the online cloud benefits so as to build the security level in the framework.

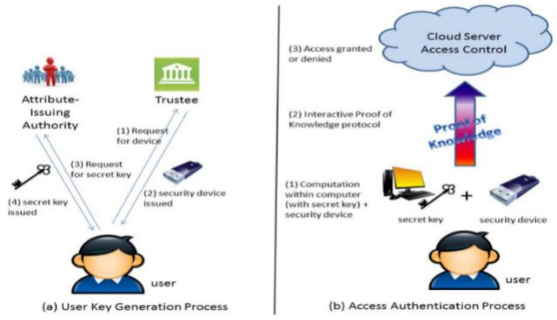
II. Related Work

The worldview of key-protected cryptography was presented in. The general thought of key-protected security was to store long haul enters in a physically-secure yet computationally-restricted gadget. Momentary mystery keys are kept by clients on a ground-breaking however unreliable gadget where cryptographic calculations happen. Transient mysteries are then revived at discrete timespans by means of communication between the client and the base while the open key stays unaltered all through the lifetime of the framework. Toward the start of each timeframe, the client acquires a halfway mystery key from the gadget. By consolidating this incomplete mystery key with the mystery key for the past period, the client re-establishes the mystery key for the present timeframe. Not quite the same as our idea, key-protected cryptosystem requires all clients to refresh their keys in each timespan. The key update process requires the security gadget. When the key has been refreshed, the marking or decoding calculation does not require the gadget anything else inside a similar time

II. Methodology

The system design focuses on mainly technical and non-technical activities. The interface is developed as part of graphic design layout of the user in created as part of interface design webapps structure are made as a part of architectural and navigation design, the main aim when the web application interface was being developed was to provide three question to end users.

a) When am I:- This represents that the interface should provide indication of where the user is currently accessed and the location of the content.
b) What can I do now:-This represents various option provided to the user. These option represents function, links and whether the content is relevant are not.
c) Where have I been:- This facilitates basic navigation between various pages and must provide map regarding where the user has been and different paths.



III. Results and Discussion

1. Figure (a) represents the home screen of fine grained two factor access control which contains all domains.
2. Figure (b) represents the interface containing both Pseudonym Key and private key.

Figure (a)

Figure (b)

IV. Conclusion and Future Scope

In this paper, 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". We leave as future work to further improve the efficiency while keeping all nice features of the system.

The future work will be focused on implementing the same model to an enterprise application where an education organisation can perform its distribution of study materials to authorised persons. And we would like to bring the application to mobile platform where it is feasible for users to access and needs are remotely also.

ACKNOWLEDGMENT

I have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals and organizations. I would like to extend my sincere thanks to all of them. I am very obligated toReva University and our mentor for their direction and consistent supervision just as for giving essential data with respect to the venture and additionally for their help in finishing the undertaking.

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 blacklist able 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

