ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

Survey on Two-Factor Based Access in Cloud Storage System

Jyotsna Barpute [1], Prof.Shubhangi Suryawanshi[2]

M. E Student, Dept. of Computer Engineering, G.H.Raisoni Institute of Engineering And Technology, Savitribai Phule Pune University, Pune, India[1]

Assistant Professor, Dept. of Computer Engineering , G.H.Raisoni Institute of Engineering And Technology, Savitribai Phule Pune University, Pune, India [2]

ABSTRACT: In this paper, we present another fine-grained two-factor verification (2FA) access control system for online cloud computing administrations. In particular, in our proposed 2FA access control system, an attribute-based access control component is executed with the need of both a client secret key and a lightweight security gadget. As a client can't access the system in the event that they don't hold both, the instrument can improve the security of the system, particularly in those situations where numerous clients have a similar PC for electronic cloud administrations. What's more, attribute-based control in the system moreover empowers the cloud server to limit the access to those clients with a similar arrangement of attributes while protecting client security, i.e., the cloud server just realizes that the client satisfies the required predicate, however has no clue on the correct character of the client. At long last, we likewise do a re-enactment to exhibit the practicability of our proposed 2FA system.

KEYWORDS: Fined-grained, Two-Factor, Cloud ,Web services.

I. INTRODUCTION

Cloud computing is a virtual host computer system that empowers undertakings to purchase, rent, offer, or appropriate programming and other advanced assets over the web as an on request benefit. It no longer relies on upon a server or a number of machines that physically exist, as it is a virtual system. There are numerous utilizations of cloud computing, for example, data sharing , information stockpiling ,enormous information administration [4], restorative data system and so on. End clients access cloud-based applications through a web program, thin customer or portable application while the business programming also, client's information are put away on servers at a remote area. The advantages of online cloud computing administrations are gigantic, which incorporate the simplicity of accessibility, diminished expenses also, capital uses, expanded operational efficiencies, adaptability, adaptability and quick time to showcase. In spite of the fact that the new worldview of cloud computing gives incredible points of interest, there are in the mean time 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 access the cloud system for different applications and administrations, client verification has turned into a basic part for any cloud system. A client is required to login before utilizing the cloud benefits or accessing the touchy information put away in the cloud. There are two issues for the customary record/password based system. To begin with, the customary record/secret word based confirmation is not security safeguarding. Notwithstanding, it is well recognized that security is a basic element that must be considered in cloud computing systems. Second, it is basic to share a computer among various individuals. It possibly simple for programmers to introduce some spyware to take in the login secret key from the web-program. An as of late proposed access control display called attribute-based access control is a decent possibility to handle the principal issue. It not just gives unknown validation additionally defines access control approaches based on various attributes of the requester, environment, or the information protest. In an attribute-based access control system,1 every client has a client secret key issued by the power. Practically speaking, the client secret key is put away inside the PC. A more secure route is to utilize two-factor validation (2FA). 2FA is extremely basic among electronic e-managing an account administrations. Notwithstanding a username/secret key, the

DOI: 10.15680/IJIRCCE.2016. 0412005

client is moreover required to have a gadget to show a one-time secret key. A few systems may require the client to have a cell phone while the one-time secret key will be sent to the cell phone through SMS amid the login procedure. By utilizing 2FA, clients will have more certainty to utilize shared computers to login for electronic e-keeping money administrations. For a similar reason, it will be better to have a 2FA system for clients in the electronic cloud benefits keeping in mind the end goal to expand the security level in the system.

II. RELATED WORK

In this section, the reference are collected from all conferences, sites, articles, booka 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 journel 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 Aggreegate 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 uthentication 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.

(i) Wei Zhang, Student Member, IEEE, Yaping Lin, Member, IEEE, Sheng Xiao, Member, IEEE, JieWu, Fellow, IEEE, and Siwang Zhou" proposed a paper on "Privacy Preserving Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing".

(j) Xinyi Huang, Joseph K. Liu, Shaohua Tang, Member, IEEE, Yang Xiang, Senior Member, IEEE, Kaitai Liang, Li Xu, Member, IEEE, and Jianying Zhou" proposed a paper on "Cost-Effective Authentic and Anonymous Data Sharing with Forward Security". ID Based Ring Signature here also has disadvantage that Key exposure Network Connections Dependency.Cost is more" algorithm used are RSA/ElGamel/SHA.

III. PROPOSED SYSTEM

Modification of multiuser data, public auditing, probability for high error detection, effective user revocation and computational auditing performance can be characterized by a novel integrity auditing approach for data storage and sharing services. Attack of imitation can be avoid by given scheme. An important feature of cloud storage is data sharing. Sharing along with strong protection of data is the main aspect. Cryptography helps data owner to store data safely on cloud. While considering data privacy, we cannot rely upon traditional technique of authentication, because unexpected privilege escalation will expose all data. Solution is to encrypt data before uploading to the server with uploader's own key. Data sharing is again important functionality of cloud storage, because user can share data from anywhere and anytime and to anyone. First the admin saves file in the cloud space so that it will be available to users at any time. So he will generate a public key, which is used to encrypt the file. Then he chooses the file to upload and it is encrypted using public key. After encryption the file is uploaded to the cloud space. IP generate hash code of each file which is get uploaded by the data owner. When the user needs to access the file, the admin will share the file details with the user. The generated key sent via secure Email to the user. When the user gets the Email from the admin, he will get the file details. He can now enter the file name and key to download it, in his system. After downloading the decryption is carried out with key. Then the file is saved in the predefined folder in the client system. Un authorized access prevented by giving few preventive measures such as role based access, attack detection and preventions such as if unathorised user trying to access data files then those are identified and user gets blocked and he/she will not be log in to the system.The elimination of the costly certicate verication process makes it scalable and especially suitable for big data analytic.

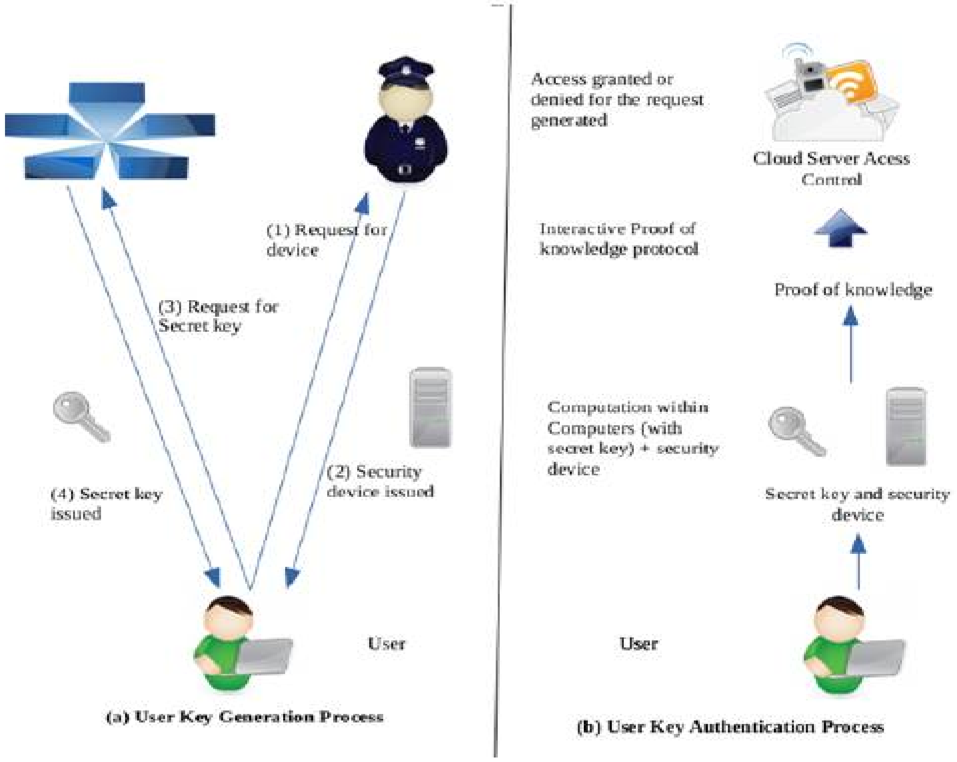
(1) Request for device
(3) Request for Secret key
(2) Security device issued
(4) Secret key issued
User
(a) User Key Generation Process
Access granted or denied for the request generated
Cloud Server Acess Control
Interactive Proof of knowledge protocol
Proof of knowledge
Computation within Computers (with secret key) + security device
Secret key and security device
User
(b) User Key Authentication Process

Fig:System Flow

DOI: 10.15680/IJIRCCE.2016. 0412005

IV. CONCLUSION AND FUTURE WORK

On this paper, we have provided a new 2fa (such aseach user secret key and a light-weight safety device) get right of entry tomanipulate system for net-primarily based cloud computing offerings. based totallyon the characteristic-primarily based get right of entry to control mechanism, the proposed2fa get entry to manage machine has been recognized to now not bestpermit the cloud server to limit the get admission to to those customers with the same set of attributes but additionally maintain consumer privateness.exact safety evaluation shows that the proposed 2fa get right of entry tocontrol gadget achieves the preferred protection necessities.we leave as future artwork to similarly enhance the efficiency while retaining all great capabilities of themachine.

REFERENCES

[1] 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”.
[2] 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.”.
[3] 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”.
[4] Mohamed Nabeel and Elisa Bertino, Fellow, IEEE proposed a paper on ”Privacy Preserving Delegated Access Control in Public Clouds”.
[5] 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”.
[6] Kaiping Xue, Member, IEEE and Peilin Hong, Member, IEEE proposed a paper on ”A Dynamic Secure Group Sharing Framework in Public Cloud Computing”.
[7] Tao Jiang, Xiaofeng Chen, and Jianfeng Ma IEEE. proposed a paper on ”Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation”.
[8] Jiawei Yuan and Shucheng Yu, Member, IEEE proposed a paper on ”Public Integrity Auditing for Dynamic Data Sharing With Multiuser Modification”.
[9] Wei Zhang, Student Member, IEEE, Yaping Lin, Member, IEEE, Sheng Xiao, Member, IEEE, Jie Wu, Fellow, IEEE, and Siwang Zhou” proposed a paper on ”Privacy Preserving Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing”.
[10] Xinyi Huang, Joseph K. Liu, Shaohua Tang, Member, IEEE, Yang Xiang, Senior Member,IEEE, Kaitai Liang, Li Xu, Member, IEEE, and Jianying Zhou” proposed a paper on ”Cost-Effective Authentic and Anonymous Data Sharing with Forward Security”.
[11] Pasquale Puzio A B, Rek Molva B, Melek Onen B, Sergio Loureiro A , “Block-level De-duplication with Encrypted Data” ACM, 2012.
[12] Pasquale Puzio “ClouDedup: Secure Deduplication with Encrypted Data for Cloud Storage vol. 5, no. 1, p. 5, 2011.