ISSN 2347 - 3983
Volume 8. No. 10, October 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter1318102020.pdf
https://doi.org/10.30534/ijeter/2020/1318102020

Multi-Layer Information Security Framework for Software – as –a- service Platform- as – a –Service and Infrastructure-as-a- Service of Cloud Computing Model

Krishan Dutt[1], Satinderjit Kaur Gill[2], Gurpreet Kour Khalsa[3], Pardeep Singh Cheema[4]
[1]Eternal University, Baru Sahib, Siramur H.P. India , kdutt96@gmail.com
[2]Eternal University, Baru Sahib, Siramur H.P. India, sk.gill78@gmail.com
[3]Eternal University, Baru Sahib, Siramur H.P. India, er.kaurgurpreet123@gmail.com
[4]Eternal University, Baru Sahib, Siramur H.P. India, pardeep13@yahoo.com

ABSTRACT

Cloud computing increased a widespread recognition as paradigm of computing. The main objective is to reduce the need for customers' security in new hardware or software by proposing flexible cloud services, with a usage customer gaining the advantages of the pay per use approach. Various security and confidentiality issues: both problems (vulnerabilities, threats, and attacks) are the pressing demand of cloud computing to find solutions (controls). We have discussed the security issues and authorization of cloud computing, customer and their privacy. Understanding number of vulnerabilities, threats, and attacks and identifying controls for these problems. We have proposed a Multilevel and multifactor Information security framework for cloud computing users with the use of cryptography techniques to guarantee the security and authorizations of the customer and data in cloud situation.

Key words: Authentication, Authorization, Access Control, Cloud Computing Multilevel framework**,**

1. INTRODUCTION

Security is one of the important feature of cloud computing, because in cloud computing mostly everything are provided as a service, like IaaS, PaaS, SaaS, and several others services. utility as a service like telephony bill and electricity bill, pay as usage based, in this type of situation security is the most important concern or how can we validate and approve the user is the actual user and owner of data. Therefore, it becomes a promising service platform, rearranging the configuration of Information. For validation, numerous methods are used, e.g. Public key infrastructure, username-passwords, symmetric key-based authentication schemes, biometric face recognition, and so on. Authentications schemes are significant procedures to check the approval of the uniqueness of all correspondence objects[1].In Cloud registering An outsider is in liable for giving the computational force, extra room and operational help and so on. Every information is kept in cloud database used by a user. Third party maintains cloud database, sometimes user hesitates to keep his information in Cloud database, So as to utilize the assets of Cloud, client needs to furnish with some character expressing that it is real substance searching for approval to utilize their assets. Client needs to pass a confirmation procedure in the event that he needs to utilize or control a far off worker or procedure money related exchanges, [2].

2. REVIEW OF LITERATURE

A detailed review of literature has been done related to our studies, there has been many techniques proposed and developed for authorization and validation , but there are very few for cloud computing authorization and confirmation of users in cloud Banyal et al[3]. developed a multifactor frame work by using three

attribute only Catchpa, OTP and Mobile EMEI base, Ullah et al[4] proposed a multistep and multifactor frame work for cloud computing, Ziyad, et al[5] developed a biometric feature frame work by the use of fingerprint and palmvienNagaraju et al [6] introduced the multifaceted validation and security insurance entryway. Li et al.[7] Presented the multi key protection saving by utilizing profound learning procedures and Harmonic encryption for plan of action Boneh and Franklin [8] contemplated the IdentyBased Encryption. Disseminated PKGs to conveyance of ace mystery key between different PKGs for power with an utilization gracious edge strategies by creating private key utilized or clients Chen et al.[9] considered IBE Paring based Cryptosystem with various confided in specialists, in which client can encode and unscramble figure text. Kate and Goldberg [10] contemplated the main execution of the dIBE conspire. Siad et al. [11] contemplated the DIBE Security model and to formalize the meaning of unidentified dIBEGrumazescu et al [12] introduced various leveled association in mix of appropriated PKGs Kalyani and Sridevi [13].developed a framework convention of circulated key giving convention was known Accountable Identity-Based Encryption. Goyal et al, in [14] proposed The possibility of Accountable Identity-Based Encryption (An IBE).two plans were introduced: one white-box An IBE plan and one fragile black-box An IBE plot. Goyal et al. [15] demonstrated the central full black-box An IBE plot. Libert and Vergnaud in [16].A convincing fragile black-box An IBE plot was introduced. Au et al. [17] broadened the constraint of An IBE and suggested a retrievable white-box An IBE plan, where the client can disengage the PKG's ruler mystery key when given a took private key made by the PKG. a skilled frail black-box . An IBE plot was presented by Libert and Vergnaud in [18] .The deciphering keys and ciphertexts in their course of action include a solid number of get-together parts, Sahai and Seyalioglu [19] improved Goyal et al, [14] and gave an absolutely secure full black-box An IBE think up. The open prominence issue for the sensitive black-box An IBE was first settled by Lai et al. [20], where the going with essentially needs an open after key, not the client's private key. Kiayias and Tang [21] exhorted the best way to deal with move any IBE to frail black-box An IBE. Han et al. [22] proposed a careful versatile online business progression subject to their character based plaintext-checkable encryption plot Cheng et al. [9] applied An IBE to propose a capable assurance protecting structure, Ainapure et al [23] proposed the amazed fleecy based approval plot work for appropriated registering for side channel ambush by using log archive and hashing limit. [24] Dinker et al proposed an approval and endorsements an amazed security check which included three phases diagram work for electronic devices and phones the three phases incorporate mystery express , security check using accelerometer, and biometric affirmations Zhao et al.[25]presented a solid structure with the proportionate security confirmation. These cryptographic inclinations the benefits of both the IBE with appropriated PKGs and an IBE. Specifically, it assigns the control to various PKGs, while added substance the perceptibility that could give a conclusive result to perceive the questionable between the customer and the PKGs

3. PROBLEM OF STATEMENT

The Main challenges of Cloud computing are security, respectability, and trust of quality. Customers' ensure that their data, which is put away on the cloud won't be recovered by different customers. To accomplish security on the cloud there are such a significant number of procedures and techniques of accessible. A portion of these procedures is Encryption: In this method, encryption techniques are utilized to shroud the first information with the assistance of the encryption key. The information is changed into a unintelligible structure called ciphertext and afterward put away remote storage Authentication: In this procedure, a login system is utilized to approve that the main true client is get into the cloud information. It requires making a client name and secret phrase. Approval rehearses: A rundown of Authorized customer is utilized to recognize, who can get to information put away on cloud framework. Notwithstanding, numerous individuals despite everything worry that different customers could get to data kept on a far off putting away framework and they will change it. Hackers can likewise attempt to take the physical

gear on which data are put away. A representative from cloud specialist organization could change or erase information utilizing his/her legitimate client name and secret phrase. Rather than every one of these dangers, customers are receiving distributed computing broadly .storage organizations are financing a great deal of reserve to ensure, that their customer's information would be protected. They are attempting to restrict the choice of data robbery or misuse. We are talking about certain techniques here that are helping how to get security on cloud

4. PROPOSED MULTI-LEVEL AUTHENTICATION TECHNIQUE

In this segment, the proposed frame and execution of different stages and exercises of secure are discussed in detail. Following are the assumptions that should not be disregarded during the execution of the proposed work. All the clients and CSP should be loyal in the registration stage. After registration stage is finished, no client, CSP is trusted. Clients are required to check themselves during login and confirmation level by giving genuine and accurate ID subtleties for getting to cloud administrations, applications and assets.
When common verification is done, the worker and CSP are al-ways trusted and it is expected that the worker be never undermined with the framework enemies. The proposed model comprises of three stages: enlistment stage, login and approval stage and information encryption stage.

4.1. Registration Stage

A client needs to register to ISF by giving suitable recognizable proof information. The worker forms client's information and registers the client the calculation for new Customer enrollment is as following:
In the registration stage, client needs to enroll at the ISF by giving proper recognizable proof data. The worker forms client's information and registers the client the calculation for new client enrollment is as following:

4.2 leve1 Authentication by User name and Password

Stage 1: UA – User name and Password produced
Stage 2 UA-User is confirmed by CSP Step3 If User name and Password is right and verified by CSP
Stage 4 Username Password verified permit client
If not verified go stage 2
Step5 else permit client
Step6 End
Step7 Exit

4.3.Level2 Authentication by One time Password

Step-1: User solicitations to ISF worker for new enlistment.
Step-2:User enters new client ID and secret key and
submits for enrollment.
Step-3:ISF worker checks for uniqueness of the mentioned ID. If not, it goes to step-2 else continues
Step-4:User gives every single required accreditation and submits.
Step-5:ISF–>U:M1, worker produces a one time secret key (OTP)
sends to client side , and showcases OTP
Step-6:IFS=>U:M2, worker creates a mystery confirmation code, sends to client email-id and asks client to
enter the confirmation code.
Step-7:U=>ISF:M1, client enter the OTP
what's more, sends to worker as OTP answer.

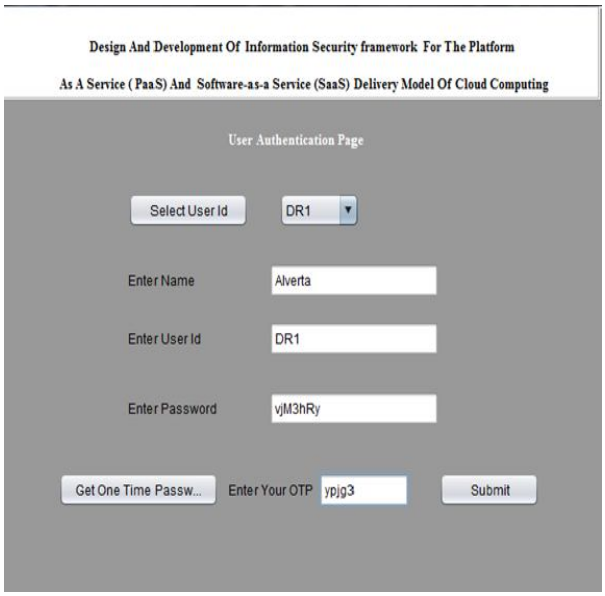

Figure 1: Authentication by OTP and Password

4.5 Level3 Authentication by Qubit key

The client is verified in Information security outline work by producing the key at the both end in this stage requested that th information be gotten to

The Following procedure are as follow:

Stages 1 client request that the document get to

Step2 the client send he mystery key to the Information security outline work worker for validations

Steps3 IFS Cloud specialist co-op get the created key and confirm the client

Step4 if the Secret shared key is incorrect ISF dropped the mentioned of the client and go to stage 1

Stage 5 if the key is coordinated the client pushed ahead to the following stage

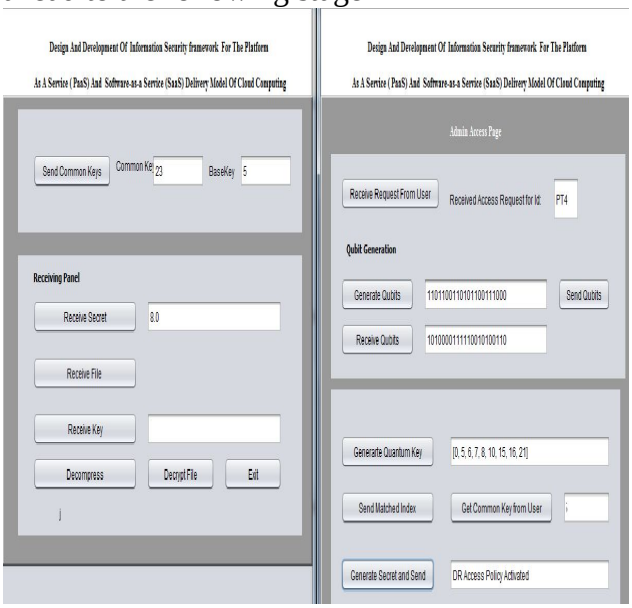

Figure 2: Exchange of Key between user and CSP Using Information Security Framework

4.6 Level 4 Authentication by Encryption and Decryption Data

The data file which the user asked the permission to access the file is encrypted by the cloud service provider along with the secret key after receiving the key and file the user matches the key if the key is match then only user able to access the data the algorthim for encryption and decryption is as follow

Encryption

Contributor A does the following:-

Gets the beneficiary B's Public key (n,e)(n,e).

Represent the plaintext message as a positive integer mm with $1<m<n1<m<n$

Compute the ciphertext c=me mod n c=me mod n.

Send the cipher-text to B.

Decoding

Recipients B do the accompanying:-

Utilize his private key (n,d)(n,d) to figure m=cd mod nm=cd mod n.

retrieve the plaintext from the message agent mm.

5. RESULT AND DISCUSSION

Secure credential management:: The ISF worker stores all the credentials of the client in a safe database. The worker checks the accessibility of a one of a kind ID for every client at the hour of new enrollment. This change office makes the system intrinsically more grounded contrasted with the static secret key based instrument. Replay assault: Three confirmation levels depend on three variables mystery key (K) and one-time secret phrase (OTP) Shared Secret key. Likewise, legitimate client login ID and secret key are required for verification. Man In The Middle Attack(MITM): In this structure regardless of whether assailants figure out how to get the client ID and secret phrase and can sign in into the framework, they can't get to cloud administrations and assets, as the client needs confirmation which requires a mystery key (K), once password(OTP),. These insider facts keys just traded between the client and the worker utilizing a different secure OOB channel. Taken verifier assault and unapproved affirmation assault: In the proposed framework, all confirmation factors are not accessible concurrent. Subsequently, regardless of whether one accreditation is taken or lost, verification needs different boundaries for login. Also, the structure gives a certification change office and if there should be an occurrence of a robbery, the client can change the necessary boundaries. Subsequently taken verifier assault and unapproved get to episode isn't relevant in this structure Phishing assault: In this system, basic approval among the client and the ISF worker, in light of multifaceted accreditations is performed. The mystery key, OTP, and shared key are mandatory for validation. Just the certifiable worker can send legitimate verification data. Furthermore, client reactions can be confirmed by

the approved worker as it were.) Password speculating assault: the proposed structure verification is made on multi-factors utilizing the mystery key, The utilization of OOB secure channel for trade of accreditations which gives more vigor to this plan. In the proposed structure, just secret word foreseeing isn't Figure 1.User verification framework(client name and secret key, Figure2 client with confirmation

6. CONCLUSIONS AND FUTURE SCOPE

Conclusions and Future Scope In proposed system we developed multilevel user authentication Information Security frame work for securing data from malicious users in cloud computing atmosphere. User is authenticating in each layer using not the same validation techniques. Compared with existing two factors and three factor validation, the proposed Information Security frame multifactor or multilayer authentication provides more security, high verification and ease of admittance information in cloud. The anticipated structure provides protection for the mapping of a variety of data essentials to every supplier using multifactor authentication storage boundary. This projected approach requires eminent implementation attempt; it provides significant data for cloud atmosphere conditions that can be capable of have elevated collision on subsequently innovation systems. When the user using this multilayer authentication technique to transfer the data, they really feel that their data's are secure. Our upcoming effort is to make longer the multifactor authentication data storage in to four factor authentication with digital signature

REFERENCES

1. Fan, Chun-I., Pei-Hsiu Ho, and Ruei-Hau Hsu. "Provably secure nested one-time secret mechanisms for fast mutual authentication and key exchange in mobile communications." IEEE/ACM Transactions on Networking 18, no. 3 (2009): 996-1009.
2. Juang, Wen-Shenq, Sian-Teng Chen, and Horng-TwuLiaw. "Robust and efficient password-authenticated key agreement using smart cards." IEEE Transactions on Industrial Electronics 55, no. 6 (2008): 2551-2556.
3. Banyal, Rohitash Kumar, Pragya Jain, and VijendraKumar Jain. "Multi-factor authentication framework for cloud computing." In 2013 Fifth International Conference on Computational Intelligence, Modelling and Simulation, pp. 105-110. IEEE, 2013.
4. Ullah, Sultan, ZhengXuefeng, and Zhou Feng. "TCLOUD: a multi–factor access control framework for cloud computing." International Journal of Security and Its Applications 7, no. 2 (2013): 15-26.
5. Ziyad, Shabana, and A. Kannammal. "A multifactor biometric authentication for the cloud." In Computational Intelligence, Cyber Security and Computational Models, pp. 395-403. Springer, New Delhi, 2014.
6. Nagaraju, Sabout, and LathaParthiban. "Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway." Journal of Cloud Computing 4, no. 1 (2015): 22.
7. Li, Ping, Jin Li, Zhengan Huang, Tong Li, Chong-ZhiGao, Siu-Ming Yiu, and Kai Chen. "Multi-key privacy-preserving deep learning in cloud computing." Future Generation Computer Systems 74 (2017): 76-85.
8. Boneh, Dan, and Matt Franklin. "Identity-based encryption from the Weil pairing." In Annual international cryptology conference, pp. 213-229.Springer, Berlin, Heidelberg, 2001.
9. Cheng, Hongbing, ChunmingRong, ManyunQian, and Weihong Wang. "Accountable privacy-preserving mechanism for cloud computing based on identity-based encryption." IEEE Access 6 (2018): 37869-37882.
10. Chen, Liqun, Keith Harrison, David Soldera, and Nigel P. Smart. "Applications of multiple trust authorities in pairing based cryptosystems." In International Conference on Infrastructure Security, pp. 260-275.Springer, Berlin, Heidelberg, 2002.
11. Siad, Amar. "Anonymous identity-based encryption with distributed private-key generator and searchable encryption." In 2012 5th International Conference on New

Technologies, Mobility and Security (NTMS), pp. 1-8. IEEE, 2012.
12. Grumăzescu, Constantin, Mihai-LicăPura, and Victor-ValeriuPatriciu. "Hybrid distributed-hierarchical identity based cryptographic scheme for wireless sensor networks." In New Contributions in Information Systems and Technologies, pp. 949-958.Springer, Cham, 2015.
13. Kalyani, Dasari, and R. Sridevi. "Robust distributed key issuing protocol for identity based cryptography." In 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 821-825.IEEE, 2016.
14. Goyal, Vipul. "Reducing trust in the PKG in identity based cryptosystems." In Annual International Cryptology Conference, pp. 430-447.Springer, Berlin, Heidelberg, 2007.
15. Goyal, Vipul, Steve Lu, AmitSahai, and Brent Waters. "Black-box accountable authority identity-based encryption." In Proceedings of the 15th ACM conference on Computer and communications security, pp. 427-436. 2008.
16. Libert, Benoît, and Damien Vergnaud. "Towards black-box accountable authority IBE with short ciphertexts and private keys." In International Workshop on Public Key Cryptography, pp. 235-255.Springer, Berlin, Heidelberg, 2009.
17. Au, Man Ho, Qiong Huang, Joseph K. Liu, Willy Susilo, Duncan S. Wong, and Guomin Yang. "Traceable and retrievable identity-based encryption." In International Conference on Applied Cryptography and Network Security, pp. 94-110.Springer, Berlin, Heidelberg, 2008.
18. Libert, Benoît, and Damien Vergnaud. "Towards black-box accountable authority IBE with short ciphertexts and private keys." In International Workshop on Public Key Cryptography, pp. 235-255.Springer, Berlin, Heidelberg, 2009.
19. Sahai, Amit, and HakanSeyalioglu. "Fully secure accountable-authority identity-based encryption." In International Workshop on Public Key Cryptography, pp. 296-316.Springer, Berlin, Heidelberg, 2011.
20. Lai, Junzuo, Robert H. Deng, Yunlei Zhao, and JianWeng. "Accountable authority identity-based encryption with public traceability." In Cryptographers' Track at the RSA Conference, pp. 326-342.Springer, Berlin, Heidelberg, 2013.
21. Kiayias, Aggelos, and Qiang Tang. "Making any identity-based encryption accountable, efficiently." In European Symposium on Research in Computer Security, pp. 326-346.Springer, Cham, 2015.
22. Han, Jinguang, Ye Yang, Xinyi Huang, Tsz Hon Yuen, Jiguo Li, and Jie Cao. "Accountable mobile E-commerce scheme via identity-based plaintext-checkable encryption." Information Sciences 345 (2016): 143-155.
23. Ainapure, Bharati, Deven Shah, and A. AnandaRao. "Adaptive multilevel fuzzy-based authentication framework to mitigate Cache side channel attack in cloud computing." International Journal of Modeling, Simulation, and Scientific Computing 9, no. 05 (2018): 1850045..
24. Dinker, A. G., Sharma, V., Mansi, & Singh, N. (2018).Multilevel authentication scheme for security critical networks. Journal of Information and Optimization Sciences, 39(1), 357-367.
25. Zhao, Zhen, Ge Wu, Willy Susilo, FuchunGuo, Baocang Wang, and Yupu Hu. "Accountable identity-based encryption with distributed private key generators." Information Sciences 505 (2019): 352-
366.