Enhanced Authentication and Data Privacy Preserving in Cloud Computing using MAC Partition Technique

P.G.Siva Sharma Karthick[1], M.Lavanya[2], S.Nasima Banu[3], M.Muthu Ishwarya[4], M.Sindhuja[5],

[1]Assistant Professor, Dept. Computer Science and Engineering, Nadar Saraswathi College of Engineering & Technology, Theni, Tamil Nadu, India.

[2,3,4,5]Student, Dept. Computer Science and Engineering, Nadar Saraswathi College of Engineering & Technology, Theni, Tamil Nadu, India

Abstract—Cloud computing is shared pools of configurable computer system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a public utility. In our work analyse of data present in the cloud get partitioned for security by using alert system. The admin user inserts the various files with the help of the keywords in the format of word document. Moreover in the cloud these files are to be inserted with OTP key mechanism and some of the partitioned files are to be maintained in encrypted form. When the users have to access these file they will be permitted only the proper authentication is succeeded after that the OTP is sent to the end user with the proper key and the partitioned information on the files. This OTP will be received through registered mail of the users. Using this OTP user access and download these files. The enhanced form of cryptographic algorithms is used for transferring data to and from the user side. This work has its implementation in the real world environment such as banking sectors, economical industries etc**.**

Index Terms —OTP, MAC partition, Privacy Preserving.

I.INTRODUCTION

Nowadays, cloud computing is turning into a huge growing technology in IT industries.it's a good impact in numerous sectors. So, several organizations area unit involving to the present technology and giving numerous services. Security could be a major issue in cloud computing. though cloud computing helps to form human life easier and straightforward, however it's a concern of security side. Users and CSP perpetually confine mind fairness regarding security of hold on data/files likewise as correct credentials. Peoples area unit storing and sharing period of time video, audio, photos etc. contents by victimization itinerant in cloud setting .a correct security technique will build it safer and stop information loses or taken by hackers or intruders. altogether space of IT industries, security is usually considered as a dominant field. In cloud computing, security perpetually play a significant role for quality of services (QoS). Cloud computing handles essential information and it may be accessed from anyplace within the world through web. therefore it makes security as a very important space of concern . Cloud computing has progressed from a daring vision to large deployments in numerous application domains. However, the quality of technology underlying cloud computing introduces novel security risks and challenges. Threats and mitigation techniques for the IaaS model are beneath intensive scrutiny in recent years whereas the business has endowed in increased security solutions and issued best observe recommendations. From AN end-user purpose of read the safety of cloud infrastructure implies unquestionable trust within the cloud supplier, in some cases substantiated by reports of external auditors. whereas suppliers might provide security enhancements like protection of information at rest, end-users have restricted or no management over such mechanisms. there's a transparent would like for usable and efficient cloud platform security mechanisms appropriate for organizations that have faith in cloud infrastructure. One such mechanism is platform integrity verification for reason hosts that support the virtualized cloud infrastructure. many giant cloud vendors have signaled sensible implementations of this mechanism, primarily to shield the cloud infrastructure from corporate executive threats and advanced persistent threats. we tend to see 2 major improvement vectors relating to these implementations. First, details of such proprietary solutions aren't disclosed and may therefore not be enforced and improved by alternative cloud platforms. Second, to the most effective of our data, none of the solutions provides cloud tenants a signal relating to the integrity of reason hosts supporting their slice of the cloud infrastructure. to handle this, we tend to propose a collection of protocols for trustworthy launch of virtual machines (VM) in IaaS, which give tenants with a signal that the requested VM instances were launched on a bunch with AN expected software system stack.

II.RELATED WORK

Cloud computing contains a huge growing nature in large space of the planet. therefore it's a high risk. once any business desires to travel with cloud computing, it considers numerous facet of risk like correct authentication, information security with privacy that ought to be integrated with its services [10]. Some authors have thought of information Protection, Loss of information, Traffic hijacking, Isolation of Resources and Malicious business executive as security concern [2]. AmitHendreet. al. [3] analyzed numerous security threats like information breaches, Data loss, Traffic hijacking, Insecure interfaces yet as arthropod genus, Denial of service, Malicious Insiders, Misuse of cloud facilities, Inadequate because of weakness business and Public Technology. Abhirupet. al. [5] offered a dynamic resource allocation technique for security purpose. Huang et. al. [4] shows Infrastructure-as-a-Service for cloud security. AsishAich et al. [1] delineated numerous cloud surroundings security risk like information run, DDoS attacks, Misuse of Cloud systems, unsure Lines and arthropod genus, Malicious Insiders, Shared Technology and repair Hijacking. They conjointly suggested some resolution to those problems. Aarti Singh et. al [8] mentioned security of cloud computing in numerous level. They showed Virtual Machine Security, Towards Interface Security etc., as numerous cloud level security. Cryptography will confirm a lot of security in data technology. an appropriate coding and decipherment methodology will guarantee information security in cloud computing. numerous rule exists for cryptography like DES, AES, RSA etc. AkshayAroraet. at [2] projected cloud security scheme. They used multi-factor authentication for guaranteeing information security. They conjointly send just once word (OTP) to the users by mail for with success login. once with success login, users will send or retrieve information from cloud surroundings. Ones information reaches to cloud finish, information can endure in coding method and hold on within the cloud. They used hybrid cryptography system as well as RSA and AES. this method appears to be sensible for information security, however if any unwelcome person gets credentials of any user, he can ready to amendment or modify information. By taking this downside, we have a tendency to offered an appropriate authentication system and cloud finish car coding method that may defend information and make sure that if any unwelcome person get certificate of any users he won't be ready to amendment cloud finish information.

III. PROPOSED SYSTEM

Our main goals are to secure hold on knowledge and authentication system in cloud setting. several researchers tried to secure varied credentials of users like secure login, storing data/file with encoding, key management etc. By any means that, if a hacker enters into the system, he could steal data/files from may finish. Our planned work is to associate degree analyse the cloud partition knowledge security by mistreatment an alert system. The admin inserts the assorted files with the assistance of the keywords. within the cloud system, these files ar to be inserted with OTP key mechanism.

When the users are to be searched within the cloud these files are to be within the format of the partition once the user accesses these files with the assistance of the OTP. This OTP are received within the mail to the users. mistreatmentthis OTP user access and transfer these files.

A. Users Authentication :When any clients/users can access his data/files or send new files, he has got to login together with his document (user ID and password). If his document is valid, then he can enter into next step of authentication. By now, system can generate a replacement key (KEY1) employing a hash operate with hold on KEY and delivers to the user/client by a secured channel (email, mobile etc.). User can enter KEY1 into the system. System can match this KEY1 with its antecedently generated KEY1. If with success matched, system can generate once more a KEY mistreatment anti-hash operate from KEY1 and matched with its hold on KEY. If matched once more with success, then system can treat this user as a sound user. This authentication system works in 3 steps. Firstly, activity user ID and watchword. Secondly, confirmative KEY1 (generated employing a hash operate with hold on KEY). This KEY1 are sent by a secured channel to the user. Thirdly, confirmative hold on KEY with new generated KEY mistreatment anti-hash operate with KEY1 (user provided KEY1). we've same earlier that, hackers are caught even he provides valid user ID and watchword. He also will be caught even whereas accessing the file that hold on KEY. As system can generate KEY1 employing a hash operate with hold on KEY and sends KEY1 to the user by a secure channel, the invalid users/ hackers won't be able to access this KEY1. So, he won't be able to provide new KEY1. thus there's no thanks to access data/file by associate degree invalid user

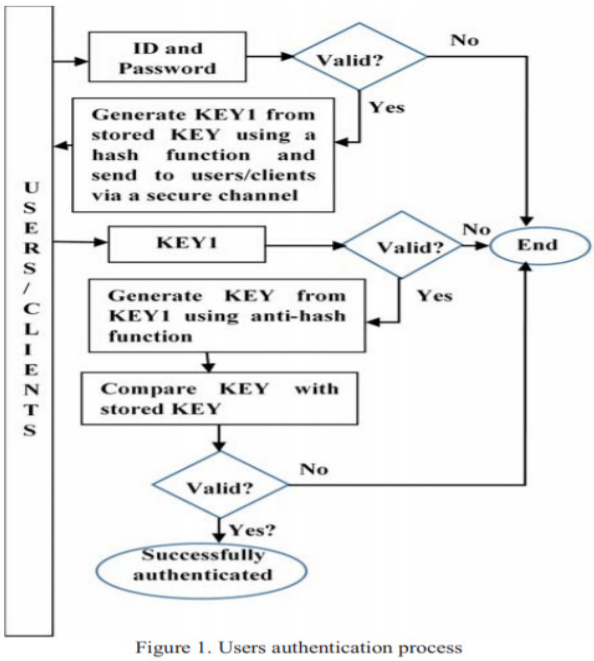

Figure 1. Users authentication process

An extra protection is additionally on the market by substantiative keep KEY with freshly generated KEY mistreatment anti-hash operate with equipped KEY1. this

technique is delineated in Fig. one and algorithmic rule one. once with success login, user can ready to access his data/file or send new file to cloud. Encrypted files/data are decrypted mistreatment valid KEY and can send to the users.

B. Cloud finish machine cryptography machine cryptography procedure is delineated in Fig. a pair of and algorithmic rule a pair of. In the Fig. 2, we tend to projected an automatic cryptography system. This cryptography system could also be used hybrid cryptography system together with RSA and AES or the other appropriate cryptography methodology. when login (described in previous section) users might access or send new data/files to store within the cloud and later he might logout. when sure-fire logout, the system can lock those files/data, the user has been accessed or hold on. Then system can produce a brand new key (KEY2) by employing a hash operate with antecedently used KEY. victimisation this new key(KEY2), those files/data are encrypted and new key(KEY2) are replaced with previous hold on KEY.

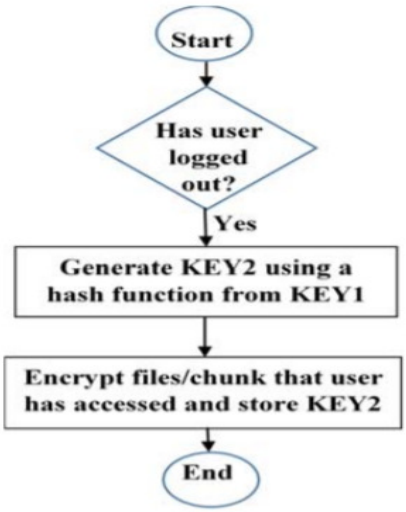

Figure 2. Cloud end auto encryption

II.PROPOSED WORK

Algorithm

1. At first, User login will be verified
2. If user logout, then generate KEY2 using a hash function with KEY1.
3. Encrypt files/data that has been accessed/stored by thisuser using a suitable encryption algorithm.
4. replace KEY1 by KEY2 and exit.

IV.SIMULATION AND RESULTS

We have simulated our protocol by CloudSim machine. For this we've created Associate in Nursing setting. we've created our own category for projected algorithms. once simulating the protocol, it's been ascertained that for further level of automotive vehicle encoding and KEY generation, it takes a bit bit time which may be neglected. we've created a hacker role with a user's credentials. we tend to ascertained that if this hacker will enter into cloud finish, then revised secret's sent to user email or mobile. This secret's not possible to induce by hacker. once more data/files is being encrypted mechanically once logged out by the user and latest secret's saved to a different file, that the hacker won't able to rewrite this file. therefore we are able to give a high level security in cloud computing by projected protocol

V.CONCLUSION

we have a tendency to planned machine cryptography method in cloud finish and 3 steps user authentication method during this paper.This procedure ensures further level of cryptography within the cloud finish. we've shown that if any hacker gets user's document, he could enter on cloud setting, however he won't be ready to access data/files or amendment or modify that data/file. This creates further profit to each user and Cloud Service suppliers (CSP). This protocol will be tested in massive knowledge analysis like health knowledge and academic knowledge etc.

REFERENCES

[1]. Arockiam and S. Monikandan, "Efficient cloud storage confidentiality to ensure data security," 2014 International Conference on Computer Communication and Informatics, Coimbatore, 2014, pp. 1-5.
[2] D. Singh and H. K. Verma, "A new framework for cloud storage confidentiality to ensure information security," 2016 Symposium on Colossal Data Analysis and Networking (CDAN), Indore, 2016, pp. 1-5.
[3] Maninder Singh Bhajwa, Himani, and Sandeep Singh Kang, An Enhanced Data Owner Centric Model for Ensuring Data Security in Cloud", 2015 IEEE Xplore, pp. 500-503.
[4] K. Suthar and J. Patel, "EncryScation: A novel framework for cloud IaaS, DaaS security using encryption and Obfuscation techniques," 2015 5th Nirma University International Conference on Engineering (NUiCONE), Ahmedabad, 2015, pp. 1-5.
[5] S. A. Oli and L. Arockiam, "Confidentiality technique to obfuscate the numerical data to enhance security in public cloud storage," 2017 International Conference on Algorithms,Methodology, Models and Applications in Emerging Technologies (ICAMMAET), Chennai, 2017, pp. 1-6.
[6] K. Inayah, B. E. Sukmono, R. Purwoko and S. Indarjani, "Insertion attack effects on standard PRNGs ANSI X9.17 and ANSI X9.31 based on statistical distance tests and entropy difference tests," 2013 International Conference on Computer, Control, Informatics and Its Applications (IC3INA), Jakarta, 2013, pp. 219- 224.
[7] Y. Zhang, C. Xu, X. Liang, H. Li, Y. Mu and X. Zhang, "Efficient Public Verification of Data Integrity for Cloud Storage Systems from Indistinguishability Obfuscation," in

IEEETransactions on Information Forensics and Security, vol. 12, no. 3, pp. 676-688, March 2017.
[8] Shaanan N. Cohney, Matthew D. Green, and NadiaHeninger,"Practical state recovery attacks against legacy RNG implementations", 2018 ACM SIGSAC Conference on Computer and Communications Security.
[9] Abinesh Kamal K. U. and ShijuSathyadevan, "Intrusion detection system using big data framework", ARPN Journal of Engineering and Applied Sciences, June 2017.
[10] S. Santhanalakshmi, Sangeeta, K., and Patra, G. K., "Design of secure Cryptographic hash function using soft computing techniques", International Journal of Advances in Soft Computing and and its Applications, vol. 9, pp. 188-203, 2017
[11] Random number generator recommendations for applications,20june 2019,www.codeproject.com.
[12] PriaBharti and RoopaliSoni, "A New Approach of Data Hiding in Images using Cryptography and Steganography", International Journal of Computer Applications (0975 – 8887) Volume 58– No.18, November 2012.
[13] Wafaa M. Abduallah1, Subhi R. MohmmedZeebaree, "New Data hiding method based on DNA and VigenereAutokey", Academic Journal of Nawroz University (AJNU) 83, 2017.
[14] AkashdeepBhardwaja, GVB Subrahmanyamb, VinayAvasthic and HanumatSastry, "Security Algorithms for Cloud Computing", International Conference on Computational Modeling and Security (CMS 2016).
[15] SairamNatarajan, ManikandanGanesan and Krishnan Ganesan, "A Novel Approach for Data Security Enhancement Using Multi Level Encryption Scheme", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (1) , 2011, 469-473.
[16] Anamika Sirohi1 and Vishal Shrivastava, "A Multi-Level Security Mechanism for Data Storage in Cloud Computing: A Review", International Journal for Research in Applied Science & EngineeringTechnology (IJRASET), 2016.