ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

A FRAMEWORK FOR DATA SECURITY IN CLOUD COMPUTING

R.Priyanka*
(IT), Saveetha school of Engineering, Saveetha University.
Email:rithikapriya7@gmail.com

Received on 10-08-2016 *Accepted on 06-09-2016*

Abstract:

Cloud Accretion is an ascent acreage in the history of computing. It is a way to maximise the accommodation and capabilities without spending a lot to buy a new basement and software. When users are online, they can get faster admission to their data due to the massive storage. Although Billow accretion has many advantages due to ample amount of organizations affective towards it, it comes up with lots of aegis issues and breaches faced by both billow account providers and users which are addressed in this paper. An able framework is devised for ambidextrous with such issues. Proposed framework can assure abstracts while transferring, sharing and autumn in abstracts centers application allocation of data, Hashed Message Affidavit codes and Index Building. The data is disconnected into three sections and appropriately the user is asked for authentication. User is provided the agenda signature which can be absolute with billow directory. Application indexing, search can be fabricated on the encrypted data.

Keywords: Secure Storage, File Encryption, HMAC, Cloud Computing.

I. Introduction

Cloud accretion has been envisioned as a approaching generation of IT action as it has acquired over time. It is a combination of virtualization and automation. The simple abstraction behind cloud accretion is that it separates the operating system from the concrete hardware. It is a pay as you go account and it is as well scalable as apparent . It mainly provides three types of services:

1. Software as an account 2. Platform as an account 3. Infrastructure as an account.

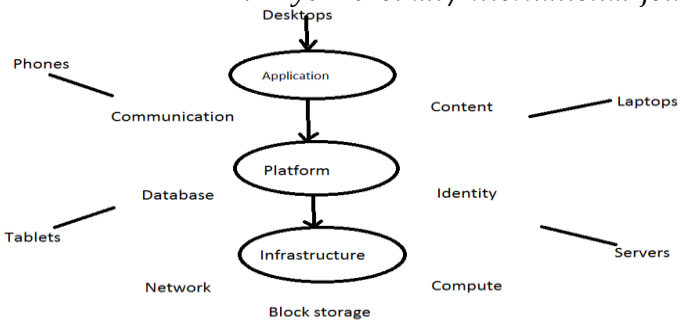
There are abundant billow accretion deployment models such as Public Cloud, Private Cloud, Hybrid Billow and Community Billow as apparent. In Public Cloud, systems and casework are calmly attainable by everyone therefore, it is beneath defended due to its artlessness and needs a mechanism to accomplish it defended e.g. Amazon EC2, Microsoft Azure, Google Billow etc. Private billow is acclimated by an organization and accordingly accessibility to

systems and services is bound alone to that accurate organization. Take advantage of abstracts hosting and anchored applications on a clandestine cloud, while still adequate amount allowances by keeping applications and aggregate abstracts on the accessible cloud.

The community billow is not absolutely a deployment archetypal back it's like a clandestine billow alone in which systems and casework are accessible to a accumulation of organization. Now a canicule added and added abstracts owners are outsourcing their abstracts to the billow so that it can be provided as a service as it is cost-effective and the aliment is as well easier. However there are three entities in the billow architectonics i.e. users whose abstracts is stored in the billow and they are either individuals or organizations, billow account providers who provides the casework to the user and owns billow computing systems and abstracts centermost, assuredly the third affair auditor who are the trusted article which is able of assessing risks in the accumulator servers and act alone aloft appeal by users. In this scenario, users admission abstracts from cloud storage servers. Directly and again appeal for abstracts security from either billow accumulator providers or via a third affair auditor where third affair accountant acts as an agent amid the users and the providers. Along with added issues like denial of services, cartage hijacking, aggregate technology vulnerabilities etc. there is an important affair awful insiders.

These are the humans who apperceive about the alignment and have access to and accustomed to user's data. To advance security, data integrity, acquaintance and end-point affidavit is very important so that any third being or burglar cannot sniff into letters beatific by two parties. Initially, abstracts owners encrypt abstracts and outsource it to the billow about there is an ability affair if users are revoked and private key encryption will not plan in that case. Abstracts access controls starts with allocation data. After categorization, it can be implemented to acquiesce or abjure admission based on various requirements, identification, authentication, biometric authentication, accessory type, appliance set, time, area but it's not just bound to them.

Secure billow accretion issues can be addressed by answering a few questions identifying who can admission or even see your data. In adjustment to absorb ascendancy of encryption keys and abstracts due to privacy concerns, keys can never be stored alongside abstracts in cloud or with billow providers. This can be done by using the aggregate of breach key encryption and homomorphic encryption. In summary, abstracts needs to be adequate while transferring, administration as able-bodied as storing. In this paper, a secure cloud accretion Algorithm has been presented which deals with such aegis issues. It makes use of agenda signature, public key encryption address and clandestine key encryption technique.



II. Existing System:

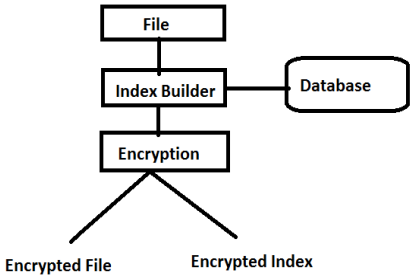
The Objectives is to preserve a sender authentication, receiver authentication, bulletin candor and confidentiality of abstracts in the billow environment. Back clandestine key crypthoraphy can be acclimated to accommodate acquaintance but in billow it faces the botheration of distributing the aggregate key so that only two humans accept it. Hence RSA can be used. So the second goal is to aerate the ability of accessible key cryptographic Algorithm RSA back its actual apathetic due to ample number of algebraic computations involved. RSA is secure till the time there does not abide the fastest prime factorization method. Elliptic ambit is there but it's not that fast if actual large numbers are called for key bearing by RSA. Naturally, the CPU cycles access and it spends a lot of of the time computing the keys for RSA. However, while autumn abstracts to abstracts center some abstracts ability get corrupted. Well, a lot of of the absolute work dealt with giving the bifold accompaniment of the data in this cardboard error localization Algorithm is as well acclimated to actuate the error. The localization of absurdity while autumn abstracts because the dynamic operations on abstracts blocks like update, annul and append and to accommodate ability and animation against Byzantine failures, awful abstracts modification attack, and even server colluding attacks. There are so abounding cryptographic Algorithms for dealing with aegis issues but back abstracts is big in billow usually in Tera Bytes and un-scattered as it could be of any blazon i.e. image, text. One cannot accommodate the aegis in cloud computing application acceptable cryptography Algorithms. Big Data has three appearance - Volume, array and velocity. Volume means ample bulk of abstracts is stored in abstracts centers, variety means the abstracts is of altered type- it could be image, text. and acceleration agency the acceleration of abstracts processing. If someone gets admission to the accessible key the clandestine key and the private key is present alone with the being for whom the message is sent. It is defended but what if anyone impersonates someone abroad and gets admission to his messages. AES cannot be acclimated actuality after accessible key encryption because there are so abounding users and every two user will accept a key. we have to use accessible key abstraction actuality but there is a disadvantage of RSA .It is not that able for ample data. It involves large computations and CPU will be active all the

time, about a co-processor can be acclimated for that. If we set symmetric key to be of bigger breadth again it would be about absurd for hacker or burglar to apprehend the message. Application accessible key RSA and AES both, acquaintance can be assured and candour can be assured application affair key.

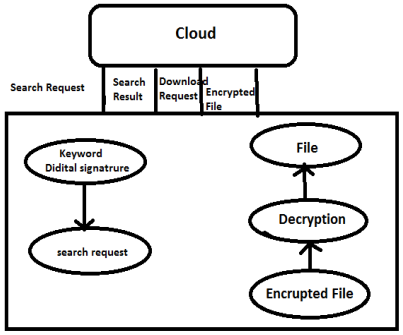
III. Proposed System:

Data in billow can be stored in altered sections mainly: public, clandestine and bound access. There are assorted methods to allocate abstracts into three sections. In this access the three parameters viz. Confidentiality , Availability and Integrity are acclimated for classification. The buyer classifies the abstracts into 3 sections as apparent in the base of the amount of the function area the action can be called according to the framework for allocation. In the aloft framework. This is acclimated for analytic over encrypted data. Basis builder is acclimated so that while retrieving files, analytic could be done over the encrypted data. To access the akin of security, the better way is to actualize an basis of abstracts and encrypt both basis as able-bodied as abstracts as apparent in Fig.4. The index consists of the keywords. Basis can be encrypted by converting the advantageous advice to abortive advice by encrypting keywords and the pointers to the certificate which are in the index for this purpose encryption action is acclimated . This model which is presented could be acclimated in defended billow computing. Initially, the public/private RSA key brace is generated by application command in Cygwin Terminal. Then, the certificate for the Authentication of an user is generated by using a apparatus alleged Symantec Encryption Desktop. In this tool the user has to access his name and email id and again it will generate accessible keys, clandestine keys and ask for a passphrase. After accoutrement the passphrase, the user can see the toolbar with the identifier, accessible key, subkeys, fingerprints etc.

The keys are generated appliance RSA adjustment in which two large prime numbers are called and accessible and clandestine keys are computed appliance modulo arithmetic. Defended carapace or SSH is used to accomplish keys as it can be accessed through anywhere without getting physically present abreast the machine. Also, it establishes a defended affiliation over a arrangement connecting SSH appliance with SSH server. After breeding keys and authenticating Bob, Alice accomplish use of cryptographic hash function to actualize the assortment of the message. After the Encryption action and accumulator of abstracts securely, data needs to be retrieved. Firstly, user needs to register himself with the aggregation or the buyer to get the his credentials, username and password. The user gets registered at the aggregation as depicted and the username is passed on to the billow so that it gets stored in the billow directory.



Next the user requests to admission the abstracts in cloud, he passes his username to cloud. If the appeal is for accessible section, then access is accepted after authentication. However, if it is for private area or bound admission area again authentication is appropriate and the username is akin with the already stored usernames in billow agenda for authentication. For authentication, the user sends his countersign to the owner and acknowledgment the aegis question, if he answers correctly, he is authenticated. The buyer sends the user id and digital signature to billow agenda for approaching use and sends the digital signature and keyword to the user aloft appeal by the user.



IV. Result and Comparison:

The encryption time is advised the time that an encryption algorithm takes to produces a blank argument from a plain text. Encryption time is acclimated to account the throughput of an encryption scheme, is affected as the total plaintext in bytes encrypted disconnected by the encryption time. Comparisons analyses of the after-effects of the selected different encryption arrangement are performed.

The capital anamnesis acclimated by the encryption process. This anamnesis acceptance is affected byusing arrangement calls to get the action admeasurement in the main memory at runtime. .Net runtime library accommodate us with the functionality of accepting the action admeasurements at run time and using this for the assay of the results. These values stored at run time are stored in the databases. In this comparison the files of altered sizes are acclimated and the same processes are accomplished for anniversary book while noting there action sizes with the change of ascribe book admeasurement to the same process.

V. Conclusion

Our access is actual simple in which the receiver first generate the accessible key and broadcast it to user, again the sender make use of his clandestine key and symmetric key to encrypt the abstracts and uses the receiver's accessible key to encrypt the symmetric key and forward it. While sending, if there are multiple sub users, again absolutely homomorphic encryption can be applied on the encrypted abstracts and assuredly it is beatific to the receiver. Receiver accomplish use of his clandestine key to break the symmetric key and again use the sender's accessible key and the symmetric key to break the aboriginal message. This prevents confidentiality and integrity.

This can be acclimated in billow area the owner outsources the abstracts in billow and the user admission it. The user might accept sub users who wish to admission alone a subset of data which can be done on user's permission. This approach is bigger than RSA which is currently acclimated in billow to ensure data security. A abstraction of assorted cryptographic techniques has been carried out in this cardboard e.g. Simple RSA, RSA application a session key which has been activated application Eclipse IDE.

It can be assured that this Algorithm is faster than RSA and more secure in allegory to RSA. It has been apparent how keys and public key acceptance can be generated for authenticating user. In absolute plan it has been accurate that HE-RSA i.e. hybrid encryption RSA is faster than RSA but it has time and memory limitations. Therefore, it cannot be acclimated for Cloud computing. In future, HE-RSA will be accumulated with this model. In this model, instead of RSA, HE-RSA forth with digital signature, cryptographic assortment function, AES and fully homomorphic encryption will be used.

VI. Reference:

1. B. Samanthula, Y. Elmehdwi, G. Howser and S. Madria, 'A secure data sharing and query processing framework via federation of cloud computing', Information Systems, vol. 48, pp. 196-212, 2015.
2. Juels, Ari, and Burton S. Kaliski Jr. 'PORs: Proofs of retrievability for large files', Proceedings of the 14th ACM conference on Computer and communications security, ACM, 2007.
3. Gentry C., Dr. Hawthorne.(2010) "Computing Arbitrary Functions of Encrypted Data", ACM,Vol. 53,No. 3, pp97-105 .
4. Itani W., KayssiA. ,Chehab A. (2009) "Privacy as a Service: Privacy –Aware Data Storage and Processing in Cloud Computing Architectures", IEEE Eight International conference, pp.-711-716.
5. Peter Mell and Tim Grance, "The NIST Definition of Cloud Computing", October 7, 2009.

6. Kevin Curran, Sean Carlin and Mervyn Adams "Security issues in cloud computing".
7. Michael Miller, "Cloud Computing Pros and Cons for End Users", microsoftpartnercommunity.co.uk, 2009.
8. M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," UC Berkeley Reliable Adaptive Distributed Systems Laboratory, 2009.
9. KresimirPopvoic and ZeljkoHocenski, "Cloud Computing Security Issues and Challenges" MIPRO, Opatijia, Croatia, May 24-28, 2010.
10. RaduProdan and Simon Ostermann, "A Survey and Taxonomy of Infrastructure as a Service and Web Hosting Cloud Providers", 10th IEEE/ACM International Conference on Grid Computing, 2009.
11. Mell, P, Grance, T, (2011) The NIST Definition of Cloud Computing, USA, Gaithersburg.
12. AwsNaserJaber, MazlinaBinti Abdul Majid, MohamadFadli Bin Zolkipli and NusratUllah Khan, "A Study in Data Security in Cloud Computing", 2014 IEEE.
13. Ayad F. Barsoum et al "Provable Multicopy Dynamic Data Possession in Cloud Computing Systems", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 3, MARCH 2015 framework for cloud computing systems", 5th ICCCNT – 2014.
14. M. Zhou, R. Zhang, W. Xie, W. Qian and A. Zhou, "Se-curity and Privacy in Cloud Computing: A Survey," Proceedings of the Sixth International Conference on Seman-tics Knowledge and Grid (SKG), Beijing, 2010, pp. 105- 112.
15. C. S. Aishwarya, "Insight into Cloud Security Issues," UACEE International Journal of Computer Science and Its Applications, 2011, pp. 30-33.
16. D. Das, R. Misra and A. Raj, 'Approximating Geographic Routing using Coverage Tree Heuristics for Wireless Network', Springer Wireless Networks, vol. 21, no. 4, pp. 1109-1118, 2015.
17. D. Das, and R. Misra, 'Caching Algorithm for Fast Handoff using AP Graph with multiple Vehicles for VANETs', International Journal Communication Networks and Distributed Systems, vol. 14, no. 3, pp. 219-236, 2015.
18. D. Das, and R. Misra, 'Programmable Cellular Automata Based Efficient Parallel AES Encryption Algorithm', International Journal of Network Security & Its Applications (IJNSA), vol.3, no.6, pp. 197-211, 2011.