International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 13
October 2017

Design of Improved Data Security in Cloud Computing Applications

Gattu Ramya
Assistant professor, Department of CSE
Siddhartha Institute Of Technology And Sciences, Hyderabad, Telangana, India

ABSTRACT: Cloud computing has become an important platform for companies to build their infrastructures upon. If companies are thinking to take advantage of cloud based systems, they will have to seriously reassess their current security strategies as well as the cloud-specific aspects to be a successful solution provider.The data can be stored remotely in the cloud by the users and can be accessed using thin clients as and when required.One of the major issue in cloud today is data security in cloud computing.Storage of data in the cloud can be risky because of use of Internet by cloud based services which means less control over the stored data. One of the major concern in cloud is how do we grab all the benefits of the cloud while maintaining security controls over the organizations assets. Our aim is to propose a more reliable, decentralized light weight key management technique for cloud systems which provides more effecient data security and key management in cloud systems.

KEYWORDS-Cloud security; key management; server colluding attacks

I. INTRODUCTION

Cloud computing is a brand new technology that is a consequence ofwrapping Virtualization, parallel computing and then distributed computing into a single device. The NISTdefinition of cloud computing "Cloud computing is actually asending type that enabling ubiquitous, convenient,efficient on-demand network access to a pool of sharedconfigurable computing materials including networks,storage, programs, server and services which could be quickly provisioned and reduced". This cloud model isconsists of 5 important qualities, 3 service models, and 4 deployment models.The cloud computing is actually a web-based design that is connected with more than a single process.

Cloud computing isthe mix of essential technique that is energy computing as well as service-oriented architecture.Cloud computing means delivering everything software as well as hardware by making use of the web. It removes the necessity ofsetting cost devices that are high for infrastructure for anybusiness, with the assistance of cloud computing thebusiness takes proper care of its capabilities go rather than to produce a costly infrastructure.In cloud atmosphere, all the information are outsourced to an external provider and they also take concern of that data is nowa duty of the cloud provider and we are able to use this data on virtual devices or maybe some other device. Since thedata center of the cloud provider is actually dispersed to all over in theworld and we are able to access the data of ours from any corner of the world. Cloud Computing is the outcome of improvements inthe presented technologies. At the present world ofmarketing system, Cloud computing is actually among the mostimportant and developing option for both the users and the developers. Within the cloud environment, resources are actually sharedamong the servers, individuals and users.

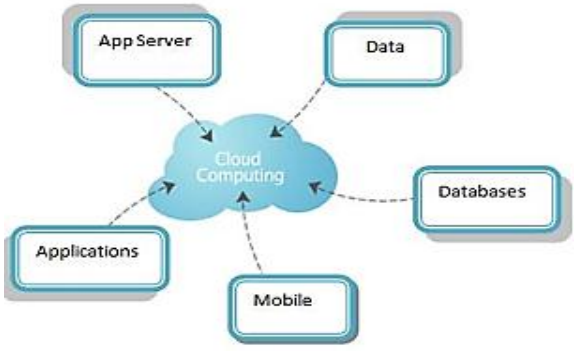

Fig1. Cloud computing

These Cloud services can be further comes under the threecategories.

 SaaS- Application that is deployed over anetwork, typically the web, accessible via a browser orprogram interface; referred to as software on demand.

 PaaS- A platform on which user can build theirapplication using languages, libraries, tools and servicessupported by provider.

 IaaS- Processing and storage capacity,networking and computing resources where the user hascontrol over operating system and deployed application;sometimes referred to as utility computing.

There are various policies issues and threats in cloudcomputing technology which include privacy, segregation,storage, reliability, security, capacity and more. But mostimportant among these to concern is security and how serviceprovider assures it to maintain. Generally cloud computinghas several customers such as ordinary users, academia andenterprises who have different motivations to move to cloud.If cloud clients are academia, security effect on performanceof computing and for them cloud providers have to find a wayto combine security and performance. For enterprises mostimportant problem is also security but with different vision. So, we mainly concentrate on data security of cloudcomputing.

II. RELATED WORKS

Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing (2009)" describes that "CloudComputing has been envisioned as the nextgeneration architecture of IT Enterprise. It movesthe application software and databases to thecentralized large data centers, where themanagement of the data and services may not befully trustworthy. This unique paradigm bringsabout many new security challenges, which havenot been well understood. This work studies theproblem of ensuring the integrity of data storagein Cloud Computing. We first identify thedifficulties and potential security problems ofdirect extensions with fully dynamic data updatesfrom prior works and then show how to constructan elegant verification scheme for seamlessintegration of these two salient features in ourprotocol design.

• ***"Data Management in the Cloud: Limitationsand Opportunities, March 2009"*** is focused todiscuss the limitations and opportunities ofdeploying data management issues on theseemerging cloud computing platforms. Wespeculate that large scale data analysis tasks,decision support systems, and applicationspecifically data marts are more likely to takeadvantage of cloud computing platforms than

operational, transactional database systems (atleast initially). We present a list of features that aDBMS designed for large scale data analysis tasksrunning on an Amazon-style offering shouldcontain. We then discuss some currently availableopen source and commercial database options thatcan be used to perform such analysis tasks, andconclude that none of these options, as presentlyarchitected, match the requisite features. We thusexpress the need for a new DBMS, designedspecifically for cloud computing environments.

• ***"Security Guidance for Critical Areas of Focus in Cloud Computing, April 2009",*** is intended toprovide security practitioners with acomprehensive roadmap for being proactive indeveloping positive and secure relationships withcloud providers. Much of this guidance is alsoquite relevant to the cloud provider to improve thequality and security of their service offerings. Aswith any initial venture, there will certainly beguidance that we could improve upon. We willquite likely modify the number of domains andchange the focus of some areas of concern.

• ***"Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control (2009)",*** "characterizes the problems and theirimpact on adoption. In addition, and equallyimportantly, we describe how the combinationof existing research thrusts has the potentialto alleviate many of the concerns impedingadoption. In particular, we argue that withcontinued research advances in trustedcomputing and computation-supportingencryption, life in the cloud can beadvantageous from a business intelligencestandpoint over the isolated alternative that ismore common today.

• ***"CryptoNET: Software Protection and Secure Execution Environment (2010)",***

describesprotection of software modules which is based onstrong encryption techniques, for example publickey encryption and digital signature. Theseprotected software modules are encapsulated inour designed XML file which describes a generalsyntax of protected software modules. In addition,our designed system also securely distributessoftware modules to authorized user. Securesoftware distribution system is based on wellestablished standards and protocols like FIPS-196based extended strong authentication protocol andSAML based authorization security policies. Wealso designed secure execution environmentwhich is capable to execute signed and encryptedsoftware modules, supports standard securityservices and network security protocols. Theseare: transparent handling of certificates, use ofFIPS-201 compliant smart cards, single-sign-onprotocol, strong authentication protocol, andsecure asynchronous sessions".

• ***"Security Issues for cloud computing (2010)"***discusses security issues for cloud computing andpresent a layered framework for secure clouds andthen focus on two of the layers, i.e., the storagelayer and the data layer. In particular, the authorsdiscuss a scheme for secure third partypublications of documents in a cloud. Next, thepaper will converse secure federated queryprocessing with map Reduce and Hadoop, anddiscuss the use of secure co-processors for cloudcomputing. Finally, the authors discuss XACMLimplementation for Hadoop and discuss theirbeliefs that building trusted applications fromuntrusted components will be a major aspect ofsecure cloud computing.

• ***"Deployment Models: Towards Eliminating Security Concerns from Cloud Computing (2010)"*** claims that Cloud computing has becomea popular choice as an alternative to investing newIT systems. When making decisions on adoptingcloud computing related solutions, security hasalways been a major concern. This articlesummarizes security concerns in cloud computingand proposes five service deployment models toease these concerns. The proposed modelsprovide different security related features toaddress different requirements and scenarios andcan serve as reference models for deployment.

• ***"A survey on security issues in service delivery models of cloud computing (2010)",*** discussesthat the architecture of cloud poses such a threatto the security of the existing technologies whendeployed in a cloud environment. Cloud serviceusers need to be vigilant in understanding therisks of data breaches in this new environment. Inthis paper, a survey of the different security risksthat pose a threat to the cloud is presented. Thispaper is a survey more specifically to the differentsecurity issues that has emanated due to the natureof the service delivery models of a cloudcomputing system.

III. APPROACH

The main entities in the proposed algorithm are cloud users, cloud storage server,cloud manager, keysplitter servers, share holder servers, security servers, log editorwhich are defined in detail as follows:

1. User: The user can create, update and delete his/her profile, store andretrieve the data

2. Cloud Storage Server: It is a model of data storage on virtualized storagepools or servers located remotely. Cloud storage can be used by users to store their data. Users can buy storage capacity from the cloud hosting companies.The main responsibilities of cloud storage server are storing the encrypted document, storing the splitted encryption key values for the purpose of keymanagement .

3. Key Management Server: Key splitter server splits the encryption keysinto different shares and store the splitted keys in different share holderservers.

4. Share Holder Server: These servers stores the shares for the different keysfor different users. Share holders can be of two types. Primary share holderdirectly receive the shares from the cloud manager. Secondary share holdersare the share holders at the leaf level and these share holders receive theirshares through primary share holders.

5. Log editor: It checks the share holder servers timely to see if the shares are gettingmodified.

6. Security server: It has the encryption decryption algorithm.

Encryption process

Step 1- Split the letter of modified plaintext.

Step 2- Assign the position(i) of the letter.

Step 3- Generate the ASCII value of plaintext letter.

Step 4- E=(p+k+i)

p-plaintext, k-shared key, i-position

Step 5- Generate the ASCII character of the corresponding decimal value

in the result from the above given formula.This would be the cipher text.

Decryption process

Step 1- Generate the ASCII value of the cipher text character.

Step 2- Same encryption key is used.

Step 3- Assign the position i of the cipher text.

Step 4- D=((c-k-i)+256)

p-plaintext, k-shared key, i-position.

Step 5 Generate the ASCII character of the corresponding decimal valuein the result from the above given formula.This would be the original plain text.

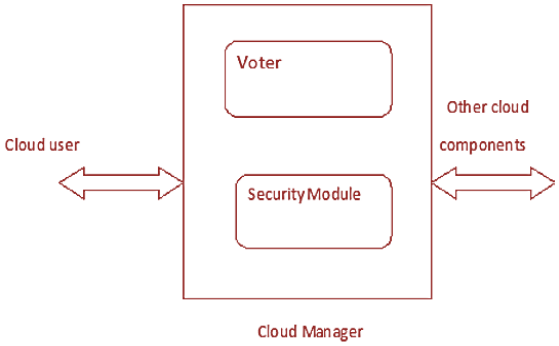

Figure.2 Cloud manager

File Upload:

When the cloud user wants to submit a file to a cloud first the file is forwardedto the cloud manager. Security module in cloud manager generates the key andencrypts the file using the encryption algorithm as shown and then forwards thekey to key management module. Encrypted file is forwarded to the cloud datastorage center. Key management module divides the key into number of shares.Sends a master key to the cloud user and distributes all the remaining keys to theShareHolderServers. All the primary share holders and secondary share holders are monitored from time to time to ensure that their values arenot modified byattacker.

File Download:

When the cloud user wants to download a file that is stored in cloud file name andshared master key are entered by cloud user. Download request is forwarded to keymanagement server. Key management server requests all the ShareHolderServersto forward their part of keys that correspond to the file name required to it.Keymanagement server combines all the shares to generate the 2nd level keys andforwards the key to the security server Security server combines the master keywith other secondary key to generate the main key. The file is decrypted and issent to the cloud user.

IV. CONCLUSION

In the cloudplatform, there is always a possibility of insider attack or outsider attack. Keys canbe accessed or stolen by employees without the knowledge of end users. Our aim isto provide secrecy to the data as well as keys that are stored in cloud systems. Ourproposed technique provides better data security and key management in cloudsystems.

REFERENCES

[1] Peter Mell and Tim Grance, "The NIST Definition ofCloud Computing", October 7, 2009, version 15, NationalInstitute of Standards and Technology (NIST).

[2] Kevin Curran, Sean Carlin and Mervyn Adams"Security issues in cloud computing", publishedin August2011, Elixir Network Engg.

[3] Kevin Hemalen, Murat Kantarcioglu, Latifur Khan,and BhavaniThuraisingham, The University of Texas atDallas, USA, "Security Issues for cloud computing",April-June 2010,international Journal of InformationSecurity and Privacy.

[4] "Security Guidance for Critical Areas of Focus inCloud Computing", April 2009, presented by CloudSecurity Alliance (CSA).

[5] Jinpeng Wei, Xiaolan Zhang, Glenn Ammons,VasanthBala and PengNing, "Managing

security of virtualmachine images in a cloud environment", November2009, Proceedings of the 2009 ACM workshop on Cloudcomputing security pages 91-96.

[6] Miranda Mowbray and Siani Pearson, "A ClientBased Privacy Manager for Cloud computing", June2009,Proceedings of the Fourth International ICSTConference on communication system software andmiddleware.

[7] Flavio Lombardi and Roberto Di Pietro, "TransparentSecurity for Cloud", March 2010, Proceedings of the 2010ACM Symposium on Applied Computing, pages 414-415.

[8] WeichaoWang,Zhiwei Li, Rodney Owens and BharatBhargava, "Secure and Efficient Access to OutsourcedData", November 2009, Proceedings of the ACMworkshop on Cloud computing security, pages 55-65.

[9] Damgrd, Ivan, et al. "Secure key management in the cloud." Cryptographyand Coding.Springer Berlin Heidelberg, 2013.270-289.

[10] Mazieres, David, et al. "Separating key management from file system security." ACM SIGOPS Operating Systems Review 33.5 (1999): 124-139.

[11] Asmuth, Charles, and John Bloom. "A modular approach to key safeguarding." IEEE transactions on information theory 30.2 (1983): 208-210.

[12] Chandramouli, Ramaswamy, Michaela Iorga, and SantoshChokhani. Cryptographic Key Management Issues and Challenges in Cloud Services. SpringerNew York, 2014.

[13] Almorsy, Mohamed, John Grundy, and Ingo Mller. "An analysis of the cloudcomputing security problem." the proc. of the 2010 Asia Pacific Cloud Workshop, Colocated with APSEC2010, Australia. 2010.

[14] Rafaeli, Sandro, and David Hutchison. "A survey of key management forsecure group communication." ACM Computing Surveys (CSUR) 35.3 (2003):309-329.

[15] Kalyani M. ."Cloud Security: Efficient and Reliable Encryption Key Management Crucial for Data Protection". https://spideroak.com/privacypost/cloudsecurity/secure-encryption-key-management-in-the-cloud/.