Volume 5, Issue 4, April 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Combined Approach to Ensure Data Security in Cloud Computing based on HMAC

Supreet Kaur, Dr. Vinay Chopra
Department of Computer Science Engineering
DAVIET, Jalandhar, Punjab, India

Abstract: Cloud computing has become a popular buzzword; it has been widely used to refer to different technologies, services, and concepts. Security is therefore a major element in any cloud computing infrastructure because it is essential to ensure that only authorized access is permitted and secure behavior is expected Security of data in cloud is one of the major issues which acts as an obstacle in the implementation of cloud computing. This paper proposes a highly active and efficient cloud security model. In this paper, a frame work covering of different techniques and specific procedures is proposed that can resourcefully protect the data from the beginning to the end i.e. from the owner to the cloud and then to the user. Our cloud security model plans to keep the most critical data security in cloud computing at different levels. The different levels are: user level, cloud service provider level, third party level and network intruder level. The proposed work draws a conceptual cloud architecture by adopting an encryption algorithm with dynamic small size key to ensure the security and doesn't compromise any information with the cloud server. To maintain data privacy re-encryption is performed with the help of third party and for data integrity Hash Based Message authentication code is generated on encrypted data. The performance methods like better encryption using HMAC and a faster detection of compromise of the clients in cloud environment is possible with the proposed system.

Keywords: Cloud computing; cloud storage server: Encryption; public and private cloud.

I. INTRODUCTION

Cloud computing provides a variety of computing resources , from servers and storage to enterprise applications such as email, security, backup/DR, voice, all delivered over the Internet. The Cloud delivers a hosting environment that is immediate, flexible, scalable, secure, and available – while saving corporations money, time and resources. It is often associated with virtualized infrastructure or hardware on demand, utility computing, IT outsourcing, platform and software as a service, and many other things that now are the focus of the IT industry. It is Internet-centric way of computing. The Internet plays a fundamental role in cloud computing, since it represents either the medium or the platform through which many cloud computing services are delivered and made accessible. This aspect is also reflected in the definition given by Armbrust et al.[2] Cloud computing refers to both the applications delivered as services over the Internet and the hardware and system software in the datacenters that provide those services. Definition proposed by the U.S. National Institute of Standards and Technology (NIST). Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Even though many cloud computing services are freely available for single users and for enterprise class services are delivered according a specific pricing scheme. In this case users subscribe to the service and establish with the service provider a service-level agreement (SLA) defining the quality-of-service parameters under which the services are delivered. The utility-oriented nature of cloud computing is clearly expressed by Buyya et al.[4] A cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers.

1.1 Major models of Cloud Computing

The three major models for deploying and accessing cloud computing environments are public clouds, private/enterprise clouds and hybrid clouds. Public clouds are the most common deployment models in which necessary IT infrastructure (e.g., virtualized datacentres) is established by a third-party service provider that makes it available to any consumer on a subscription basis. Such clouds are appealing to users because they allow users to quickly leverage compute, storage, and application services. In this environment, users' data and applications are deployed on cloud datacentres on the vendor's premises.

Large organizations that own massive computing infrastructures can still benefit from cloud computing by replicating the cloud IT service delivery model in-house. This idea has given birth to the concept of private cloud. Whenever private cloud resources are unable to meet users quality-of-service requirements, hybrid computing systems, partially composed of public cloud resources and privately owned infrastructures, are created to serve the organization's needs. These are often referred as hybrid cloud.

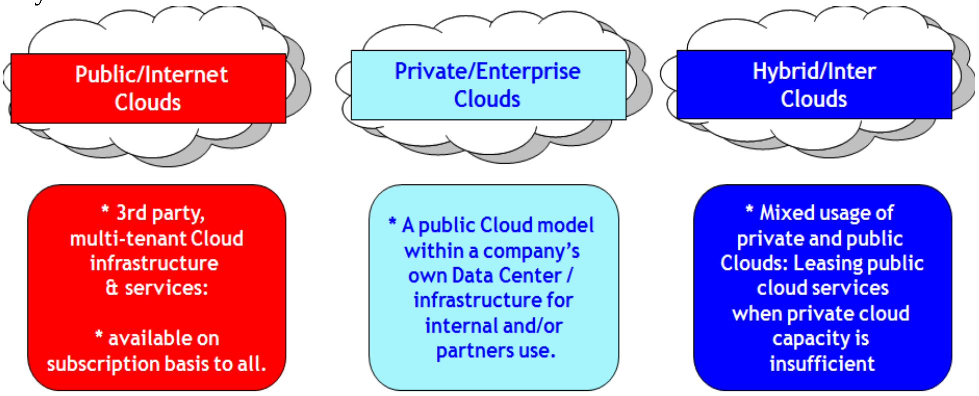
Public/Internet Clouds
Private/Enterprise Clouds
Hybrid/Inter Clouds
* 3rd party, multi-tenant Cloud infrastructure & services:
* available on subscription basis to all.
* A public Cloud model within a company's own Data Center / infrastructure for internal and/or partners use.
* Mixed usage of private and public Clouds: Leasing public cloud services when private cloud capacity is insufficient

Figure 1: Major Models of Cloud Computing

1.2 Cloud Computing Reference Model

Cloud Computing services offerings into three major categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service(SaaS). The model organizes the wide range of cloud computing services into a layered view that walks the computing stack from bottom to top.

In the Figure 1. At the base of the stack, Infrastructure-as-a-Service solutions deliver infrastructure on demand in the form of virtual hardware, storage, and networking. Virtual hardware is utilized to provide compute on demand in the form of virtual machine instances. These are created at users request on the provider's infrastructure, and users are given tools and interfaces to configure the software stack installed in the virtual machine. The pricing model is usually defined in terms of dollars per hour, where the hourly cost is influenced by the characteristics of the virtual hardware. Virtual storage is delivered in the form of raw disk space or object store. The former complements a virtual hardware offering that requires persistent storage. The latter is a more high-level abstraction for storing entities rather than files. Virtual networking identifies the collection of services that manage the networking among virtual instances and their connectivity to the Internet or private networks.

Platform-as-a-Service solutions are the next step in the stack. They deliver scalable and elastic runtime environments on demand and host the execution of applications. These services are backed by a core middleware platform that is responsible for creating the abstract environment where applications are deployed and executed. It is the responsibility of the service provider to provide scalability and to manage fault tolerance, while users are requested to focus on the logic of the application developed by leveraging the provider's APIs and libraries. This approach increases the level of abstraction at which cloud computing is leveraged but also constrains the user in a more controlled environment.

At the top of the stack, Software-as-a-Service solutions provide applications and services on demand. Most of the common functionalities of desktop applications—such as office automation, document management, photo editing, and customer relationship management (CRM) software—are replicated on the provider's infrastructure and made more scalable and accessible through a browser on demand. These applications are shared across multiple users whose interaction is isolated from the other users. The SaaS layer is also the area of social networking Websites, which leverage cloud-based infrastructures to sustain the load generated by their popularity.

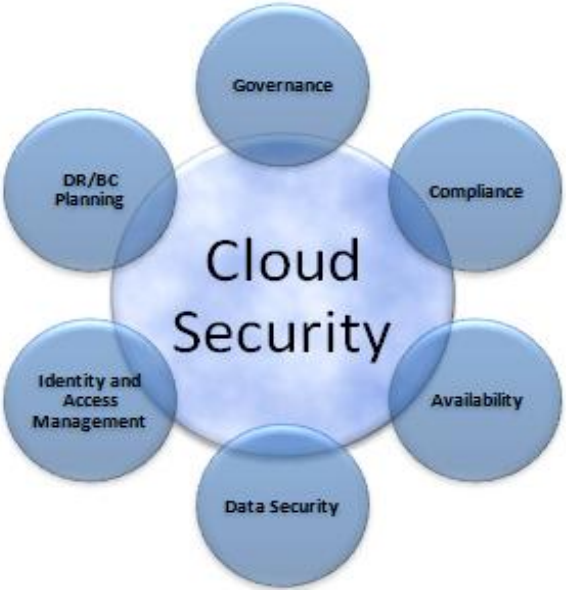

Figure2: Cloud Security Architecture

A cloud computing system consists of a collection of interconnected and virtualized computers dynamically provisioned as one or more unified computing resource(s) through negotiation of service-level agreements (SLAs) between providers and consumers. In cloud computing platforms, resources need to be dynamically re-configured and aggregated via virtualization and consumers' requirements can potentially vary over time and amendments need to be accommodated.

The cloud computing model revolves around three functional units or components as listed below:

1. Cloud Service Provider: It is an entity, which manages Cloud Storage Server (CSS), has significant storage space to preserve the clients' data and high computation power.
2. Client/Owner: Itis an entity, which has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation; it can either be individual consumer or organizations.
3. User: It is a unit, which is registered with the owner and uses the data of owner stored on the cloud. The user can be an owner itself as well.

II. LITERATURE SURVEY

In this paper, I have made a review on my topic data security in cloud computing at different levels by reading different kinds of papers and analyzing different techniques which are being used in these papers published by authors which are discussed as follows:

Varalakshmi et.al[4] describes that data Integrity is essential to secure data in a cloud environment. It is important to ensure that the stored data is neither compromised nor corrupted. Many of existing protocols reveals client's sensitive data by sharing the encryption and decryption keys with the cloud server. Also, entrusting service provider at cloud side is of no use. The proposed work draws conceptual cloud architecture by adopting an encryption algorithm with dynamic small size key to ensure the security and doesn't compromise any information with the cloud server. It involves a third party broker who encrypts the clients' information for ensuring the security, partitioned into multiple segments based on the remaining dynamic storage capacity presents in the VMs of cloud storage servers and store these encrypted segments of the clients' file on the corresponding VMs of the cloud storage providers. It then generate the hash value of the encrypted segments, store and manage these details for verification purpose. The performance measures like better encryption time and a quicker detection of compromise of the clients' files in cloud environment is possible with the proposed system.

Mohamed et.al[5] discuss about data security for both cloud computing and traditional desktop applications. This is to obtain the highest possible level of privacy. Modern Encryption algorithms play the main role in data security of cloud computing. Present an evaluation for selected eight modern encryption techniques namely: RC4, RC6, MARS, AES, DES, 3DES, Two-Fish, and Blowfish at two independent platforms namely; desktop computer and Amazon EC2 Micro Instance cloud computing environment. The evaluation has performed for those encryption algorithms according to randomness testing by using NIST statistical testing in the cloud computing environment. This evaluation uses Pseudo Random Number Generator (PRNG) to determine the most suitable technique and analysis the performance of selected modern encryption techniques. Cryptography algorithms are implemented using Java Cryptography Extensions (JCE).

Xu et.al [6] discusses important issues such as efficient user revocation and key refreshing are not straightforward, which constrains the adoption of Cipher Attribute Based Encryption (CP-ABE) in cloud storage systems. In this paper proposes a dynamic user revocation and key refreshing model for Cipher Attribute Based Encryption (CP-ABE) schemes. A key feature of our model is its generic possibility in general Cipher Attribute Based Encryption (CP-ABE) schemes to refresh the system keys or remove the access from a user without issuing new keys to other users or re-encrypting existing cipher-texts.

Huang et.al [7] proposed a whole service named SSTreasury+ which includes encryption application and cloud storage service. The user's data before uploading to the cloud could be encrypted first to prevent the data to be stolen during transmission or in the cloud storage. In addition, the decryption key which generated by our system can be portable to increase flexibility and convenience. In the backend storages uses existing cloud storage as a backup storage in order to reduce constructing costs. Proposed scheme consists of four entities – SSManager, SSGuard, SSCoffer and user. SSGuard do encryption before uploading and uploaded files store at SSCoffer. File encryption key are encrypted by user public key and store at SSManger. For decryption of file QR code is used. User shows QR code to SSGuard to decrypt files.

Sabahi [8] describes security is one of the most argued-about issues in the cloud computing field; several enterprises look at cloud computing warily due to projected security risks. The risks of compromised security and privacy may be high overall. In this paper, Comparison of the benefits and risks of cloud computing and full evaluation of the viability of cloud computing has been done. Consequently, some issues arise that clients need to consider as they contemplate moving to cloud computing for their businesses. The paper try to summarize reliability, availability, and security issues for cloud computing, propose feasible and available solutions for some of them.

Sur et.al [9] introduce the notion of certificate-based proxy re-encryption as a new cryptographic primitive to effectively support the data confidentiality on the outsourced data in public cloud storage. In particular, give a formal security model for secure certificate-based proxy re-encryption schemes and present a concrete scheme based on bilinear pairing, which enjoys the advantages of certificate-based encryption while providing the functionalities of proxy re-encryption. Scheme has chosen cipher text security in the random oracle model. In cloud computing most prevailing issue is security due to which users fear to adopt cloud. Main concern is with uploaded data to cloud is secure or not. Keeping this concern model has been proposed which provide data security in cloud. It is highly efficient and secure model that can be used to upload data in cloud without fear.

Chandel et.al [10] presents a new scheme for secure cloud creation using RC6 (Rivest cipher 6) encryption algorithm for securing the cloud environment. The results show the performance of proposed technique in public and private cloud. It is most important that a cloud service provider provides safe and secured uses of cloud to the cloud user. The method is useful in for the secured data storage and transaction over cloud.

III. SIMULATION ENVIRONMENT AND RESULTS ANALYSIS

3.1 VMware Workstation 8

VMware Workstation is the most dependable, high-performing and feature-rich virtualization platform for your Windows or Linux PC. It allows one physical PC to run multiple operating systems at the same time. No rebooting or hard-drive partitioning is required.

3.1.1 Working of VMware Workstation

VMware Workstation offers the benefits of multiple PCs without the added expense, physical setup and maintenance. VMware Workstation runs multiple operating systems and their applications in an isolated and secure virtual machine. VMware Workstation can run many virtual machines simultaneously on a single PC.

3.1.2 OpenSSL

The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, full-featured, and Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general purpose cryptography library. The project is managed by a worldwide community of volunteers that use the Internet to communicate, plan, and develop the OpenSSL toolkit and its related documentation. OpenSSL is based on the excellent SSLeay library developed by Eric Young and Tim Hudson.

libssl.a: Implementation of SSLv2, SSLv3, TLSv1 and the required code to support both SSLv2, SSLv3 and TLSv1 in the one server and client.

libcrypto.a: General encryption and X.509 v1/v3 stuff needed by SSL/TLS but not actually logically part of it. It includes routines for the following:

Ciphers libdes – EAY's libdes DES encryption package which was floating around the net for a few years, and was then relicensed as part of SSLeay. It includes 15 'modes/variations' of DES including desx in cbc mode, a fast crypt(3), and routines to read passwords from the keyboard. RC4 encryption, RC2 encryption – 4 different modes, ecb, cbc, cfb and ofb.

Blowfish encryption – 4 different modes, ecb, cbc, cfb and ofb.

IDEA encryption - 4 different modes, ecb, cbc, cfb and ofb.

Digests MD5 and MD2 message digest algorithms, fast implementations, SHA (SHA-0) and SHA-1 message digest algorithms, MDC2 message digest. A DES based hash that is popular on smart cards.

Public Key RSA encryption/decryption/generation. There is no limit on the number of bits. DSA encryption/decryption/generation. There is no limit on the number of bits. Diffie-Hellman key-exchange/key generation. There is no limit on the number of bits.

openssl: A command line tool that can be used for: Creation of RSA, DH and DSA key parameters Creation of X.509 certificates, CSRs and CRLs Calculation of Message Digests , Encryption and Decryption with Ciphers, SSL/TLS Client and Server Tests and Handling of S/MIME signed or encrypted mail.

3.2 Proposed Cloud Model

The model is divided into two phases and consists of user level, cloud service provider level, third party level and network intruder level for secure cloud. The phases are:

1. Phase I (Uploading or Data Storage)
2. Phase II (Downloading or Data Retrieval)

Phase I- Uploading

3.2.1 Key Generation and Distribution

In this security model data owner generate the Keys and divide the keys into key pieces. Owner keeps his piece with it for encryption. Distribute other piece of key to third party for re-encryption and also store key pieces for corresponding to user id for later use.

3.2.2 Re-Encryption and Indexing

For maintaining data privacy, data is encrypted and then uploaded to cloud. In this model owner perform encryption on data with its key piece and give encrypted data to third party. Third party re-encrypt the data with its key piece and then upload to cloud. As it is very complicated to search on encrypted data so indexing of data has been made by owner. Indexing is way to retrieve data faster. As we do not want our data disclosure to cloud provider or network attacker or third party so index is encrypted by owner first with its key piece. Further pass to third party to re-encrypt it before uploading to cloud.

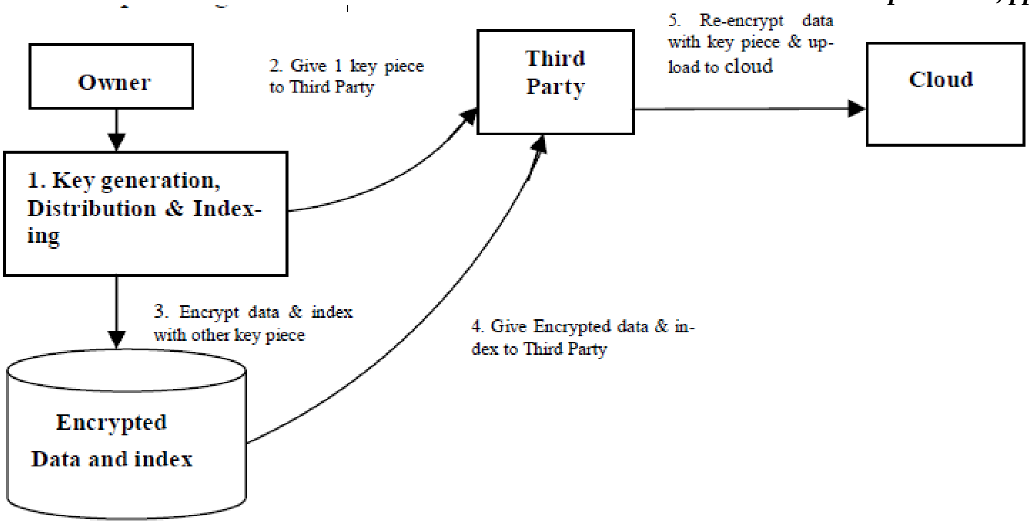
Owner
1. Key generation, Distribution & Indexing
2. Give 1 key piece to Third Party
Third Party
3. Encrypt data & index with other key piece
Encrypted Data and index
4. Give Encrypted data & index to Third Party
5. Re-encrypt data with key piece & upload to cloud
Cloud

Figure 3. Re-Encryption and Indexing

3.2.3 Hash message authentication code (HMAC)

Hash message authentication code (HMAC), a mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative FIPS-approved cryptographic hash function, in combination with a shared secret key. The cryptographic strength of HMAC depends on the properties of the underlying hash function. (MSE).

An HMAC function is used by the message sender to produce a value (the MAC) that is formed by condensing the secret key and the message input. The MAC is typically sent to the message receiver along with the message. The receiver computes the MAC on the received message using the same key and HMAC function as was used by the sender, and compares the result computed with the received MAC. If the two values match, the message has been correctly received, and the receiver is assured that the sender is a member of the community of users that share the key.

HMAC shall be used in combination with a cryptographic hash function specified in a Federal Information Processing Standard (FIPS). HMAC uses a secret key for the calculation and verification of the MACs. The main goals behind the HMAC construction [RFC2104] are:

- To use available hash functions without modifications; in particular, hash functions that perform well in software, and for which code is freely and widely available.
- To preserve the original performance of the hash function without incurring a significant degradation.
- To use and handle keys in a simple way.
- To have a well-understood cryptographic analysis of the strength of the authentication mechanism based on reasonable assumptions on the underlying hash function, and
- To allow for easy replace ability of the underlying hash function in the event that faster or more secure hash functions are later available.

HMAC Parameters and Symbols

H MAC uses the following parameters:
B-Block size (in bytes) of the input to the FIPS-approved hash function; e.g., for
SHA-1, B= 64.
H- FIPS-approved hash function, e.g., FIPS 180-1, Secure Hash Algorithm-1 (SHA-1).
Ipad- Inner pad; the byte x’36’ repeated B times.
K- Secret key shared between the originator and the intended receiver(s).
K0-The key K with zeros appended to form a B byte key.
L- Block size (in bytes) of the output of the FIPS-approved hash function; for SHA-1,L= 20.
Opad- Outer pad; the byte x’5c’ repeated B times.
T- The number of bytes of MAC.
Text- The data on which the HMAC is calculated; the length of the data is n bits, where the maximum value for n depends on the hash algorithm used.
X’N’-Hexadecimal notation, where each ‘N’ represents 4 binary bits.
||-Concatenation and
Exclusive-Or operation.

3.2.4 HMAC for Data Integrity

Although data is in encrypted format but there is fear of data being tampered during transit or on storage of data? To resolve this fear of data tampering hash-based message authentication code (HMAC) is calculated after data encryption. Basically, HMAC is process to use cryptographic hash function for message in the form of data authentication. It is encrypted by owner then re-encrypted by third party and uploaded along with data to cloud.

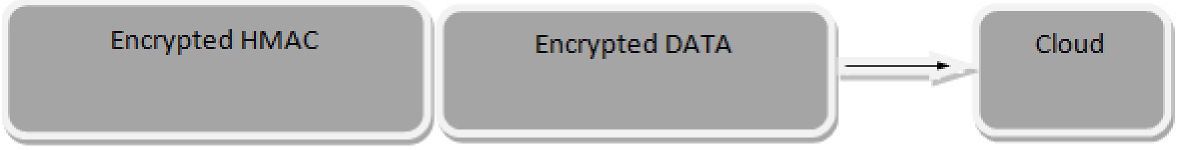

Figure 4. HMAC for Data Integrity

3.2.5 Role-based Dual User Authentication

When the data is needed by data owner or user they have to download the data from cloud. If the data is required by data owner then it gets direct access to cloud as an administrator of cloud. Data owner have full privilege of cloud so it can add or revoke user and also give role-based access to its data. If data is required by user then user have undergo dual verification which is carried by third party and further verified by data owner. Owner gives list of authorized user with login id and password to third party.. Data owner verify user using smartcard if verified then owner provide cloud login id, password, information about Message Authentication code (MAC) and passcode of private key in encrypted format. This encrypted data is decrypted using smartcard. User sends the identity of user to cloud so that cloud service provider allow user to login to cloud to access data. Now user login to cloud to access data. There is role based access to data i.e. user can update, read or delete etc. according to data owner wish.

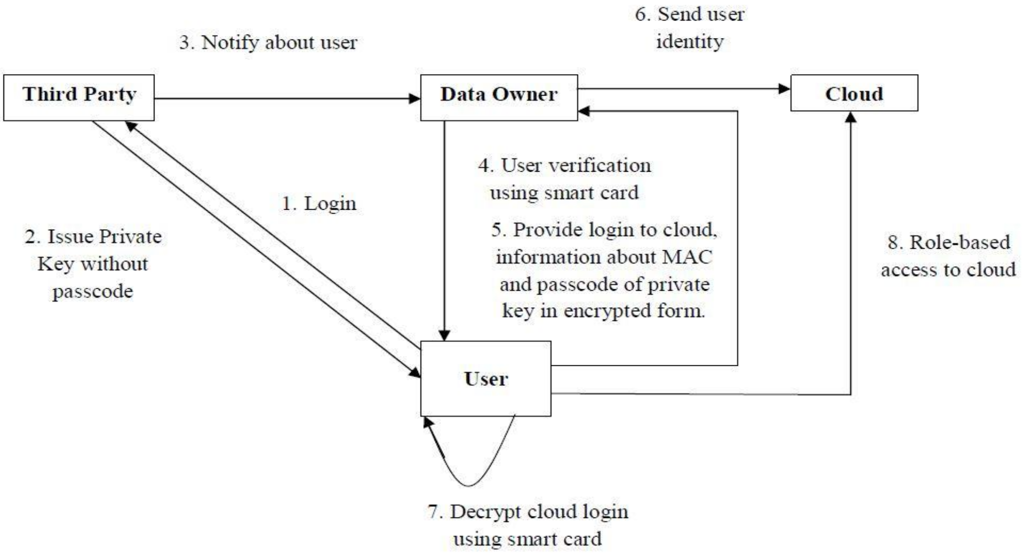
6. Send user identity
3. Notify about user
Third Party
Data Owner
Cloud
4. User verification using smart card
1. Login
5. Provide login to cloud, information about MAC and passcode of private key in encrypted form.
2. Issue Private Key without passcode
8. Role-based access to cloud
User
7. Decrypt cloud login using smart card

Figure 5. Role-Based Dual User Authentication

IV. RESULTS

The proposed model has been evaluated with implementation. This model has been verified using OpenSSL tool [17] in red hat Linux and own Cloud [18]. Figure 6 shows that after implementation various security parameters i.e. Key Management, user roles, HMAC and dual user authentication. HMAC provides less data security than user roles and this user roles provide less security than Key Management technique. Basically if we combine all security parameters i.e. HMAC, classification of data, key Management and dual user authentication, it results in highly secured approach for uploading data to cloud. It results in highly secured proposed model used in various cloud environment which is denoted as peak value as shown in figure 6.

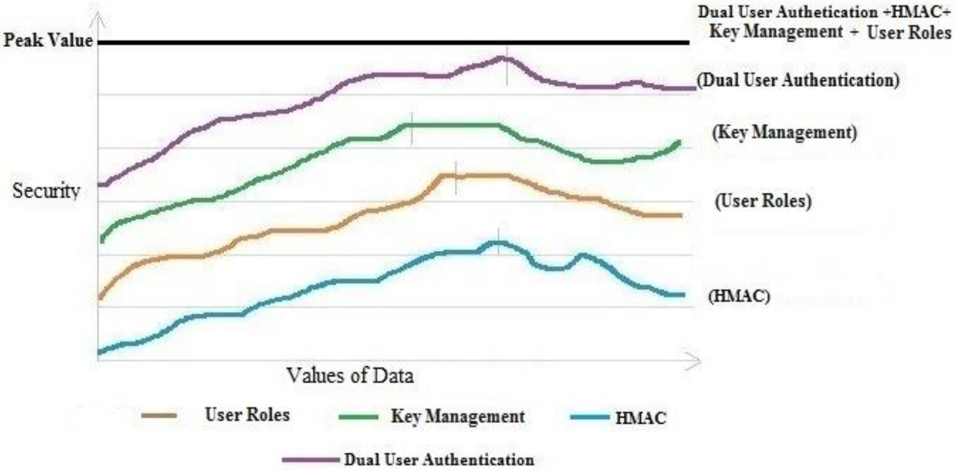

Figure 6. Security Evaluation

V. CONCLUSION

Data security is checked at different levels that are user level, cloud service provider level, network intruder level as well as at cloud service provider level. The proposed technique provides a way to protect the data, check the integrity and authentication by different levels such as user level, cloud service provider level, third party level and network intruder level and highly secure to adopt in real life while storing and retrieving data from cloud. In cloud computing most dominant issue is security due to which users fear to approve cloud. The main apprehension is with uploaded data to cloud is secure or not. Keeping this concern model has been proposed which provide data security in cloud. The proposed HMAC model gives outstanding results as compared to different types of cloud network models. This model provides data confidentiality, user roles, HMAC and key management. It is highly efficient and secure model that can be used to upload data in cloud without fear. This model is suitable for various areas of secure cloud development such as public cloud, private cloud.

REFERENCES

[1] Mrinal RajkumarBuyya, Christian Vecchiola and S. ThamaraiSelvi, Mastering Cloud Computing Foundations and Applications Programming.Morgan Kaufmann, USA.

[2] Jing Huang Jing, LI Renfa, and TangZhuo, "*The Research of the Data Security for Cloud Disk Based on the Hadoop Framework*", IEEE,2013.

[3] Sandeep K. Sood, "*A Combined Approach to Ensure Data Security in Cloud Computing*", Submitted to Journal of Network and Computer Applications, Elsevier Ltd, 2012.

[4] P.Varalakshmi, Hamsavardhini Deventhiran, "Integrity Checking for Cloud Environment Using Encryption Algorithm", IEEE, 2012.

[5] Eman M.Mohamed ,Sherif EI-Etriby, "Randomness Testing of Modem Encryption Techniques in Cloud Environment", 8th International Conference on Informatics and Systems, 2012.

[6] Zhiqian Xu, Keith M. Martin, "Dynamic User Revocation and Key Refresh-ing for Attribute-Based Encryption in Cloud Storage", International Conference on Trust, Security and Privacy in Computing and Communications, IEEE,2012.

[7] Kuan-Ying Huang, Guo-Heng Luo,Shyan-Ming Yuan, "SSTreasury+: A Secure and Elastic Cloud Data Encryption System", International Conference on Genetic and Evolutionary Computing, IEEE,2012.

[8] Farzad Sabahi, "Cloud Computing Security Threats and Responses",IEEE,2011

[9] Chul Sur, Youngho Park, Sang Uk Shin, Changho Seo , Kyung Hyune Rhee, "Certificate-Based Proxy Re-Encryption for Public Cloud Storage", International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IEEE,2013.

[10] Narendra Chandel, Sanjay Mishra, Neetesh Gupta, AmitSinhal, "Creation of Secure Cloud Environment using RC6", IEEE,2013.

[11] Eman M.Mohamed and Sherif EI-Etriby, "*Randomness Testing of Modem Encryption Techniques in Cloud Environment*", 8th International Conference on Informatics and Systems, 2012.

[12] Zhiqian Xu and Keith M. Martin, "*Dynamic User Revocation and Key Refreshing for Attribute-Based Encryption in Cloud Storage*", International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, 2012.

[13] Kuan-Ying Huang, Guo-Heng Luo and Shyan-Ming Yuan, "*SSTreasury+: A Secure and* E*lastic Cloud Data Encryption System*", International Conference on Genetic and Evolutionary Computing, IEEE(2012).

[14] Chul Sur, Youngho Park, Sang Uk Shin, Changho Seo and Kyung Hyune Rhee, "Certificate-Based Proxy Re-Encryption for Public Cloud Storage", International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IEEE, 2013.

[15] NarendraChandel, Sanjay Mishra, Neetesh Gupta and AmitSinhal, "Creation of Secure Cloud Environment using RC6", IEEE,2013.

[16] Miranda Mowbray and Siani Pearson, "Protecting Personal Information in Cloud Computing", Springer Verlag, 2012

[17] Chun-I Fan and Shi-Yuan Huang, "Controllable Privacy Preserving Search Based on Symmetric Predicate Encryption in Cloud Storage", International Conference on Cyber Enabled Distributed Computing and Knowledge Discovery, IEEE, 2011.

[18] Keiko Hashizume, David G Rosado2, Eduardo Fernández-Medina2 and Eduardo B Fernandez, "An analysis of security issues for cloud computing", Springer,2013.

[19] Swetha Reddy Lenkala, KaiqiXiong and Sachin Shetty, "Security Risk Assessment of Cloud Carrier", IEEE,2013.

[20] Marten van Dijk and Ari Juels, "On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing", ACM,2010.

[21] Balachandra Reddy Kandukuri, Ramakrishna Paturi V and AtanuRakshit, "Cloud Security Issues", IEEE 2009