iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** XII **Month of publication:** December 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 3 Issue XII, December 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

To Analysis the Data Security in Cloud Computing At User, Cloud Server and Third Party Level Using HMAC

Anamika Sirohi[1], Vishal Shrivastava[2]
[1,2]*Department of Computer Science and Engineering,*
ARYA college of Engineering and IT, Jaipur, Rajasthan, India.

Abstract-Cloud computing is an upcoming uprising in computer science and information technology industry because of its performance, security, accessibility, low cost and many other amenities. Cloud security is a multifaceted and highly complex issue. Today security is main issue in cloud. All industry is moving toward cloud computing so security of data on cloud is essential so different security algorithm (like DES, AES, RSA etc.) has been implemented. The cloud computing model revolves around three functional units or components like Cloud Service Provider (manages Cloud Storage Server), Client/Owner (for data maintenance and computation) and User (registered with the owner and uses the data of owner stored on the cloud.)In this paper, we consider to realize efficient and secure data sharing in proposed cloud, that is, a trusted private cloud and a public cloud are assumed in our system. Data security is major issue prevailing in world of cloud computing and to overcome that issue the model has been proposed. Proposed model has been organized using HMAC algorithm that it give throughout data security in cloud computing at different levels. The model is highly secure and protects the data during transit as well as data at rest. It also secures the data against all threats i.e. insight as well as outsight.
Keywords: Cloud computing; Cryptographic process; Hash MAC; Public and Private Cloud.

I. INTRODUCTION

Cloud computing is an extension of grid computing and distributed computing, which is a software concept indeed [1], it works through variety of technologies such as software technologies, integration, management, and the use of various hardware resources. Cloud computing is realized mainly through the virtual technology [2]. Cloud computing is often considered the successor of grid computing. In reality, it embodies aspects of all these three major technologies. Computing clouds are deployed in large datacenters hosted by a single organization that provides services to others. Clouds are characterized by the fact of having virtually infinite capacity, being tolerant to failures, and being always on, as in the case of mainframes. In many cases, the computing nodes that form the infrastructure of computing clouds are commodity machines, as in the case of clusters. The services made available by a cloud vendor are consumed on a pay-per-use basis, and clouds fully implement the utility vision introduced by grid computing.

Although cloud computing has been rapidly developed, user's concerns about data security are the main obstacles that impede cloud computing from widely deployed. These concerns, ranging from security and privacy of outsourced data to unauthorized access to shared data, are originated from the fact that cloud servers are very likely to be in a different trusted domain from that of the cloud users. To eliminate these concerns, a natural solution is to encrypt data by client before outsourcing. However, encryption may destroy some implicit attributes of original data and render the encrypted data difficult to be utilized. This fact would cause most of data operations impossible. For example, if a user wants to retrieve documents containing a certain keyword, he/she has to download all the data and decrypt it locally, causing huge communication and computation overhead. The security problems of cloud disk are not only the traditional problems but also new

problems in cloud computing. [3] Described the security threats and challenges of the cloud computing with its three basic patterns (Saas, Paas, Iaas). [4][5][6] Analyzed and summarized the threats being faced from different aspects. Cloud disk's weak security mainly occurs in the following aspects:

Transmission security: data in transmission process may be intercepted, but the data transmission is not working

with the strong encryption protection measures.

Access control: access control authority is weak, the user data stored in the clouds without setting access authority, the user lost

Volume 3 Issue XII, December 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

absolute right to monitor.

Data storage: user upload data after the clouds, it is likely to be distributive stored, users do not know the specific position where the data is stored. And the confidential data and non-confidential data stored is not classified, which may cause the leakage of data.

Cloud computing represents a distributing computing mechanism that by the utilize of the high speed network, data processing is moved from private PC or servers to the remote computer clusters (big data centers owned by the cloud service providers), any user has a potential super computer at hand and can access the data and get the computing capability at any time, from anywhere, you only need to pay for the resources which you have used, don't care about who provide the resources and in what way.

Actually, clouds [3] are Internet-based and it tries to disguise complexity for clients. Cloud computing refers to both the applications delivered as services over the Internet and the hardware and software in the datacenters that provide those services. Cloud providers use virtualization technologies combined with self-service abilities for computing resources via network infrastructure. In cloud environments, several kinds of virtual machines are hosted on the same physical server as infrastructure. In cloud, costumers must only pay for what they use and have not to pay for local resources which they need to such as storage or infrastructure.

Three major milestones have led to cloud computing: mainframe computing, cluster computing and grid computing. Mainframes: These were the first examples of large computational facilities leveraging multiple processing units. Mainframes were powerful, highly reliable computers specialized for large data movement and massive input/output (I/O) operations. They were mostly used by large organizations for bulk data processing tasks such as online transactions, enterprise resource planning, and other operations involving the processing of significant amounts of data. Clusters: Cluster computing started as a low-cost alternative to the use of mainframes and supercomputers. The technology advancement that created faster and more powerful mainframes and supercomputers eventually generated an increased availability of cheap commodity machines as a side effect. Starting in the 1980s, clusters become the standard technology for parallel and high-performance computing.

Data Security concerns with sensitivity of data stored to different types of cloud environment. This major issue is barrier to different range of people and barred them from adopting cloud. To resolve this problem related to sensitivity of data a security model based on verification of data at different security level that i.e. cloud service provider level, network intruder level, user level or third party level has been proposed. In this model, deployment standard algorithm Rivest-Shamir-Adleman(RSA) to encrypt data before sourcing it to cloud and also made the scheme for dual authentication of users.

Initially, organization store sensitive data internally protected with different security means but now days many organization started storing their data towards cloud. Still some organization lags behind in adoption of cloud due to security. Data security is most prominent issue of cloud computing. When the users upload their data to cloud then they have no direct hold over data. They only have to trust the cloud service provider for data security. When these providers are untrusted then data is unsafe. Data owner cannot trust anyone while outsourcing its data. Its main role is to protect data by themselves. On the basis of main responsibility of data owner towards data security an approach of data owner centric protection has been designed in form of model. Data is protected against third party, network intruder and cloud service provider. Re-encryption, HMAC and Identity based user authentication techniques has been used in this model. Proposed model give data owner control over its data storage at cloud and make them feel free without any fear of losing their data at cloud.

Figure 1: Cloud Computing

Cloud computing can effectively address the computing needs of users of versatile scales ranging from an individual to large organizations. This paper proposes a cloud computing model which effectively handles the issues related to cloud data security including confidentiality, integrity, authentication and authorization. Our model handles both external as well as internal data security threats. It makes use of a hybrid cloud architecture using both private as well as public cloud. A dual layer of security is used in our model. One is authentication based on username and password and the other, the condition that the user should possess the key to decrypt a password stored at the cloud, without which the password filled by the user and the password stored cannot be compared. This completes the user authentication phase of our security model. For user authorization, a user role is associated with each user and stored at the cloud database. The user can only perform operations with respect to this role. This role is the one determined by the entity known as data owner in our model. Also, for processing data at the cloud and keeping it safe from the cloud, a cryptographic process is proposed.

A. 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.

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.

II. RELATED WORK

The Cloud is a terminology with a long history in telephony, which has in the past decade, been adopted as a metaphor for internet based services, with a common depiction in network diagrams as a cloud outline. The underlying concept dates back to 1960 when John McCarthy opinion that "Computation may someday be organized as a public utility"; indeed it shares characteristics with service bureaus which date back to the 1960s. The term cloud had already come into commercial use in the early 1990s to refer to large Asynchronous Transfer Mode (ATM) networks. By the turn of the 21ist century, the term "cloud computing" had started to appear, although major focus at this time was on Software as a Service (SaaS). In 1999, salesforce.com was established by Marc Benioff, Parker Harris. They applied many technologies of consumer web sites like Google and Yahoo! to business applications. They also provided the concept of "On demand" and "SaaS" with their real business and successful customers. IBM extended these concepts in 2001, as detailed in the Autonomic Computing Manifesto, which describes advanced automation techniques such as self-monitoring, self-healing, self-configuring and self optimizing in the management of complex IT systems with heterogeneous storage, servers, applications, networks, security mechanisms and other system elements that can be virtualized across an enterprise. Amazon.com played a

key role in the development of cloud computing by modernizing their data centers. It found that the new cloud architecture resulted in significant internal efficiency improvements and providing access to their systems by way of Amazon Web Services in 2005 on a utility computing basis. 2007 saw increased activity with Google, IBM and a number of universities embarking on a large scale cloud computing research project, around the time the term started gaining popularity in the mainstream press. In August 2008, Gartner Research observed that "organizations are switching from company-owned hardware and software assets to per-use service-based models". The projected

shift to cloud computing will result in dramatic growth in IT products in some areas and in significant reductions in

other areas. Despite all the hope of gaining maximum advantage from this cloud computing, it seems to have born with security and management concerns, which time to time hinders its growth. For this, lot of research work has been done to secure the data in cloud computing (primary concern) from every perspective, but everything seems to face a new challenge as soon as it is employed.

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:

Sood et.al [3] proposed approach to ensure data security in cloud computing. In this proposed approach key generation, encryption, indexing of data, user authentication and data integrity is performed by data owner itself. Unfortunately, there will be high overhead on data owner and hence time consuming too. Thilakanathan et.al [4] proposed scheme using proxy re-encryption for security of data. In this scheme data owner encrypt the data using his key piece then proxy encrypt the data using his key piece. Decryption is also carried in similar fashion. However, if proxy is fake then data becomes insecure. Sharma et.al.[5] discussed different service model of cloud computing and highlights the key security issues, challenges and solution at different layers of cloud. Jingwei et.al.[6] discussed efficient model for secure data sharing in cloud. The proposed model consists of user, authority, hybrid cloud and owner. The data is stored at private cloud and data shared is encrypted Encryption technology used is keyword-based encryption. The keys are generated by authority and given to user group for encryption and decryption. The model has some issues like if authority is fake then data is insecure and also it is costly to use the model. Sood et.al [7] proposed the scheme to highly secure the data at cloud. They provided improved data security by using concept of hybrid cloud. In this scheme the sensitive data i.e. about 3%-5% is stored at private cloud and rest of the data at public cloud. This model is applicable to organisations whose sensitive data is about 3%-5%. If the sensitive data increases then this model will prove to be expensive. The white papers [8] of many organisations describes three types of data security models in cloud. First model

Consists of key generation and encryption on data is performed by data owner itself. However this model results in high overhead for data owner. Second model describes encryption performed by data owner and key generation by cloud service provider. Unfortunately, cloud service provider is fake then data is insecure hands. Third model encryption and key generation is control by cloud service provider. If cloud service provider is fake then data is endangered. Hwang et.al [9] proposed business model in which encryption/decryption service and storage as a service of user data were separated i.e. they were not provided by single operator. After encryption/decryption performed system should delete all the data. Varalakshmi et.al [10] proposed system consists of three entities cloud broker, client and cloud storage. Broker handles encryption, hash key, decryption and local database management. According to cloud space available the client files are partitioned into segment and hash values of segments has been generated. When the client needs its file it sends request to broker then broker download the file, partition the file into segments and then calculate the hash values. For checking the data integrity hash values before uploading to the after downloading are matched.

III. SIMULATION ENVIRONMENT

The proposed model combines the benefits of private and public clouds. It effectively uses hash codes, symmetric encryption, user specific roles, a cryptographic process and dual verification in order to enhance the overall security of the data that is stored on the cloud. The proposed cloud security model has various aspects, each having a specific purpose and all collectively contributing in making our proposed model superior to various other proposed models. Cloud security [11] is a multifaceted and highly complex issue. The data owners' especially of large organizations fear possible data misuse by the cloud provider without their knowledge. This concern is a major deterrent in the path of shifting operations to the cloud. Any kind of security and privacy violation is critical and can produce dire consequences. The main stumbling block concern is data security at different levels. Client may range from an individual to big organization. Data Security at different levels concerns with two aspects: External level security and Internal Level security. External level security deals with data insecure against third party, cloud service provider or network intruder. Internal

level security deals with authorized users or employee of an organization. Data Security concerns with sensitivity of data stored to different types of cloud environment. This major issue is barrier to different range of people and barred them from adopting cloud. As soon as cloud security issues are further organized and strict regulations and governance for cloud operation are in position so that more and more business owners will feel safe to opt for cloud computing.

Proposed model has been organized in such manner that it give throughout data security in cloud computing at different levels. The different threat levels are: user level, cloud service provider level, third party level and network intruder level. Data is protected against all level of threats. In proposed model data remains private during transit as well as data at rest and from untrusted parities. The goals of proposed model are to provide:

Security at User Level: Data remain secure from dishonest employee of organization or intruder.

Security at cloud service provider: Data remain private from untrusted or fake cloud provider.

Security at Third Party level: Data security against untrustworthy third party if involved data protection.

Network Intruder: Data remains secure during transit or over network form intruders.

Data Confidentiality: Data secrecy is maintained throughout the model i.e. data at rest or over network or during transit.

Data Privacy: Data Leakage is not there without authentication so data remains private.

Overhead: As model is based on owner centric approach so all the overhead will on data owner but this model has been proposed such that data owner overhead should be less.

Data Integrity: To check data tampering over the network by the network intruder during transit of data is kept main concern in model.

In order to secure data encryption is technique used in proposed model. Encryption of data is carried according sensitivity of data. The data is classified as: Type0 and Type1.

Type0 – Data is not sensitive i.e. no need to encrypt data. Data is directly uploaded to cloud without encryption.

Type1 – Data is sensitive and need to encrypt data before uploading to cloud.

Type0 or Type1 depends on response of data owner. For Type1 data follow Data Encryption Mechanism.

A. Data Encryption Mechanism

Data Encryption is carried by two entities: third party and data owner. Third party acts as Key Management Infrastructure (KMI). Key Management Infrastructure consists of key generation and key storage. Main responsibility of third party is to generate asymmetric keys and give required key to data owner for encrypting data. After data encryption the required Key i.e. public key is returned back to key storage. Key storage protects, maintain and store the key. Key maintenance and protection includes providing keys only after verification of required users. Keys are encrypted with passcode by data owner. The standard algorithms Rivest-Shamir-Adleman (RSA) used for generating keys and data encryption.

Volume 3 Issue XII, December 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

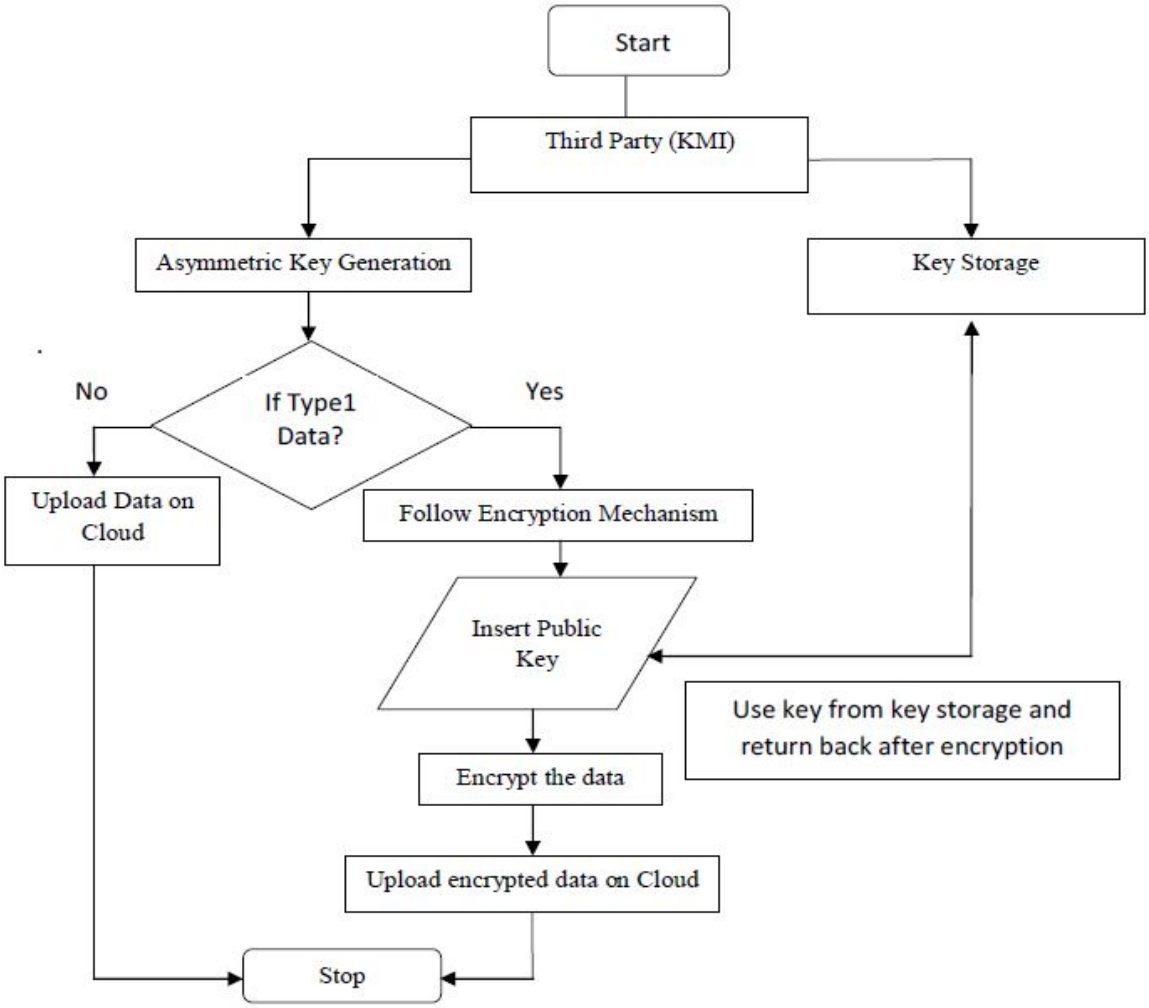


Figure 2. Data Encryption Mechanism

B. Message Authentication Code

Message Authentication Code is also encrypted in the same manner as data by following data encryption mechanism. Encrypted data and Message Authentication Code are uploaded to cloud. The standard Message-Digest5 (MD5) algorithm is used for calculating Message Authentication Code for data integrity.

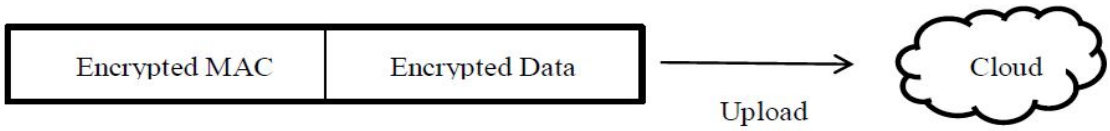


Figure 3: Uploading Data to Cloud

C. Message Authentication Code Verification

Now user has downloaded encrypted data and Message Authentication Code. Users decrypt Message Authentication Code first and calculate Message Authentication Code on encrypted data. If both the Message Authentication Code i.e. decrypted Message Authentication Code and calculated Message Authentication Code are same then decrypt the data and use it otherwise report to data owner about Message Authentication Code mismatch.

Volume 3 Issue XII, December 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

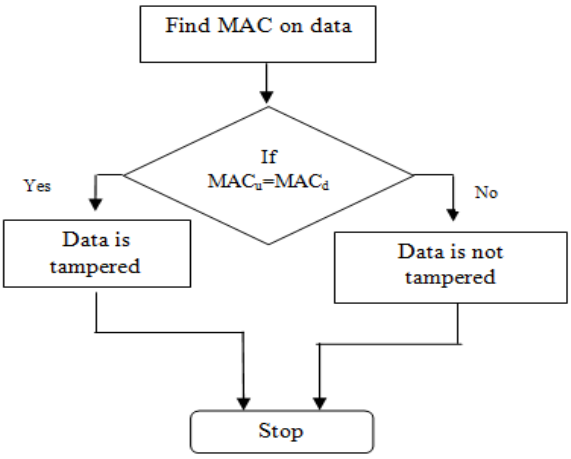


Figure 4: Data Integrity

D. Encipher and Indexing

Based on classification of data, corresponding encipher technique is used. Data owner identifies the type of data. If data is of type 1 then encryption is used otherwise obfuscation is used. Before these techniques, indexing is performed. After indexing as well as data applied according to technique are uploaded to cloud.

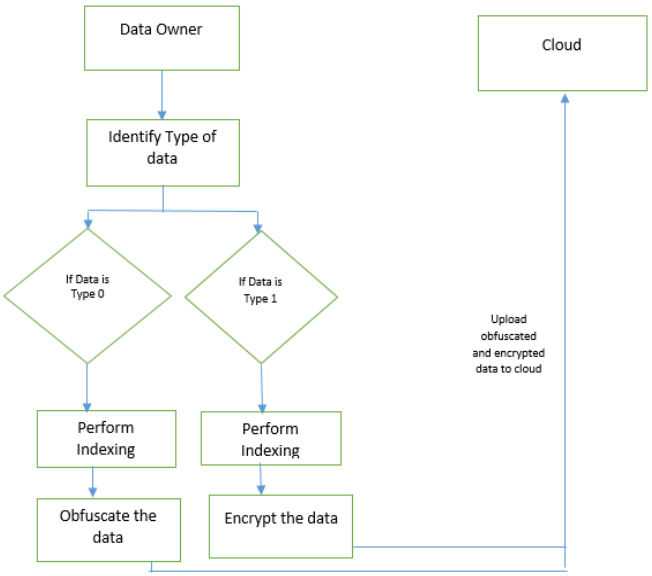


Figure 5. Encipher and Indexing

E. 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. VMware Workstation maps the physical hardware resources to the virtual machine's resources, so each virtual machine has its own CPU, memory, disks, I/O devices and more. Each virtual machine is the full equivalent of a traditional PC. VMware Workstation installs just like a standard program on a Windows or Linux PC. VMware Workstation is recognized for its broad operating system support, rich user experience, a comprehensive feature set and high performance. VMware Workstation is designed for professionals that rely on virtual machines to get their job done.

Volume 3 Issue XII, December 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

F. OpenSSL

OpenSSL is based on the excellent SSLeay library developed by Eric Young and Tim Hudson. The OpenSSL toolkit is licensed under an Apache-style licence, which basically means that you are free to get and use it for commercial and non-commercial purposes subject to some simple license conditions. Secure Sockets Layer is an application-level protocol which was developed by the Netscape Corporation for the purpose of transmitting sensitive information, such as Credit Card details, via the Internet. SSL works by using a private key to encrypt data transferred over the SSL-enabled connection, thus thwarting eavesdropping of the information. The most popular use of SSL is in conjunction with web browsing (using the HTTP protocol), but many network applications can benefit from using SSL. By convention, URLs that require an SSL connection start with https: instead of http. The OpenSSL toolkit includes:

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.

G. Message Authentication Code (MAC) Generation

Step1: Message Authentication Code (MAC) is generated on encrypted data using Message-Digest algorithm. Openssl dgst –md5 filename

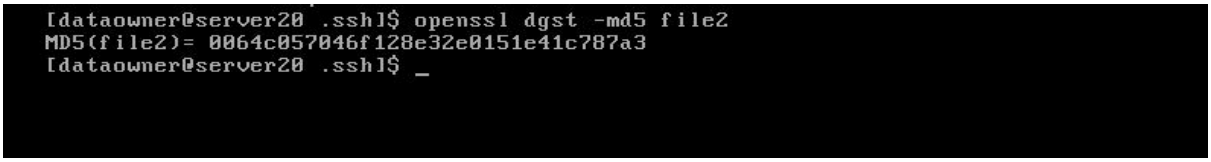


Figure 6: Message Authentication Code (MAC) Generation

Step2: Encrypt the md5 output same as done before in data encryption openssl rsautl –encrypt –pubin –inkey PUBLIC_KEY.pem –in md5 –out md

H. Role Based Access To Cloud

Step1: Data-owner have full control over cloud i.e. data owner act as administrator. Data-owner can add new user, delete user and revoke user anytime.

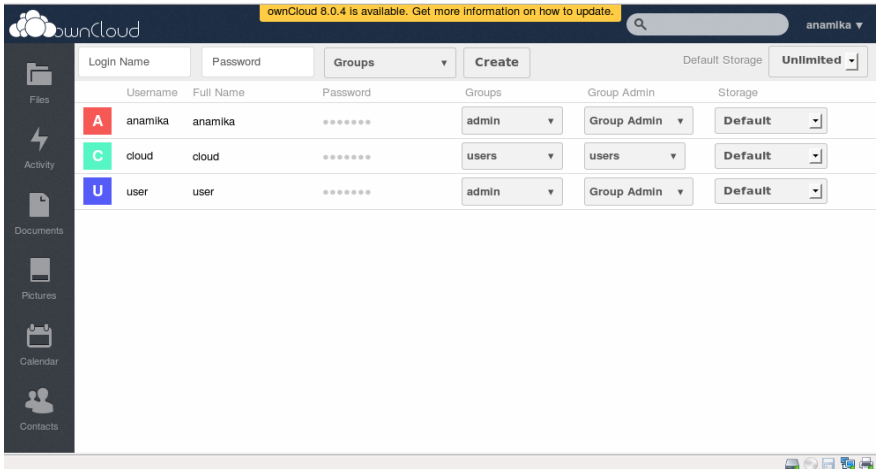


Figure 7: User Creation and Deletion by data owner on cloud

Step2: User decrypts the md file for data integrity and generates message authentication code on encrypted file2. Matches both MAC, if same then decrypt the file2 and use the data otherwise report to data owner.

Volume 3 Issue XII, December 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

```
[anamika@server21 ~]$ ls
Desktop    Downloads  k1  login  Music      plaintext         Public     Videos
Documents  file2      k2  md     Pictures   PRIVATE KEYS.pem  Templates
[anamika@server21 ~]$ openssl rsautl -decrypt -inkey PRIVATE_KEYS.pem -in md -out m
d1
Enter pass phrase for PRIVATE_KEYS.pem:
[anamika@server21 ~]$ ls
Desktop    Downloads  k1  login  md1    Pictures   PRIVATE_KEYS.pem  Templates
Documents  file2      k2  md     Music  plaintext  Public            Videos
[anamika@server21 ~]$ cat md1
MD5=0064c0570046f128e32e0151e41c787a3
[anamika@server21 ~]$ openssl dgst -md5 file2
MD5(file2)= 0064c057046f128e32e0151e41c787a3
[anamika@server21 ~]$ openssl rsautl -decrypt -inkey PRIVATE_KEYS.pem -in file2 -out file
Enter pass phrase for PRIVATE_KEYS.pem:
[anamika@server21 ~]$ cat file1
cat: file1: No such file or directory
[anamika@server21 ~]$ cat file
hi hws u
[anamika@server21 ~]$
```

Figure 8: File Decryption and Message Authenication Code matching by User

IV. RESULTS ANALYSIS

Proposed model has been organized so that it give throughout data security in cloud computing at different levels. Comparative Analysis between proposed model and other exiting security model has been illustrated below:

Table 6.1: Comparative Analysis

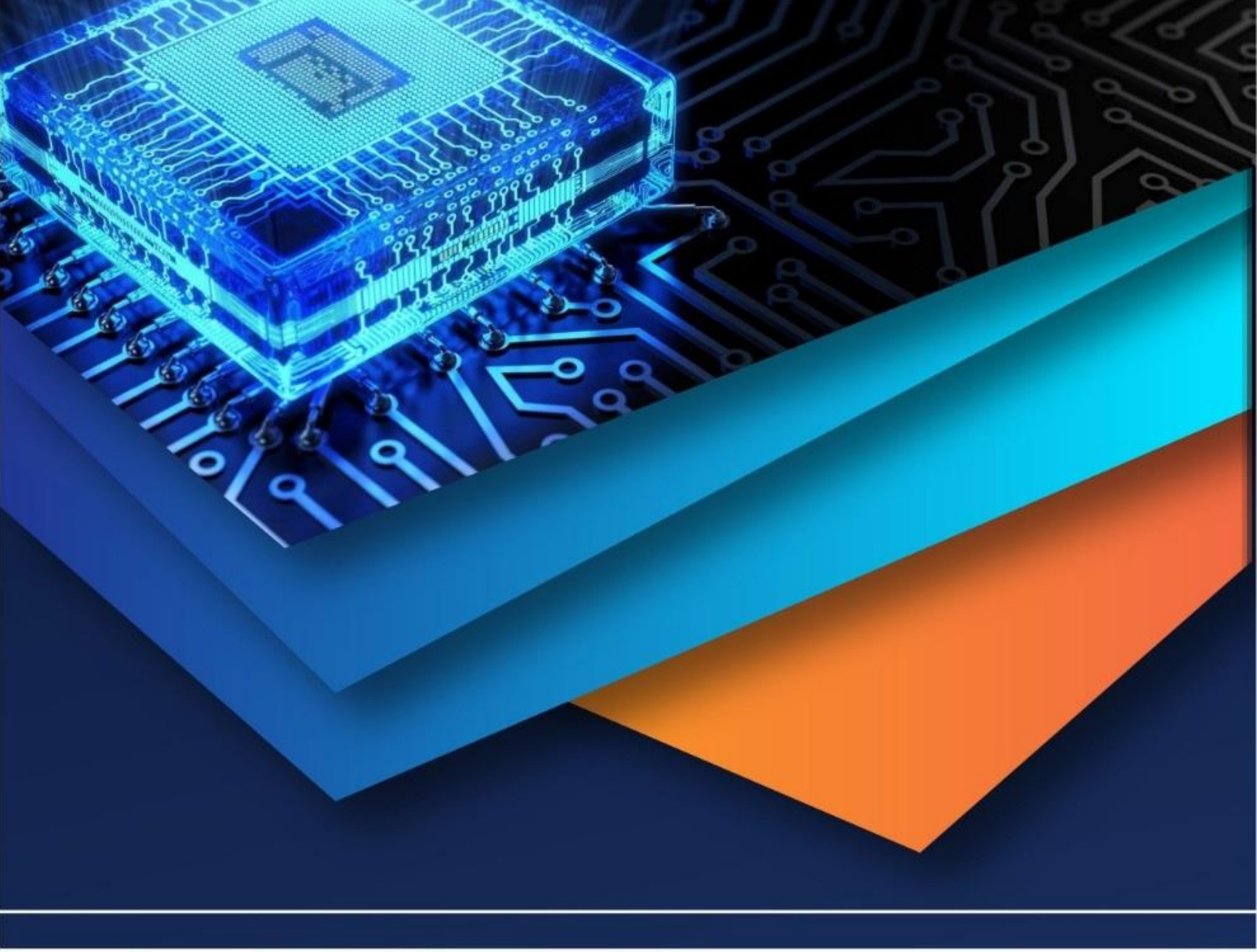
Parameters	Sood et al [7]	Jing et al [6]	Sood et al [11]	Thilakanthan et al [8]	Li et al [10]	White papers [12]	Proposed model
Availability	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Integrity	Yes	No	Yes	No	No	May be	Yes
Cost Effective	Yes	Yes	No	Yes	No	Yes	Yes
Authentication	Yes	No	Yes	Yes	Yes	Yes	Yes
Efficient	No	No	No	No	No	No	Yes

V. CONCLUSION & FUTURE SCOPE

Proposed Model is achieving data security at cloud computing. It is secure from all threats prevailing and harming the data. It provides security when data at rest as well as during transmission and from untrusted parities .This model provides data confidentiality, rapid availability on demand, data Integrity and minimum overhead to data owner, cost effective and efficient. Proposed Model has been designed in a way that biggest issue of data security in cloud computing has been resolved and user fearlessly adopt cloud. By comparing with rest of the models it has been concluded that the proposed model is highly secure, data remains private from untrusted parities and free from internal and as well as external threats. The model is highly secure and protects the data during transit as well as data at rest. It also secures the data against all threats i.e. insight as well as outsight.

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] Danan Thilakanatha, Shiping Chen,Surya Nepal, Rafael A. Calvo and Leila Alem, "A platform for secure monitoring and sharing of generic health data in the Cloud", Elsevier Ltd, 2013.
[5] Pardeep Sharma, Sandeep K. Sood, Sumeet Kaur, "Cloud Implementation Issues and What to Compute on Cloud", International Journal of Advances in Computer Networks and its Security, vol.1, no. 1, pp. 130-135, 2011.
[6] Jingwei Li, Jin Li, Zheli Liu and Chunfu Jia "Enabling efficient and secure data sharing in cloud computing" Concurrency Computat.:Pract Exper.,John Wiley & Sons, Ltd.,2013.
[7] Sandeep K. Sood, "A Highly Secure Hybrid Security model for Data Security at Cloud ", Submitted to Security and Communication Networks, John Wiley and Sons (Interscience), Special Issue on Trust and Security in Cloud Computing, 2012.
[8] Amazon Web Services.: "Encrypting Data at Rest in AWS", https://aws.amazon.com/whitepapers.
[9] Jing-Jang Hwang, Hung-Kai Chuang, Yi-Chang Hsu and Chien-Hsing Wu, "A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service", National Science Council of Taiwan Government.
[10] P.Varalakshmi and Hamsavardhini Deventhiran, "Integrity Checking for Cloud Environment Using Encryption Algorithm", IEEE, 2012.
[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 Elastic 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



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY