E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

SECURE CLOUD SIMULATION USING TRIPLE DES

[A Perfect Solution on Infrastructure as a Service]

Nagesh M.Wankhade, Kiran A. Sahare, Prof. Vaishali G. Bhujade
Department of computer Engineering
Bapurao Deshmukh college of Engineering, Sewagram, Wardha-442001
nageshwankhade1@gmail.com, krnsahare@gmail.com, vaishali.bhujade@rediffmail.com

ABSTRACT— this model is already quite common for consumer apps like email and photo sharing, and for certain business applications. In this paper we present a way to secure the data using different compression and encryption algorithms and to hide its location from the users that stores and retrieves it. As with the Internet, on-demand applications have grown so ubiquitous that almost every business user interacts with at least one, whether it's an email service, a Web conferencing application, or a file hosting system. The data is stored at multiple places over the information space (over the Internet). It sounds similar to file hosting websites which stores the data that is being uploaded by different users and can be retrieved using proper authentication. The only difference is that the system for which paper is presented is an application based system like which will run on the clients own system. This application will allow users to upload file of different formats with security features including Encryption and Compression. The uploaded files can be accessed from anywhere using the application which is provided. We believe this system serves as a foundation for future work in integrating and securing information sources across the World Wide Web.

***Keywords — IaaS, SaaS, PaaS, Encryption, Decryption, Compression, Decompression, File hosting services*.**

I. INTRODUCTION

Typically, the applications used for file transfers and storage is web based and hence requires web browsers to upload the files on servers. But the problem arises the time required and the limits of a browser to run properly till the file is transferred. This application will allow the uploading of files without disturbing other processes and at the same time user may be able to work in web browsers without hanging up the uploads. The file size varies according the premium or free users. The application uses compression as well as encryption algorithms for file security and therefore takes more time to upload a file. The key to encryption can be taken by user or a default key for users can be taken according to the design of application. After the implementation of the application, it needs to be hosted so that it is available to the end user. For this purpose various hosting services including cloud are available.

1. CLOUD COMPUTING

Software, Platform, and Infrastructure as a Service are the three main service delivery models for Cloud Computing. Those models are accessible as a service over the Internet. The Cloud services are made available as pay-as-you-go where users pay only for the resources they actually use for a specific time, unlike traditional services, e.g., web hosting. Furthermore, the pricing for cloud services generally varies according to QoS requirements. The cloud deployment models, based on their relationship to the enterprise, are classified to private, public, and hybrid. Public Cloud services are sold as Utility Computing, while private Cloud refers to internal datacenters of an enterprise which are not available to the general public.

Examples of emerging Cloud Computing Platforms include Microsoft Azure1, Amazon EC22, and Google App Engine3. The confusion between Cloud and Service Oriented Architecture (SOA) has prompted us to discuss this issue and offer a brief comparison between them. SOA and Cloud Computing can be considered complementary services sharing common characteristics. Hence, if SOA is a set of principles and methodologies designed to facilitate systems integration and communication regardless of development languages and platforms, Cloud Computing, on the other hand, is designed to enable companies to utilize massive capacities instantly without having to invest into new infrastructure, train new staff, or license new software. Cloud

E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

Computing allows small and medium-sized businesses to completely outsource their datacenter infrastructure, as well as large companies that need huge load capacities without building larger expensive datacenters internally. Cloud Computing employs the virtualization technology to offer a secure, scalable, shared, and manageable environment. In short, regardless of the difference in designing purposes and the dependency of Cloud Computing on virtualization technology, Cloud Computing might intersect with SOA in Components as a Service, e.g., SOA via Web Service standards. Therefore, Cloud Computing and SOA can be pursued independently, or concurrently as complementary activities to provide an outstanding business.

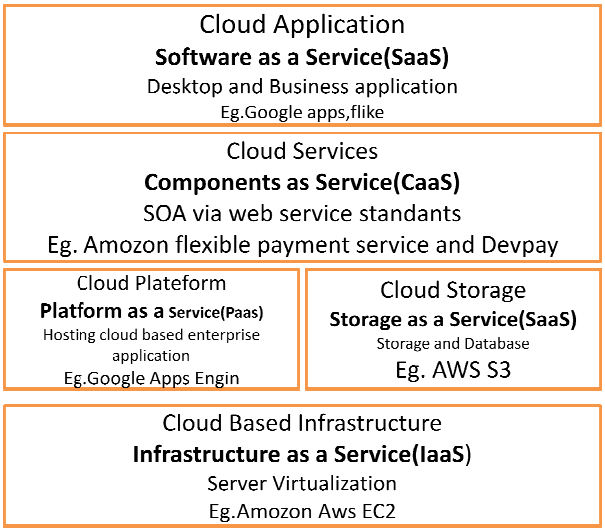

Fig 1. Cloud computing model

Cloud Computing depends primarily on IaaS layer to provide cheap and pay-as-you-go processing power, data storage, and other shared resources. This paper presents a detailed and precise study of IaaS security and privacy concerns. We have investigated security for each IaaS component: Service Level Agreement (SLA), Utility Computing (UC), Platform Virtualization, Networks & Internet Connectivity, and Computer Hardware. Furthermore, Cloud software's security that impact on IaaS and on the whole Cloud Computing is presented. We are interested in the IaaS delivery model because it is the foundation of all other delivery models, and a lack of security in this layer affects the other delivery models that are built upon IaaS layer.

2. *CLOUD COMPUTNG SECURITY ISSUES*

Data Integrity

When a data is on a cloud anyone from any location can access those data's from the cloud. Cloud does not differentiate between a sensitive data from a common data thus enabling anyone to access those sensitive data's. Thus there is a lack of data integrity in cloud computing

Data Theft

Most of the cloud Vendors instead of acquiring a server tries to lease a server from other service providers because they are cost affective and flexible for operation. The customer doesn't know about those things, there is a high possibility that the data can be stolen from the external server by a malicious user.

3. ADVANTAGES OF CLOUD AS SOLUTION

Saves time. Businesses that utilize software programs for their management needs are disadvantaged, because of the time needed to get new programs to operate at functional levels. By turning to cloud computing, you avoid

E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

these hassles. You simply need access to a computer with Internet to view the information you need.
Less glitch. Applications serviced through cloud computing require fewer versions. Upgrades are needed less frequently and are typically managed by data centers. Often, businesses experience problems with software because they are not designed to be used with similar applications.

In the rest of the paper, Section II describes literature review, Section III describes the proposed scheme and Section IV concludes the Paper.

II. LITERATURE REVIEW

Qin Liu, Guojun Wang, and Jie Wu [1], there exists a user hierarchy. In which the user at upper level share secure cloud storage service with the entire lower level user. The principle used for encryption is hierarchical identity based encryption algorithm which takes the number as well as the public keys of recipients as input. This input is presented to the user at upper level .The upper level user encrypts the file only once and store only one copy in "cloud" and then send to all lower level recipients and this encrypted file decrypted by each lower level user with the help of their own private key.

Uma Somani, Kanika Lakhani, Manish Mundra [2], We are emphasizing more focus on the problem in cloud computing like security and data, files system, backups, network traffic and host security. To overcome this problem we used digital signature with RSA algorithm. Sender takes the documents from the cloud then it is broken into number of lines with the help of hashing algorithm and these lines are called Message Digest. After this, sender encrypts Message digest with his private keys and this result is Digital Signature. Now, sender encrypts the digitally signed Sign with receivers public key and receiver decrypts it with his private key and sender public key .for verification as well ,all this using RSA algorithm.

Ashutosh Kumar Dubey , Animesh Kumar Dube, Mayank Namdev, Shiv Shakti Shrivastava [3].we have focused on the increased degree of connectivity and the amount of data which requires larger infrastructures with dynamic load and access balancing. This results in used of cloud computing but there are some security concerns in cloud computing environment. So, we proposed a new cloud computing environment where we approach a new cloud computing environment which is controlled by both the client and cloud environment administrator. For this purpose, we apply RSA and MD5 algorithm. When the cloud user upload data in cloud environment, the data is uploaded in encrypted form using RSA algorithm and cloud admin can decrypt using their own private key. For updating the data in cloud environment, admin request the user for source key. Cloud user sends a secure key with a message digest tag for updating the data. If any outsider performs a change in the key the tag bit is also changed which indicate the key is not secure and correct.

Xiang Tana, Bo Aib [4].we have emphasizing on use of cloud computing technology in railway department to achieve the Sharing of railway information resources and to improve the capacity of information processing. But with cloud computing several difficulties also have been faced. One of such difficulties is cloud computing security. This paper will explore the status of development of cloud computing security analyze the data privacy, security auditing, data monitoring and other challenges that the cloud computing security faced with. So we have proposed a cloud computing security reference framework for rail way system.

Arthur Resumed, Henry C. H. Chen, Yang Tang, Patrick P. C. Lee, and John C. S. Lui [5].we laid emphasis on cloud storage that enables individuals and enter prisons to outcome the storage of data backups to remote cloud providers at a low cost. We present Fade Version a secure cloud backup system that serves as a security layer on top of today's cloud storage services. It follows the standard version control backup design that eliminates storage of redundant data across the different version of backups. Above all fade version applies cryptographic protection to data backup as well as enables assured deletion .i.e in the cloud client can assuredly delete.

Eman M.Mohamed and Sherif EI-Etriby [6]. Proposed Cloud computing becomes the next generation architecture of IT Enterprise. Clouds are massively complex systems. They can be reduced to simple primitives, that are replicated thousands of times, and common functional units. The complexity of cloud computing create many issues related to security as well as all aspects of Cloud computing. One of the most important issues is data security.

E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

We 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.

Cloud computing is based on five attributes

- Multi-tenancy (shared resources): Cloud computing is based on a business model in which resources are shared.
- Elasticity: Users can rapidly increase and decrease their computing resources as needed.
- Self-provisioning of resources: Users self-provision resources, such as additional systems (processing Capability, software, storage) and network resources
- Massive scalability: Cloud computing provides the ability to scale to tens of thousands of systems, as well as the ability to massively scale bandwidth and storage space.
- Pay as you used: Users to pay for only the resources they actually use and for only the time they require them.

The evaluation of eight modem encryption techniques show that RC6, AES, DES and Blowfish results were slightly better than other-encryption methods, Which the pervious methods have more than the P - value in a very safe area. Finally, AES encryption method is a suitable algorithm for the Amazon EC2 environment, but Blowfish and DES are more suitable when we focus on time of encryption method. On the selected encryption algorithms, sequence complexity values will exceed its threshold values for randomness only in Random Excursions Variant test and Excursions test. These two tests are not applicable, which there are insufficient number of cycles. On the selected encryption algorithms, sequence complexity values will exceed its threshold values for randomness only in Random Excursions Variant test and Random Excursions test. These two tests are not applicable, which there are insufficient number of cycles.

1. SECURITY MECHANISMS

Encryption of data plays a vital role in the real time environment to keep the data out of reach of unauthorized people, such that it is not altered and tampered and sending the in spitted format is most secured way to transfer the data through the network.

1.1. ENCRYPTION ALGORITHMS

Data Encryption Standard (DES)

It is one of the most widely accepted, publicly available cryptographic systems today. It was developed by IBM in the 1970s but was later adopted by the US government as a national bureau of standards as an official Federal Information Processing Standard (FIPS) for the United States in 1976. It uses a 56-bit key to encrypt the 64 bit block size data. It processes 64-bit inputs into 64-bit cipher-text and algorithm performs 16 iterations [1, 18].

Triple DES (TDES)

Triple DES (aka 3DES, 3-DES, TDES) is based on the DES (Data Encryption Standard) algorithm; it was developed in 1998 and derived from DES. Therefore it is very easy to modify existing software to use Triple DES. It also has the advantage of proven reliability and a longer key length that eliminates many of the attacks that can be used to reduce the amount of time it takes to break DES. However, even this more powerful version of DES may not be strong enough to protect data for very much longer. The DES algorithm itself has become obsolete and is in need of replacement. To this end, the National Institute of Standards and Technology (NIST) ratified the Advanced Encryption Standard (AES) as a replacement for DES. Triple DES has been endorsed by NIST as a temporary standard to be used until AES was finished. The AES is at least as strong as Triple DES and much faster. Many security systems use both Triple DES and AES. AES is the default algorithm on most systems. Triple DES will be kept around for compatibility reasons for many years after that.

Triple DES is another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. In Stealth, you simply type in the entire 192-bit (24 character) key rather than entering each of the three keys individually. The Triple DES DLL then breaks the user-provided key into three sub keys, padding the keys if necessary so they are each 64 bits long. The procedure for encryption is exactly the same as regular DES, but it

E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

is repeated three times, hence the name Triple DES. The data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key.

Triple DES runs three times slower than DES, but is much more secure if used properly. The procedure for decrypting something is the same as the procedure for encryption, except it is executed in reverse. Like DES, data is encrypted and decrypted in 64-bit chunks. Although the input key for DES is 64 bits long, the actual key used by DES is only 56 bits in length. The least significant (right-most) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56 bits. This means that the effective key strength for Triple DES is actually 168 bits because each of the three keys contains 8 parity bits that are not used during the encryption process. It applies the DES cipher algorithm three times to each of the data blocks. It has a key size of 168 bits but provides at most 112 bits of security remaining 56 bits are utilized in the keying options.

The block size used in the algorithm is 64 bits and 48 DES equivalent rounds have been used to encrypt the data. The security of TDES is effective but the main limitation of the standard is that 56 bits are not actually used for the encryption.

Message Digest (MD5) Algorithm

The MD5 message-digest algorithm is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value. MD5 has been utilized in a wide variety of security applications, and is also commonly used to check data integrity. MD5 was designed by Ron Rivest in 1991 to replace an earlier hash function, MD4. An MD5 hash value is typically expressed as a hexadecimal number, 32 digits long.

The security of the MD5 hash function is severely compromised. A collision attack exists that can find collisions within seconds on a computer with a 2.6 GHz Pentium 4 processor (complexity of $2^{24.1}$). Further, there is also a chosen-prefix collision attack that can produce a collision for two chosen arbitrarily different inputs within hours, using off-the-shelf computing hardware (complexity 2^{39}) The ability to find collisions has been greatly aided by the use of off-the-shelf GPUs. On an NVIDIA GeForce 8400GS graphics processor, 16–18 million hashes per second can be computed. An NVIDIA GeForce 8800 Ultra can calculate more than 200 million hashes per second. These hash and collision attacks have been demonstrated in the public in various situations, including colliding document files and digital certificates.

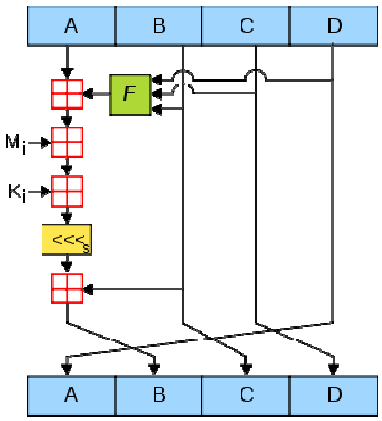

Figure 2. One MD5 operation.

E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

MD5 consists of 64 of these operations, grouped in four rounds of 16 operations. *F* is a nonlinear function; one function is used in each round. M_i denotes a 32-bit block of the message input, and K_{id} denotes a 32-bit constant, different for each operation. $\lll_s$ *denotes* a left bit rotation by *s* places; *s* varies for each operation. $\boxplus$ denotes addition modulo 2^{32}.

MD5 processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks (sixteen 32-bit words); the message is padded so that its length is divisible by 512. The padding works as follows: first a single bit, 1, is appended to the end of the message. This is followed by as many zeros as are required to bring the length of the message up to 64 bits less than a multiple of 512. The remaining bits are filled up with 64 bits representing the length of the original message, modulo 2^{64}.
The main MD5 algorithm operates on a 128-bit state, divided into four 32-bit words, denoted *A*, *B*, *C* and *D*. These are initialized to certain fixed constants. The main algorithm then uses each 512-bit message block in turn to modify the state. The processing of a message block consists of four similar stages, termed *rounds*; each round is composed of 16 similar operations based on a non-linear function *F*, modular addition, and left rotation. Figure 1 illustrates one operation within a round. There are four possible functions *F*; a different one is used in each round:

Level of Protection

The techniques have been compared on the basis of that how much:

- CPU time would be required by a machine for a given processing speed to generate the key, encrypt and decrypt the data.
- The amount of memory required to hold the data in encryption process.
- Number of users accommodated by the model.
- Time required by the model to recover the data in case of key failure.

III. PROPOSED WORK

As application developers, our job now is to figure out which platform components are going to allow us to build all of these features. The system architecture shows the core design of the application. The system serves the purpose of file hosting and hence requires a server that holds data. Multiple clients can logged in to the server and share files. The system should work in the flow as shown below:

- User should register on website and download the application and install it.
- User has to log in through the application and performs operation user wants.
- User should register on website and download the application and install it.
- Database is in 3rd normal form.
- Data compression by using zipping upto 70%.
- Data size is 4MB with full binary support.
- Existing system is updated from 3 tiers to N tier that improve the security.
- 256 bit AES encryption algorithm is used for file security.
- Proposed system is multicloud compatible that is it is independent of backend services and infrastructure
- All the quality attributes are taken into consideration and it comprises of all persistent systems standards

E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

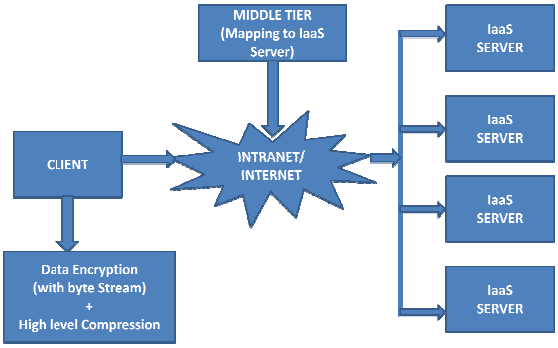

Fig 3. System Architecture

1. USE OF JAVA NETWORK LAUNCH PROTOCOL

The Java Network Launch Protocol enables an application to be launched on a client desktop by using resources that are hosted on a remote web server. Java Plug-in software and Java Web Start software are considered JNLP clients because they can launch remotely hosted applets and applications on a client desktop. See Java Network Launching Protocol and API Specification Change Log for details. Recent improvements in deployment technologies enable us to launch rich Internet applications (RIAs) by using JNLP. Both applets and Java Web Start applications can be launched by using this protocol. RIAs that are launched by using JNLP also have access to JNLP APIs. These JNLP APIs allow the RIAs to access the client desktop with the user's permission. JNLP is enabled by a RIA's JNLP file. The JNLP file describes the RIA. The JNLP file specifies the name of the main JAR file, the version of Java Runtime Environment software that is required to run the RIA, name and display information, optional packages, runtime parameters, system properties, and so on.

2. MATHEMATICAL MODEL

2.1. Calculating Upload Time

G= {f | f Î group of files ^ f Î (*.*)}

Let t be the time required for uploading the file to server.

For private Files:

t=E (f) +C (f) +U (f)

For public Files:

t=U (f)

Where,

E (f) is time required for Encryption using AES 256.

C (f) is time required for ZIP compression

U (f) is time required for uploading files through network.

2.2. Calculating Download Time

G= {f | f Î group of files ^ f Î (*.*)}

Let t be the time required for downloading the file from server.

E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

For private Files:

t=DE (f) +DC (f) +D (f)

For public Files:

t=D (f)

Where,

DE (f) is time required for Decryption using AES 256.

DC (f) is time required for ZIP decompression

D (f) is time required for downloading files through network.

IV. CONCLUSION AND FUTURE WORK

IaaS is the foundation layer of the Cloud Computing delivery model that consists of multiple components and technologies. Each component in Cloud infrastructure has its vulnerability which might impact the whole Cloud's computing security. Cloud Computing business grows rapidly despite security concerns, so collaborations between Cloud parties would assist in overcoming security challenges and promote secure Cloud Computing services. In this paper, we investigated the security challenges that associated with IaaS implementation and deployment. The security issues presented here concern the security of each IaaS component in addition to recent proposed solutions. Our future research vision will focus on two directions to provide confidentiality, integrity, and secure Infrastructure management for IaaS service. First, extending techniques such as proposed in TCCP into IaaS layer to improve confidentiality and integrity of VMs. Second, integrating TCCP with secure resources management schemes to get more controlled isolation environment. Finally, a prototype will be implemented to demonstrate the system feasibility and performance.

REFERENCES

[1] Qin Liu, Guojun Wang, and Jie Wu"Efficient Sharing of Secure Cloud Storage Services" 2010 .10th IEEE International Conference on Computer and Information Technology (CIT - 2010).
[2] Uma Somani, Kanika Lakhani, Manish Mundra"Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing" 2010 IEEE 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).
[3] Ashutosh Kumar Dubey 1, Animesh Kumar Dubey 2, Mayank Namdev3, Shiv Shakti Shrivastava4 "Cloud-User Security Based on R SA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment "in 2011.
[4] Xiang Tana, Bo Aib"The Issues of Cloud Computing Security in High-speed Railway "in 2011.
[5] Arthur Rahumed, Henry C. H. Chen, Yang Tang, Patrick P. C. Lee, and John C. S. Lui "A Secure Cloud Backup System with Assured Deletion and Version Control" 2011 International Conference on Parallel Processing Workshops.
[6] Eman M.Mohamed and Sherif EI-Etriby "Randomness Testing of Modem Encryption Techniques in Cloud Environment" in year 2008