ISSN 2277-3061

A NOVEL APPROACH OF HYBRID MODEL OF ENCRYPTION ALGORITHMS AND FRAGMENTATION TO ENSURE CLOUD SECURITY

Amandeep Kaur [(1)], Mr. Pawan Luthra [(2)]
[(1)] Research Scholar, Department of Computer Science & Engineering, SBSSTC, Ferozepur, Punjab.
amanthind59@gmail.com
[(2)] Assistant Professor, Department of Computer Science & Engineering, SBSSTC, Ferozepur, Punjab.
pawanluthra81@gmail.com

ABSTRACT

Cloud is a term used as a metaphor for the wide area networks (like internet) or any such large networked environment. It came partly from the cloud-like symbol used to represent the complexities of the networks in the schematic diagrams. It represents all the complexities of the network which may include everything from cables, routers, servers, data centers and all such other devices. Cloud based systems saves data off multiple organizations on shared hardware systems. Data segregation is done by encrypting data of users, but encryption is not complete solution. In the proposed work, we have tried to increase the cloud security by using encryption algorithms like AES and RSA along with OTP authentication. We have also fragmented the data by using data distribution at the server end.

Keywords

Cloud Computing; Cloud Security; Confidentiality; MD5; Encryption; OTP; AES; RSA; Fragmentation; Replication.

Council for Innovative Research
Peer Review Research Publishing System

Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY

Vol. 14, No. 12

www.ijctonline.com, editorijctonline@gmail.com

INTRODUCTION

As per the definition provided by the National Institute for Standards and Technology (NIST) (Badger et al., 2011), “Cloud Computing is a model for enabling 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”. It represents a paradigm shift in information technology many of us are likely to see in our lifetime. While the customers are excited by the opportunities to reduce the capital costs, and the chance to divest themselves of infrastructure management and focus on core competencies, and above all the agility offered by the on-demand provisioning of computing, there are issues and challenges which need to be addressed before a ubiquitous adoption may happen.

Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. There are four basic cloud delivery models, as outlined by NIST (Badger et al., 2011), based on who provides the cloud services. The agencies may employ one model or a combination of different models for efficient and optimized delivery of applications and business services.

CLOUD COMPUTING SECURITY AND PRIVACY ISSUES

This section addresses the core theme i.e., the security and privacy-related challenges in cloud computing. There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure. Furthermore, virtualization paradigm in cloud computing leads to several security concerns. For example, mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. In addition, resource allocation and memory management algorithms have to be secure. Finally, data mining techniques may be applicable for malware detection in the clouds – an approach which is usually adopted in intrusion detection systems (IDSs).

For securing data at rest, cryptographic encryption mechanisms are certainly the best options. The hard drive manufacturers are now shipping self-encrypting drives that implement trusted storage standards of the trusted computing group (Trusted Computing Group’s White Paper, 2010). These self-encrypting drives build encryption hardware into the drive, providing automated encryption with minimal cost or performance impact. Although software encryption can also be used for protecting data, it makes the process slower and less secure since it may be possible for an adversary to steal the encryption key from the machine without being detected.

Encryption is the best option for securing data in transit as well. In addition, authentication and integrity protection mechanisms ensure that data only goes where the customer wants it to go and it is not modified in transit.

Strong authentication is a mandatory requirement for any cloud deployment. User authentication is the primary basis for access control. In the cloud environment, authentication and access control are more important than ever since the cloud and all of its data are accessible to anyone over the Internet. The trusted computing group’s (TCG’s) IF-MAP standard allows for real-time communication between a cloud service provider and the customer about authorized users and other security issues. When a user’s access privilege is revoked or reassigned, the customer’s identity management system can notify the cloud provider in real-time so that the user’s cloud access can be modified or revoked within a very short span of time.

One of the more obvious cloud concerns is separation between a cloud provider’s users (who may be competing companies or even hackers) to avoid inadvertent or intentional access to sensitive information. Typically a cloud provider would use virtual machines (VMs) and a hypervisor to separate customers. Technologies are currently available that can provide significant security improvements for VMs and virtual network separation. In addition, the trusted platform module (TPM) can provide hardware-based verification of hypervisor and VM integrity and thereby ensure strong network separation and security.

Legal and regulatory issues are extremely important in cloud computing that have security implications. To verify that a cloud provider has strong policies and practices that address legal and regulatory issues, each customer must have its legal and regulatory experts inspect cloud provider’s policies and practices to ensure their adequacy. The issues to be considered in this regard include data security and export, compliance, auditing, data retention and destruction, and legal discovery. In the areas of data retention and deletion, trusted storage and trusted platform module access techniques can play a key role in limiting access to sensitive and critical data.

As part of expecting the unexpected, customers need to plan for the possibility of cloud provider security breaches or user misbehavior. An automated response o at least automated notification is the best solution for this purpose. The IF-MAP (Metadata Access protocol) of the trusted computing group (TCG) specification enables the integration of different security systems and provides real-time notifications of incidents and of user misbehavior.

RESEARCH METHODOLOGY

A 3-step mechanism is used to provide the security at the cloud server.

ISSN 2277-3061

1. Secure Authentication using OTP: Client logins at the cloud provider by providing userId and password. In addition to that, OTP's have been used in this research work. A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device. The cloud provider generates the OTP based on user's information and sends it to the client via email.

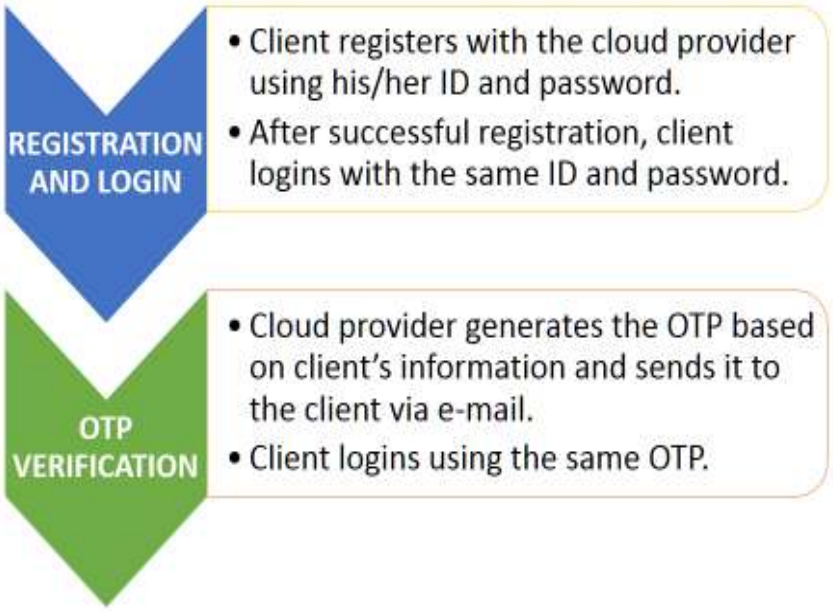

Figure 1. Cloud Authentication using OTP.

1. Client registers with cloud provider by providing his/her details like username, id and password.
2. The cloud provider stores the details in the database and informs the user about his/her successful registration.
3. Afterwards, the user will login by entering his/her ID and password. The cloud providers verifies the user and generates the OTP
4. One-Time password is generated using MD5 algorithm. It's a hashing algorithm and cloud provider will send the generated OTP to the client via e-mail.
5. Client will again login using the OTP provided by the cloud provider.

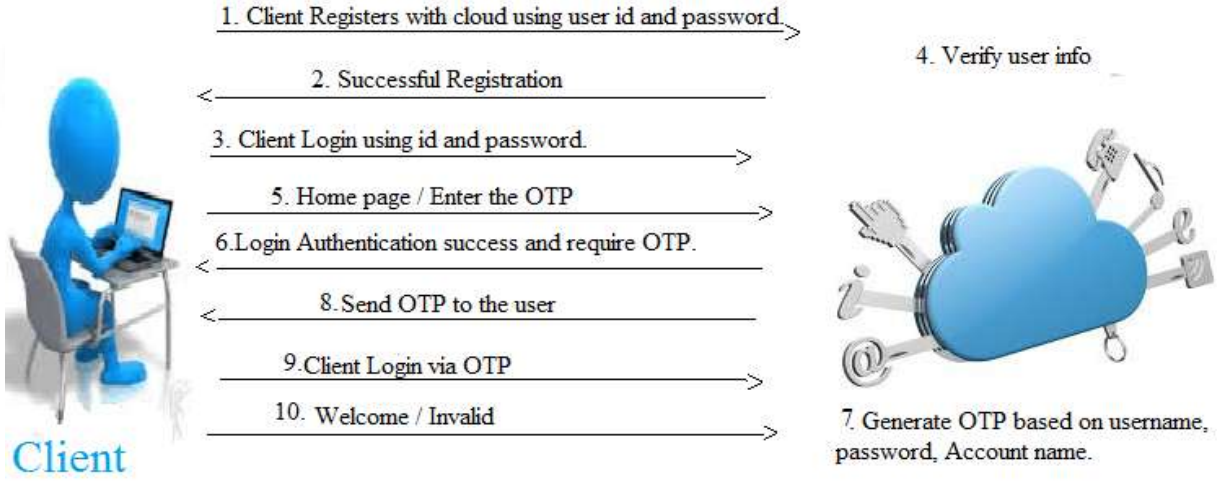

Figure 2. OTP Based Authentication Model

2. Encryption of Data at Client Side and Server Side: Client encrypts the data using RSA encryption algorithm before sending it to the cloud provider. This helps us to protect the data from the man in the middle attack.

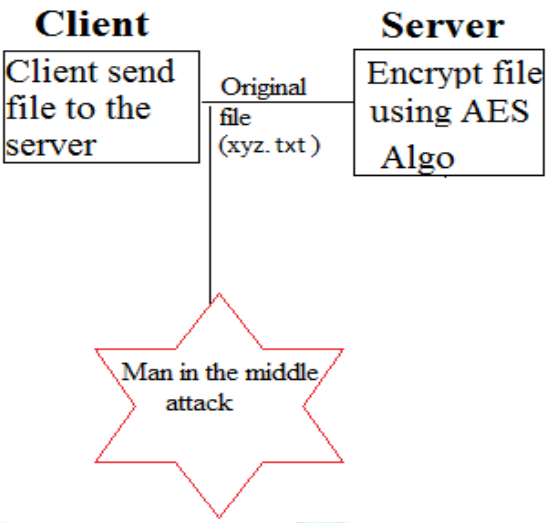

Figure 3. Man in the Middle Attack

This problem can be solved if client sends the encrypted data at the server. We have proposed a encryption mechanism at the client side using RSA algorithm.

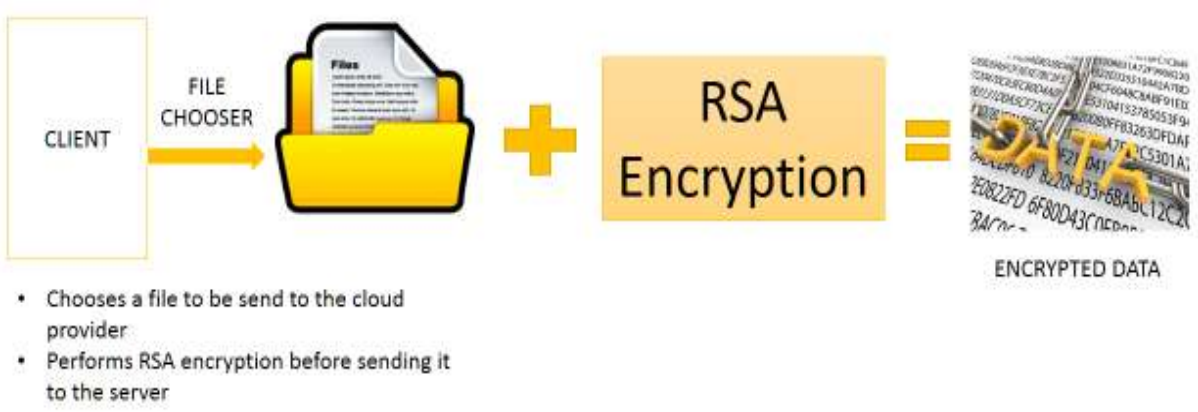

Figure 4. Client side encryption using RSA

- The file sent by the client is received at the server end and server will further perform the AES encryption on the received data.
- After encrypting the data, server will perform the fragmentation on the encrypted file and will send it to the cloud storage area.

Figure 5. Server side encryption and fragmentation

3. Cloud Zonal Storage and Replication: Cloud provider will receive the file and will store it in the different zones for security purposes. Cloud provider will also replicate the data on the backup server.

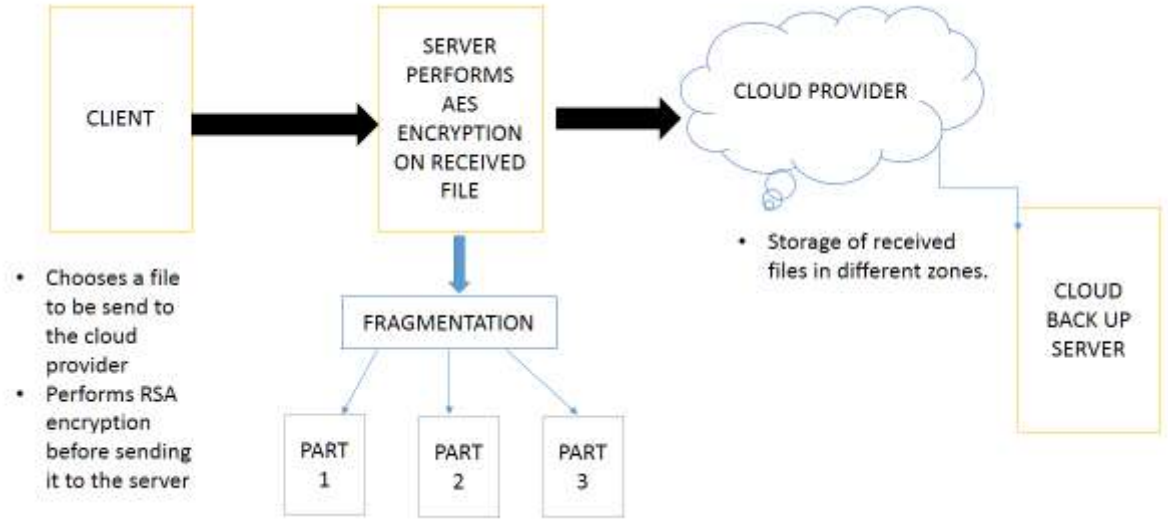

Figure 6. Proposed Methodology

Cloud based systems saves data off multiple organizations on shared hardware systems. Data segregation is done by encrypting data of users, but encryption is not complete solution. We can do segregate data by creating virtual partitions of data for saving and allowing user to access data in his partition only. Malicious activity monitoring is a tough task in cloud system as logging data might be spread over multiple hosts and data centres. Restricting user to his own virtual partition only will not allow logs to be dispersed allowing access to logs for monitoring easily. User access is another major concern in restricting user access is a major challenge in cloud based storage system. Use of virtual partition and enhanced user access control in cloud system will allow us to improve data security. Enhanced Cloud system will be compared with existing secure cloud systems. We will compare enhanced system against security, performance & ease of use.

- By distributing data on different clouds it introduces performance overhead when client needs to access all data frequently, e.g. client needs to perform a global data analysis on all data. The analysis may have to access data from multiple locations, with a degraded performance. By simply using in single cloud provider can having the following main issues: Less Security. Loss of data; No privacy; Cost of maintenance is high.

EXPERIMENTAL RESULTS

We have used the CloudSim as a simulator for implementing the proposed methodology. Cloud service providers charge users depending upon the space or service provided. In R&D, it is not always possible to have the actual cloud infrastructure for performing experiments. For any research scholar, academician or scientist, it is not feasible to hire cloud services every time and then execute their algorithms or implementations. For the purpose of research, development and testing, open source libraries are available, which give the feel of cloud services. Nowadays, in the research market, cloud simulators are widely used by research scholars and practitioners, without the need to pay any amount to a cloud service provider.

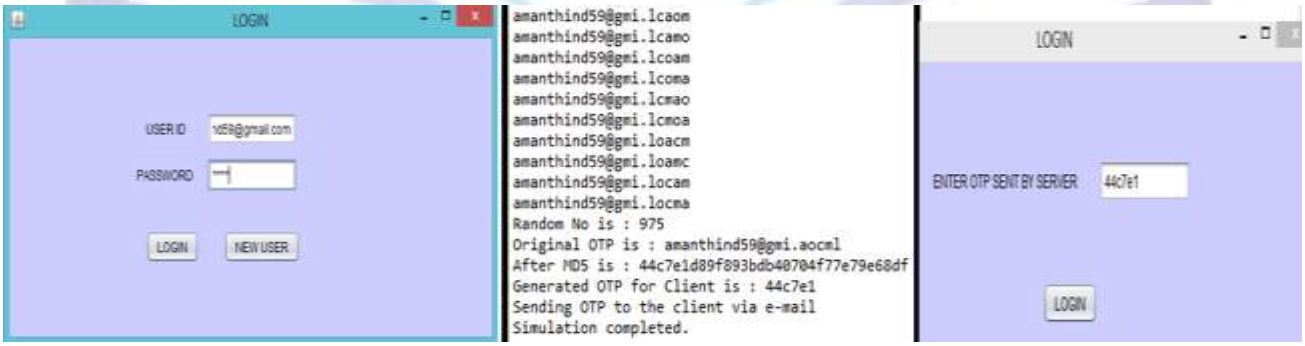

Figure 7. Login Section

Figure 7 shows the login section where the user will enter the user ID and the password. The request will be dispatched to the cloud provider where it will check the credentials of the user and will generate the OTP based on user's information. The OTP is generated with the help of MD5 and will send that generated OTP to the client's email ID.

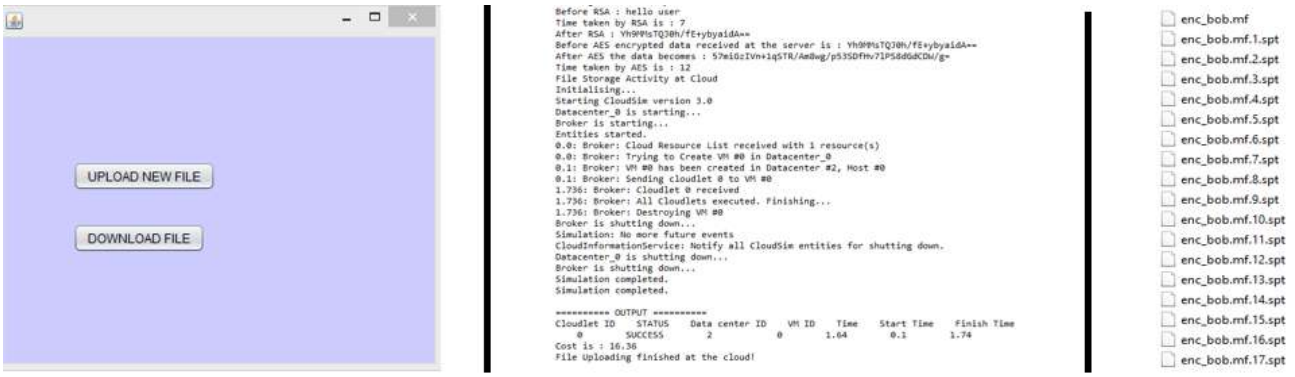

Figure 8. File Upload and Download

In Figure 8, we have demonstrated the main page of our proposed file. User can upload the file at the cloud server or can download the file from the cloud server. While Uploading the data at the cloud server, firstly RSA algorithm will encrypt the data the client side and AES will further encrypt the data at the server end. Server will divide the file into multiple parts.

Sno.	File Type	File Size	RSA Time (in Milliseconds)	AES Time (in Milliseconds)	Fragmented Parts	Cost
1	Properties File	381 bytes	201	16	146	21.8
2	JSP File	1.11 KB	562	27	435	33.36
3	XML File	3.53 KB	1268	59	1364	70.48
4	JAVA File	7.44 KB	2367	112	2432	152.35
5	HTML File	12.69 KB	3591	198	4856	265.22
6	ARFF Dataset	16.35 KB	5388	325	7865	412.34
7	JPG File	21.31 KB	9616	512	11234	656.21
8	Manifest File	25.08 KB	12633	711	14323	987.9
9	Text File	43.2 KB	17131	1312	25321	1235.21

Table 1. Different Parameters computed in the Proposed Work

Different experiments are conducted several times on different types of images like jsp page, properties file, xml file, text file etc. The files uploaded to the server are of different sizes. The number of parts, time taken by the RSA and AES algorithm have been showed in Table 1.

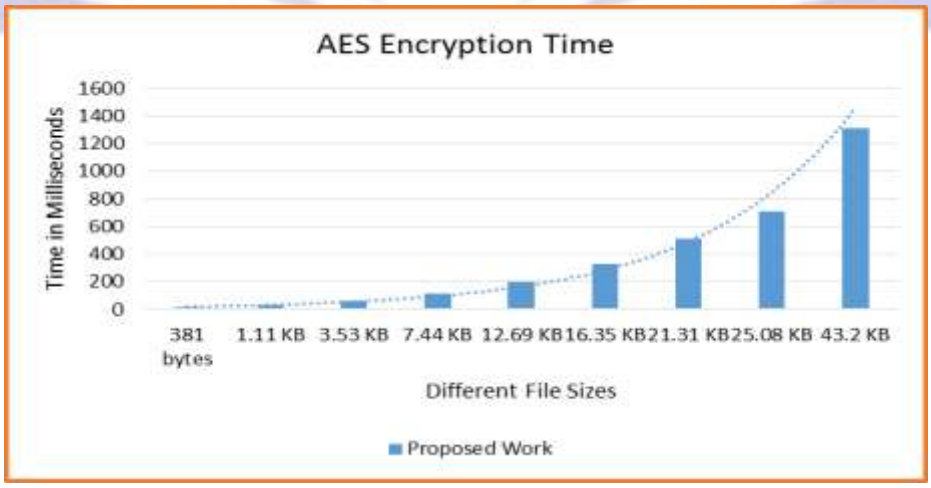

Figure 9. AES Encryption Time

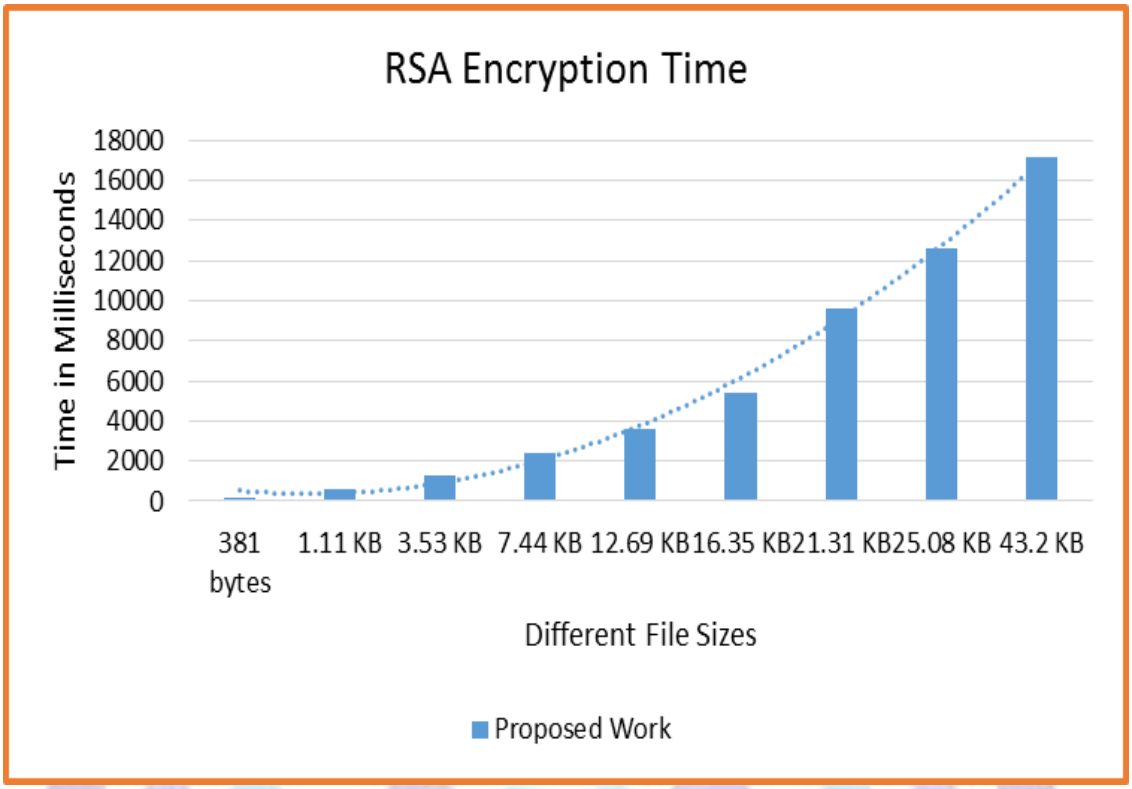

Figure 10. RSA Encryption Time

Figure 9 states as the file size increases, the data present in the file increases and time taken to encrypt the data will also increase. There is approximately exponential curve that depicts the time taken by the algorithms is directly proportional to the size of the File. Figure 10 also depicts the same behavior. Time is computed in milliseconds.

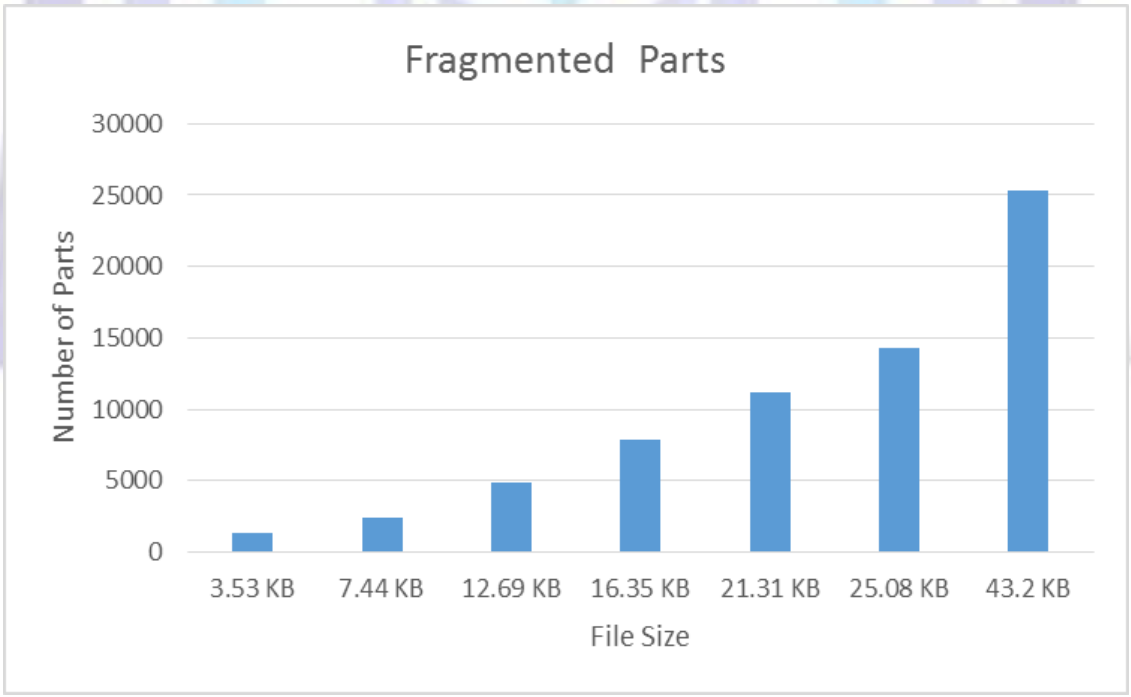

Figure 11. Fragmented Parts V/s File Size

The number of parts are increasing if we increase the file size (Figure 11). The data fragmentation is done at the server end. The cost occurred to the client has been decreased in comparison to the base paper because in the base paper, they have used the multiple cloud servers for the storage of data where as in our proposed work, we have used the single cloud server with different VM's, thereby decreasing the overall cost of the client.

Figure 12. Cost comparison chart.

CONCLUSION

With the continuous growth and expansion of cloud computing, security has become one of the serious issues. Cloud computing platform need to provide some reliable security technology to prevent security attacks, as well as the destruction of infrastructure and services. There is no doubt that the cloud computing is the development trend in the future. Cloud computing brings us the approximately infinite computing capability, good scalability, service on-demand and so on, also challenges at security, privacy, legal issues and so on. But to solving the existing issues becomes utmost urgency. To protect against the compromise of the compliance integrity and security of their applications and data, firewall, Intrusion detection and prevention, integrity monitoring, log inspection, and malware protection. Proactive enterprises and service providers should apply this protection on their cloud infrastructure, to achieve security so that they could take advantage of cloud computing ahead of thei r competitors. These security solutions should have the intelligence to be self-defending and have the ability to provide real-time detection and prevention of known and unknown threats. To advance cloud computing, the community must take proactive measures to ensure security.

REFERENCES

[1] Tejinder Sharma, Vijay Kumar Banga. Efficient and Enhanced Algorithm in Cloud Computing, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-1, March 2013.

[2] Sonal Guleria1, Dr. Sonia Vatta2, to enhance multimedia security in cloud computing environment using crossbreed algorithm, Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com, Volume 2, Issue 6, June 2013.

[3] Pradeep Bhosale Priyanka Deshmukh Girish Dimbar Ashwini Deshpande , Enhancing Data Security in Cloud Computing Using 3D Framework & Digital Signature with Encryption, International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 8, October – 2012.

[4] Jasmin James, Dr. Bhupendra Verma, efficient VM load balancing algorithm for a cloud computing environment, Jasmin James et al. International Journal on Computer Science and Engineering (IJCSE).

[5] Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou, Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing, 978-1-4244-5837-0/10/$26.00 ©2010 IEEE.

[6] Ryan K. L. Ko, Markus Kirchberg, Bu Sung Lee , From System-centric to Data-centric Logging Accountability, Trust & Security in Cloud Computing.

[7] Shuai Han, Jianchuan Xing, ensuring data storage security through a novel third party auditor scheme in cloud computing, Proceedings of IEEE CCIS2011.

[8] Jen-Sheng Wang, Che-Hung Liu, Grace TR Lin, How to Manage Information Security in Cloud Computing.

[9] Eman M.Mohamed, Hatem S.Abdelkader, Data Security Model for Cloud Computing, 978-1-61208-245-5,ICN 2103.

[10] Teemu Kanstren, Sami Lehtonen, Reijo Savola, Architecture for high confidence cloud security monitoring, 978-4799-8218-9/15 2015 IEEE.