International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 11 – No. 6, November 2016 – www.ijais.org

A Strongly Trusted Integrity Preservance based Security Framework for Critical Information Storage over Cloud Platform

Shweta Sharma
M .Tech, Delhi Technological University
Delhi

ABSTRACT

During last few years, the demand of cloud computing has immensely arisen among the Corporate/Business organizations. The cloud computing concept brings exclusive monetary benefits to the corporate houses through its pay-as per use facility. The incurred cost only lies in the consumption of hardware and software resources for any particular available business applications[1].For any particular project, all the web applications are deployed on available physical servers ,dispersed throughout the countries ,connected through cloud service providers. This mega scale growth in the adoption of cloud platform leads to extreme revenue benefits to the involved parties. But at the same time, information security also requires to be well enveloped in the cloud environment [2].In this research work, we have incorporated various cryptographic algorithms to improve the authentication module such as Challenge response Authentication protocol and file data storage using suitable and efficient Digital Signature Standard scheme along with effective encryption schemes such as AES as well. The proposed framework represents proper client –server authentication and secured & trusted architecture for stored information on cloud server. We have done research work to alleviate the security of stored information with in the cloud and also to protect it from any outside attack during information exchange between client and server.

General Terms

Information Security, Cloud Platform, File Integrity.

Keywords

Cryptography,Authentication Protocol, Digital Signature Standard Scheme (DSS), Diffie -Hellman Key Exchange scheme.

1. INTRODUCTION

In today's computing world, cloud security has emerged as an immense requirement in business projects. There have been variety of prevailing security attacks which needs to be fixed to ensure proper protection of stored client's information over cloud server[3].The Security attacks includes distributed denial of service attack (DDoS), replaying, masquerading, side channel attacks, phishing and geographical implications .In cloud computing platform, corporate organizations outsource the computing resources from other cloud vendors. The companies may decide to transfer their business applications/tools/databases on Cloud platform [4]. They are required to follow certain configurations and technical parameters related to their software and hardware needs before deciding to move to the cloud. According to [2][5], there have been various developed features of cloud computing, enforced and provided to the organizations if security and privacy risks are minimized. These features are as:-

Limitless Flexibility: The various software applications/databases can easily be accessed through cloud computing platform. This provides better scalability.

Reliability & Security: Both these features are imparted to the clients dealing with cloud Platform. These requirements serve the purpose of quality improvements in terms of service delivery to the users.

Collaboration of application units*:* Various software applications/UIs/Executable gets collaborated together on same platform to perform desirable computing functions. Thus benefits the user's adaptability.

Portability: Remote servers store and access client's data based on constraints. The client may avail its stored data and applications as per his/her requirements.

Simpler Devices: Devices such as PDAs, cellphones, video recorders etc. may be used to interface with cloud platform and thus becomes easily accessible. The true benefits of cloud computing can be utilized if real time privacy and security issues can be addressed to protect information part of the cloud platforms.

2. RELATED WORK & LIMITATIONS

In order to provide significant amount of information security for storage on cloud server, various research frameworks have been proposed and analyzed to ensure quality schemes to sustain high level security for client's data. There have been various functional models of Cloud. In case of private cloud, there exists confidential and sensitive information such as – credit cards, Intellectual property/trade secrets, Financial, Health, State/Government secrets, Proprietary/Sensitive and Personally Identifiable. Thus, Enhancing Information Security levels become the top most priority to support Cloud Computing for running businesses in IT trade.

Following summarization indicates the literature survey on distinguished proposed research work related to information integrity within the cloud platform during recent years.

2.1 Information storage using Tripwire [12]

It is a type of Intrusion Detection System tool which was used to store the hash values of a particular file within the associated Database. Any intrusion leads to recompilation of latest hash values and comparison with original values from databases. The major drawback is the requirement of databases to store the computed hash values at any point of time.

2.2 Flogger (A File centric logger to monitor file access in cloud) [11]

This tool accesses various system logs by establishing physical and virtual subnets. Their component includes various services in the form of:-File Sender daemon, File sender client program, Database loader, Windows and Linux floggers. The tool monitors every file/folder accesses briefly, keeps check on online generated system logs. The major drawback is huge database requirements which deteriorate cost effectiveness.

2.3 I3FS Tool (Intrusion detection file system [9] [10])

It consists of Berkeley Databases (Transaction based and High level performance dB).The file integrity gets verified after qualifying security and cache policies criterias.The checksums are stored in Berkeley databases against corresponding access policies. The limitation of this tool is the requirement of Berkeley databases and maintenance of database servers which may lead to server overheads in cloud environment.

2.4 Light weight File Monitoring Tool [6] [7]

It provides a light weight file integrity maintenance tool which computes the checksum of the client's stored file and saves within the file/folder. It verifies the information integrity in a cost effective manner as compared with other tools(already discussed).But it has its own limitations:-

- Absence of transparency to client in reference with determination of checksum by the server.
- There is no client involvement present during calculation of checksum by the server.
- It doesn't cater to the availability of backup replica (if in case, file integrity gets lost/disturbed).
- Client-server trust bond has no significance in this model. The attacker could impersonate as server.
- There exists a requirement of extra effective client—server relationship in order to enhance the overall quality of this model.

3. PROPOSED DESIGN FOR IMPROVISED AND RELIABLE INFORMATION INTEGRITY FRAMEWORK FOR CRITICAL INFORMATION STORAGE UNDER CLOUD PLATFORM [8] [20]

In this proposed work, we elaborate a client-server scenario for cloud computing. To provide information security to the saved client entity record on the cloud server, we have designed the following procedural events .This tool proves to be cost-effective and light weight without any additional database requirements. The Algorithm below illustrates the events sequentially in a given cloud computing scenario [14] [15] [16]

1. Initialize Client Process as P1 and Server Process as P2 (for a given cloud computing scenario).
2. P1 authenticates itself to the server (P2) using Zero Authentication Protocol.
3. If the authentication is valid, P2 allows P1 to get logged into the server and both processes exchanges secret key SP using Diffie-Hellman Key exchange method.
4. P1 selects file storage functionality (with a motive to store its own data on cloud server).
5. P2 saves the file F into shared hard disk and applies hash algorithm (SHA-1) in order to compute the final checksum output X.
6. X is stored in <output>tags in F only. (saves memory).
7. Apply AES encryption algorithm to encrypt the X.
8. Transfer X to P1.P1 applies AES decryption algorithm using secret key SP.
9. P1 applies DSS (Digital Standard Signature) algorithm using P1 private key p on X to produce FX.
10. P2 sends computed output FX to P2 for storage on cloud.
11. If P1 logged in again and applies for Integrity Verification of F.
12. P2 applies Integrity verification ( ) on X to produce FX'.
13. If FX==FX', Integrity Intact. File Preserved.
14. Else Integrity attacked. Apply Back-up Replica functionality.
15. Original File F available.
16. Integrity verification () ends.
17. Program Ends.

3.1 Advantages Of Proposed Information Integrity Model In Cloud Computing [17] [18] [19]

There are certain advantages related to given models which are as listed below:

- This research work generates trust and reliability between client and server entities.
- The client process gets directly connected with server process to compute the final checksum value to be stored in <output> tags within the file.
- This model eliminates the probability of an attacker who could even impersonate as server on the cloud platform.
- Transparency level exists between client and server entities while executing business acts. This leads to inculcation of trusted values.
- For proper secure key exchange procedures, Use of Diffie-Hellman Key exchange technique has also been collaborated into this model.

- This model proves to be economical, reliable, and trustworthy and secure for critical information storage over cloud.
- The client authenticates itself with server using proper valid Zero-Authentication Protocol which has been designed such that claimant does not reveal anything which will endanger the confidentiality of the secret. The claimant proves the verifier that he knows a secret without leaking it
- The Digital Signature Standard (DSS)scheme has been incorporated to enhance the security of the computed checksum as its smaller in size and fast in speed in terms of execution(on comparison with other signatures).

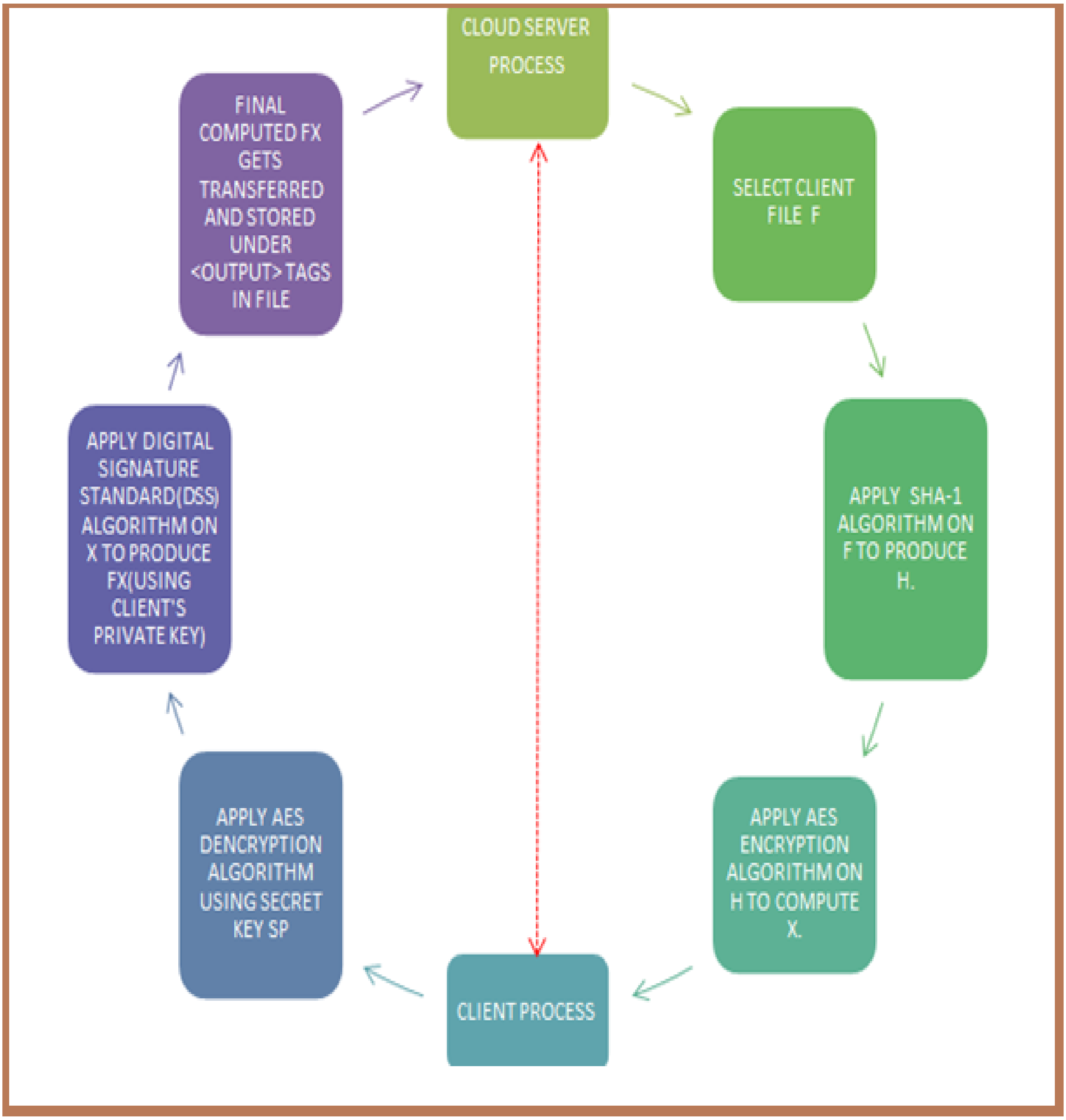
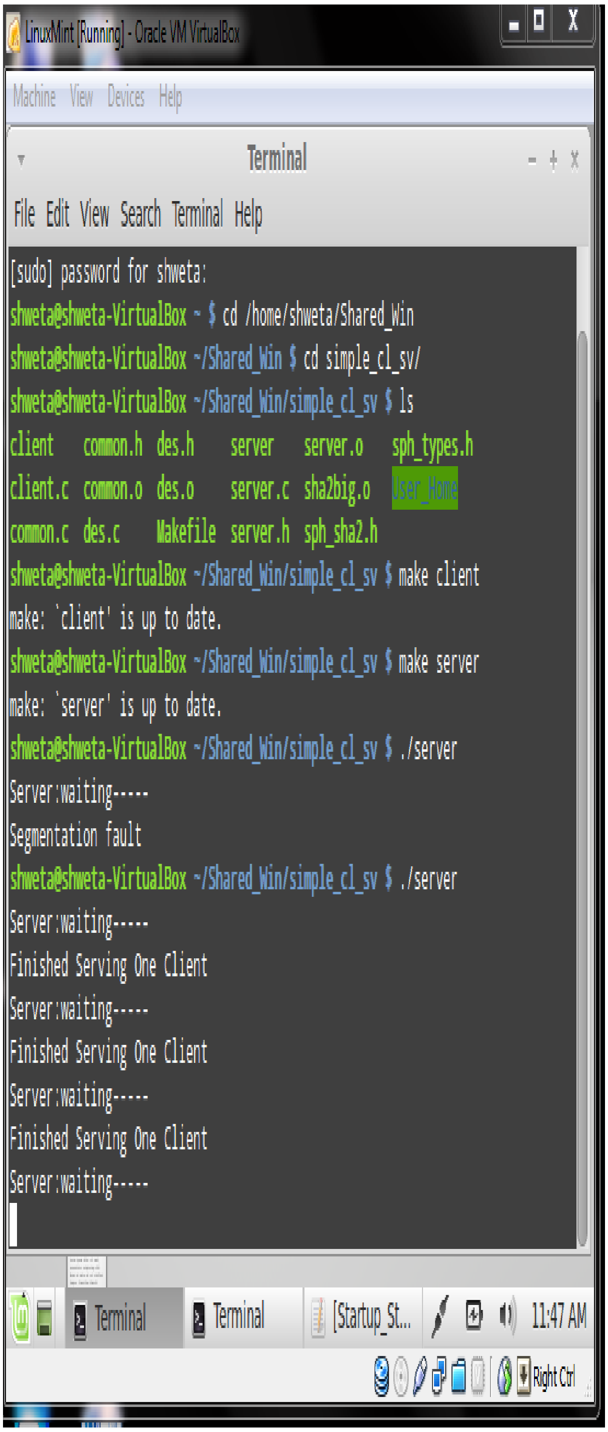

CLOUD SERVER PROCESS
SELECT CLIENT FILE F
APPLY SHA-1 ALGORITHM ON F TO PRODUCE H.
APPLY AES ENCRYPTION ALGORITHM ON H TO COMPUTE X.
CLIENT PROCESS
APPLY AES DENCRYPTION ALGORITHM USING SECRET KEY SP
APPLY DIGITAL SIGNATURE STANDARD(DSS) ALGORITHM ON X TO PRODUCE FX(USING CLIENT'S PRIVATE KEY)
FINAL COMPUTED FX GETS TRANSFERRED AND STORED UNDER <OUTPUT> TAGS IN FILE

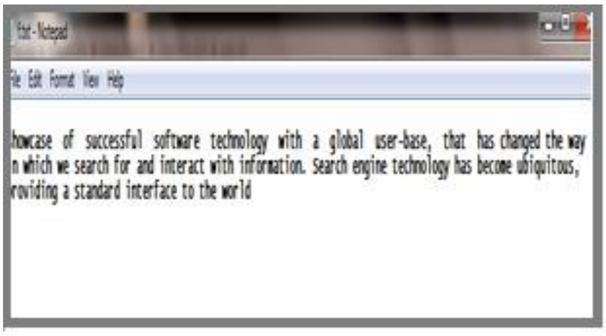
Figure1. Diagrammatic representation of strongly trusted integrity security framework for critical information storage inside cloud

4. OUTPUTS OF NEWLY PROPOSED TOOL TO ENSURE SECURITY FOR CRITICAL INFORMATION OVER CLOUD PLATFORM


LinuxMint [Running] - Oracle VM VirtualBox
Machine View Devices Help
Terminal
File Edit View Search Terminal Help
Terminal
Terminal
[Startup St...
11:47 AM
Right Ctrl

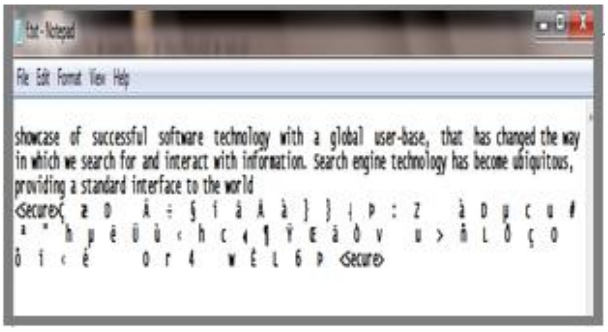
```
[sudo] password for shweta:
shweta@shweta-VirtualBox ~ $ cd /home/shweta/Shared_Win
shweta@shweta-VirtualBox ~/Shared_Win $ cd simple_cl_sv/
shweta@shweta-VirtualBox ~/Shared_Win/simple_cl_sv $ ls
client    common.h  des.h     server    server.o   sph_types.h
client.c  common.o  des.o     server.c  sha2big.o  User_Home
common.c  des.c     Makefile  server.h  sph_sha2.h
shweta@shweta-VirtualBox ~/Shared_Win/simple_cl_sv $ make client
make: `client' is up to date.
shweta@shweta-VirtualBox ~/Shared_Win/simple_cl_sv $ make server
make: `server' is up to date.
shweta@shweta-VirtualBox ~/Shared_Win/simple_cl_sv $ ./server
Server:waiting-----
Segmentation fault
shweta@shweta-VirtualBox ~/Shared_Win/simple_cl_sv $ ./server
Server:waiting-----
Finished Serving One Client
Server:waiting-----
Finished Serving One Client
Server:waiting-----
Finished Serving One Client
Server:waiting-----
```

Figure 2: Screenshot for Server Process Initialization Mode



```
howcase of successful software technology with a global user-base, that has changed the way
n which we search for and interact with information. Search engine technology has become ubiquitous,
roviding a standard interface to the world
```

Figure 3: Screenshot of Original client's data stored on server



```
showcase of successful software technology with a global user-base, that has changed the way
in which we search for and interact with information. Search engine technology has become ubiquitous,
providing a standard interface to the world
<Secure>( ž Ð  Å ÷ § í à Å à ] } ¦ Þ : Z  à Ð µ ć u ∤
ª " h µ ē Ū ù ‹ h ć ‹ ¶ Ÿ Ė ā Ô v  u › ň L Ô ç 0
ô í ‹ é   0 r 4  w Ė L 6 Þ <Secure>
```

Figure 4: Screenshot of Original Client's data stored after Integrity Calculation (stored within shown tags)

5. CONCLUSION

This proposed tool work had been executed in Oracle VM virtual box (based on LINUX, win7 Platform).The client and server processes have been developed using socket programming and specific socket address based structures. This tool performs regular integrity checks and thus supervises the intact integrity of the client's information over the cloud with better client –server communications .Thus, it can be observed that it proves to be time efficient and cost effective as it executes integrity calculation in approximately 1000 microseconds for 600 byte file which proves to be a minimal requirement as compared to long duration delays(in minutes/hours) consumed by server to perform integrity checks on client's stored information. This tool works without database software on the server. It satisfies light weight and secures storage tool criteria for cloud platform.

6. REFERENCES

[1] GA Solanki, Welcome to the Future of Computing: Cloud Computing and Legal Issues, International Journal of Scientific & Technology Research 2012, vol1, issue 9.

[2] Nelson Gonzalez, Charles Miers, Fernando Redigolo, Marcos Simplicio, Tereza Carvalho, Mats Naslund, Makan Pourzandi, A quantitative analysis of current security concerns and solutions for cloud computing, Gonzalez et al. Journal of Cloud Computing: Advances, Systems and Applications 2012.

[3] Lijun Mei, W .K .Chan, T .H .Tse, A Tale of Clouds: Paradigm comparisons and some thoughts on research issues, 2008 IEEE Asia-Pacific Services Computing Conference.

[4] Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr. Atanu Rakshit, Cloud security Issues 2009, IEEE.

[5] M. Sudha, M. Monika, Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography, Advances in Computer Science and its Applications 32 Vol. 1, No. 1, March 2012, Copyright © World Science Publisher, United States. www.worldsciencepublisher.org.

[6] Sanchika Gupta, Anjali Sardana, Padam Kumar, A light Weight Centralized File Monitoring Approach for Securing Files in Cloud Environment ,The 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012) ,IEEE 2012.

[7] Sanchika Gupta, Anjali Sardana, Padam Kumar , Ajith Abraham, A secure and light weight approach for critical data security in cloud, 2012 Fourth International Conference on Computational Aspects of Social Networks (CA Sons).

[8] Forouzan, Cryptography and Network Security, TMH 2012.

[9] S. Patil, A. Kashyap, G. Sivathanu and E. Zadok, I3FS: An in-kernel integrity checker and intrusion detection file system.

[10] Q. Nguyen Anh and T. Yoshiyasu, A novel approach for a file-system integrity monitor tool of Xen virtual machine, Book A novel approach for a file-system integrity monitor tool of Xen virtual machine, Series A novel approach for a file-system integrity monitor tool of Xen virtual machine, ed.,Editor ed.ls\eds., ACM, 2007.

[11] R.K.L. Ko, P. Jagadpramana and L. Bu Sung, Flogger: A File-Centric Logger for Monitoring File Access and Transfers within Cloud Computing Environments, Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on , pp. 765-771.

[12] H. K. Gene and H. S. Eugene, The design and implementation of tripwire: a file system integrity checker,Book The design and implementation of tripwire: a file system integrity checker, Series The design and implementation of tripwire: a file system integrity checker, ed., Editors, ACM, 1994.

[13] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacono, On technical security issues in cloud computing 2009, IEEE Computer Society.

[14] Tina Francis, S. Vadivel, Cloud Computing Security: Concerns, Strategies and Best Practices: Proceedings of 2012 Intemational of Cloud Computing, Technologies, Applications & Management, 2012 IEEE.

[15] Mr. Prashant Rewagad, Ms. Yogita Pawar, Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing, 2013 International Conference on Communication Systems and Network Technologies.

[16] Wang Jun-jie, MuSen, Security Issues and Countermeasures in Cloud Computing, 2011 IEEE.

[17] Balachandra Reddy Kandukuri , Ramakrishna Paturi V, Dr. Atanu Rakshits , “Cloud Security Issues”, 2009 IEEE International Conference on Services Computing,2009 IEEE.

[18] Mrs. G. Nalinipriya ME, (PhD), Mr. R. Aswin Kumar, “Extensive Medical Data Storage with Prominent Symmetric Algorithms On Cloud “, A Protected Framework: 2013.