Smart Integrity Manager Cloud Securer Using Triple DES

B.Thiyagarajan *
Kamalakannan .R **

* Assistant Professor, Department Of Computer Science And Engineering
Sri Manakula Vinayagar Engineering College
Madagadipet puducherry

**M.Tech Final Year Department Of Computer Science And Engineering
Sri Manakula Vinayagar Engineering College
Madagadipet puducherry

ABSTRACT

Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. More and more users store data in "clouds". Almost every enterprise application is moved to cloud which raised the concern about the integrity and privacy of data of client as well as enterprise officials. This concern makes officials hesitate to enjoy cloud service. This paper provides solution to this data integrity problem. The work proses a new architecture leading to formation of smart integrity manager and error handler which controls entire cloud environment. In our work, we use the Triple DES Encrption algorithm, on behalf of the cloud client, to verify the integrity of the data stored in the cloud.

Keywords: ***cloud computing, integrity manager, error handler, Tiple DES.***

I.INTRODUCTION

Cloud computing provides a scalable environment for growing amounts of data and processes that work on various applications and services. . Everyone has their own way of defining cloud computing. Basic working motto of cloud computing is to provide cheap and efficient service to the mass. This reduces infrastructure cost, data management cost, etc. cloud providers offers vast services such as software as a service, infrastructure as a service, platform as a service and also few hints of monitoring as a service. These are services faces a common problem of data integrity problem. In recent times, most of the enterprise application are deployed in cloud. Cloud are of three types, public cloud which is mostly maintained by third parties, private cloud which is used for specific application and hybrid cloud which is a combination of both the above mentioned clouds

II.CLOUD COMPUTING

Cloud computing refers to the delivery of computing resources over the Internet. Instead of keeping data on your own hard drive or updating applications for your needs, you use a service over the Internet, at another location, to store your information or use its applications. Doing so may give rise to certain privacy implications. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.

A. *Cloud Computing Service Models*

The cloud computing service models are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). In a Software as a Service model, a pre-made application, along with any required software, operating system, hardware, and network are provided. In PaaS, an operating system, hardware, and network are provided, and the customer installs or develops its own software and applications. The IaaS model provides just the

hardware and network; the customer installs or develops its own operating systems, software and applications.

Figure 1:***Cloud Computing service Models***

B. *Cloud Components*

A cloud computing solution is made up of several elements: clients, the datacenter, and distributed servers. As shown in Figure 2, these components make up the three parts of a cloud computing solution.Each element has a purpose and plays a specific role in delivering a functional cloud-based application.

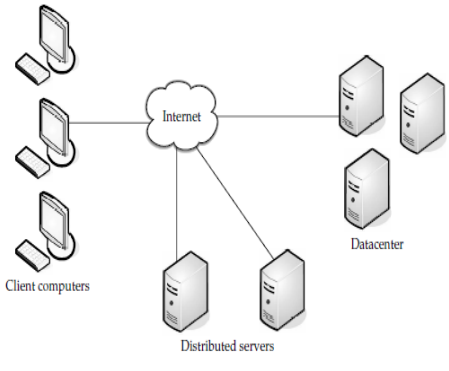

Figure 2: **Three components make up a cloud computing solution**

C.Types of Clouds

With cloud computing technology, large pools of resources can be connected through private or public networks. This technology simplifies infrastructure planning and provides dynamically scalable infrastructure for cloud based applications, data, and file storage. Businesses can choose to deploy applications on Public, Private, Hybrid clouds or the newer Community Cloud.

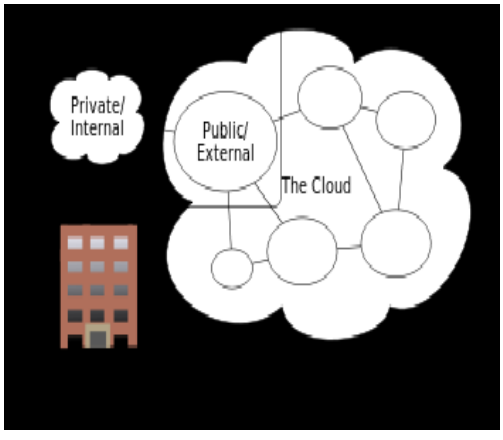

Figure 3:***Types of Clouds***

III.RELATED WORK

To accomplish this particular concept justification, several dimension like storage, interface, data type synchronization are compared. Qualitative comparison framework developed by Mie. Though Siani provides details about the privacy in cloud computing but his proposed system doesn't provide any solution to the risk that the data possess in the cloud. Few of the challenges in cloud computing were given by Tharam Dillon. Scheduling problem was addressed by Young Choon Lee and as a result has presented two sets of profit driven service request.

The data stored in cloud always is exposed to risk of losing its integrity. Any kind of hacking activity hinders integrity of private data. This paper deals with securing integrity of data and thus leading many more organisation to enter into reliable cloud computing.

IV.PROPOSED SYSTEM

In this section, we propose a framework which involves securing of files through file encryption. The file present on the device will be encrypted using password based Triple DES algorithm The user can also download any of the uploaded encrypted files and read it on the system.

Triple DES Encryption Algorithm:

The DES encryption algorithm that encrypts data three times. Three 64-bit keys are used, instead of one, for an overall key length of 192 bits (the first encryption is encrypted with second key, and the resulting cipher text is again

encrypted with a third key). The TDEA is commonly known as Triple DES (Data Encryption Standard)

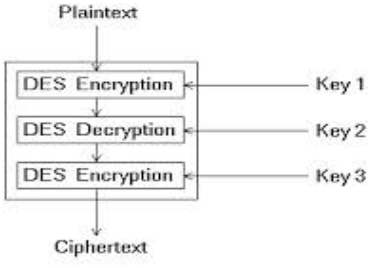

Figure 4:Triple DES Encryption algorithm

Triple DES uses a "key bundle" which comprises three DES keys, K_1, K_2 and K_3, each of 56 bits (excluding parity bits). The encryption algorithm is:

$$\text{ciphertext} = E_{K3}(D_{K2}(E_{K1}(\text{plaintext})))$$

i.e., DES encrypt with K_1, DES *decrypt* with K_2, then DES encrypt with K_3.
Decryption is the reverse:

$$\text{plaintext} = D_{K1}(E_{K2}(D_{K3}(\text{ciphertext})))$$

i.e., decrypt with K_3, *encrypt* with K_2, then decrypt with K_1.Each triple encryption encrypts one block of 64 bits of data.

A. PROPOSED SYSTEM ARCHITECTURE

The proposed system architecture diagram for security and integrity of data in cloud environment.The architecture diagram is shown in below figure 5:

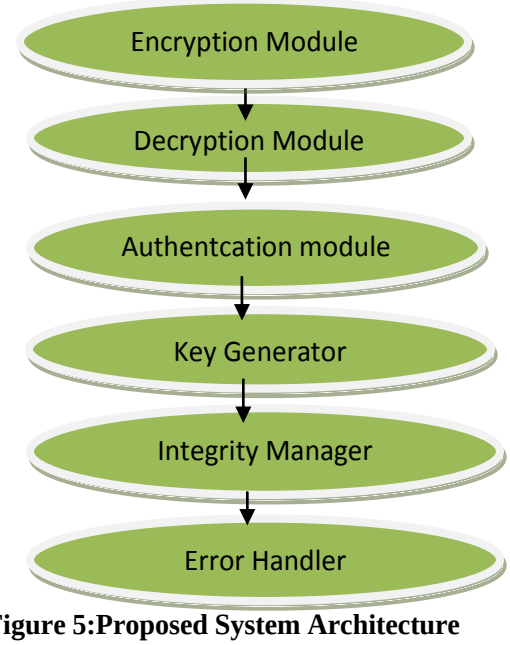

Figure 5:Proposed System Architecture

V. IMPLEMENTATION

As far as **implementation** of this particular project is concerned, there are many individual model for accomplishing the entire task.

The most important modules are

1. Encryption module

Encryption is the process of encoding messages (or information) in such a way that third parties cannot read it, but only authorized parties can.Encryption doesn't prevent hacking but it prevents the hacker from reading the data that is encrypted. In an encryption scheme, the message or information using an encryption algorithm, turning it into an unreadable ciphertext.

2. Decryption module.

Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer are able to read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys.

3. Authentication module.

Authentication is the act of confirming the truth of an attribute of a datum or entity. This might involve confirming the identity of a person or software program, tracing the origins of an artifact, or ensuring that a product is what its packaging and labeling claims to be. Authentication often involves verifying the validity of at least one form of identification.

4. Key generator

A key generator is used in many cryptographic protocols to generate a sequence with many pseudo-random characteristics. This sequence is used as an encryption key at one end of communication, and as a decryption key at the other.

5. Integrity manager

Integrity management consulting is a fast-emerging global sector that advises individuals and corporations on how to apply the highest ethical standards to every aspect of their business. At the core of integrity management is the belief that companies have a strong interest, as well as a responsibility, to act with integrity at all times.

The field of integrity management aims to address:

(i) The demand for companies to respond to increasing awareness of ethical misconduct and resulting expectations for transparency and accountability;
(ii) The requirement for companies to comply with a stricter legal framework and avoid prosecution for unethical behaviour.
(iii) The desire for executives to make their enterprises leaders in responsible and sustainable development.

6. Error handler

Exception handling in software are error checking, which maintains normal program flow with later explicit checks for contingencies reported using special return values or some auxiliary global variable such as C's errno or floating point status flags; or input validation to preemptively filter exceptional cases.

VI. CONCLUSION

Expected to produce an output which is more secure in cloud with least prone to hackers. The error handler is supposed to handle all the possible error that can occur while retrieving data from cloud. Integrity manager is supposed to generate proper keys for encrypting and decrypting and the system overall is expected to produce high security and reliability along with less complexity at server side.

REFERENCES

1. Tharam Dillon, Chen Wu and Elizabeth Chang, "Cloud Computing: Issues and Challenges", Digital Ecosystems and Business Intelligence Institute Curtin University of Technology, Perth, Australia.

2.Siani Pearson, Yun Shen and Miranda Mowbray, "A Privacy Manager for Cloud Computing", HP Labs, Long Down Avenue, Stoke Gifford, Bristol BS34 8QZ, UK.

3.Gritzalis D, Moulinos K. Kostis K.: "A Privacy-Enhancing e-Business Model Based on Infomediaries" in MMM-ACNS 2001, LNCS 2052, pg. 72–83. Springer Verlag Berlin Heidelberg 2001.

4.Cong Wang, Qian Wang and KuiRen, Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", Department of ECE, Illinois Institute of Technology.

5.Bo Peng, Bin Cui and Xiaoming Li, "Implementation Issues of A Cloud Computing Platform", Department of Computer Science and Technology, Peking University.

6.D. Chen, H. Zhao, ―Data Security and Privacy Protection Issues in Cloud Computing‖, IEEE International conference on Computer Science and Electronics Engineering, 2012.

7.K. Popovic, Z. Hocenski,‖Cloud Computing security issues and challenges‖, MIPRO, Proceedings of the 33rd International Convention, 2010.

8.vantesson, D. and Clarke, R. (2010), Privacy and consumer risks in Cloud Computing, Computer Law & Security Review, 26, p.p. 391 - 7.

9.Knorr, E. and Gruman, G. (2011), What cloud computing really means. Retrieved on Dec. 5, 2011 from http://www.infoworld.com/d/cloud-computing/wht-cloud-computing-really-means-031

10.Ward, B. T. and Sipior, J. C. (2010), The internet jurisdiction risk of cloud computing, Information Systems Management, 27, p.p. 334-9