Use of Digital Signature and Rijndael Encryption Algorithm to Enhanced Security of data in Cloud Computing Services

Prashant Rewagad[1*], Yogita Pawar [2*]
[1] Assistant Professor, Department of Computer Science & Engineering, GHRIEM, Jalgaon
2 ME-CSE, Department of Computer Science & Engineering, GHRIEM, Jalgaon

ABSTRACT
Cloud computing is an amazing technology above all other types of computing. Cloud computing implies sharing of computing resources rather than having local servers or personal individual devices to handle the applications. The goal of cloud computing is to increase the speed of computations per second by applying traditional supercomputing, or high-performance computing power. It is used in consumer-oriented applications such as recruitments, smart staffing and medical image retrieval etc. The cloud computing however, has some problems associated with it .Among them security and privacy are the main concerns. This paper focus on both security and privacy issues of cloud computing. In this paper we have proposed to use Rijndael algorithm for encryption of data on the fly to provide data security in cloud .We have also proposed to make use of digital signature to ensure privacy and authentication of client's data

Keywords: Rijndael algorithm, digital signature, encryption.

1. INTRODUCTION
The cloud computing is a model for enabling convenient ,on demand network access to a shared pool of configurable resources such as networks, servers, files storage ,applications and services. The Cloud Computing buzz is growing every day with a growing number of businesses and government establishments opting for cloud computing based services [2].
Cloud computing is a type of computing that is comparable to grid computing. Cloud computing relies on sharing computing resources rather than having local servers or personal devices to handle applications. The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios or even to deliver personalized information, or power immersive computer games[2].
To do this, cloud computing networks use large groups of servers, usually those with low-cost consumer PC technology, with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.
Cloud computing has started to obtain mass appeal in corporate data centers as it enables the data center to operate like the Internet work through the process of enabling computing resources to be accessed and shared as virtual resources in a secure and scalable manner.

2. CHARACTERSTICS
A. Agility
It means cloud computing is able to provide on demand services anywhere, at anytime, irrespective of different forms of presentations or format required by the users.

B. Reliability
The user is able to access his/her resources only. It never happens that cloud is delivering invalid or irrelevant resources. Also loss of data or acquiring wrong data is not affordable in case of business employed using cloud computing [3].

C. Fault tolerance
The cloud computing has self healing capability. It has hot backups, which plays an important role in case of server failure, etc. Hence user is always made available with resources even in presence of failures.

D. Multi-Tenancy
Several customers share infrastructure at the same time in cloud computing. This is made possible without compromising privacy and security of each of the customer's data. Privacy is very important because most of the times business associates stores sensitive and confidential data on cloud, which if leaked out can endanger the business itself.

E. Virtualization
Even user does not know where actually his/her data is store besides whose data in the cloud. The data is stored on physical machines along with virtual machines. Virtualization is very important because user needs information within span of seconds at any point of time, at any location because he plays lumsum for the same [2] .

3. CLOUD SERVICES
A. *CloudMe*
The client can Access, upload and share files from anywhere, even from phone. He can access online storage, Photos, Music, Movies, Application development, Calendar, Mail, Media Player, Word Processors etc. It has both free and premium signup. It also offers a platform for web developers Platform as a service, PaaS. The free account provides 3GB of CloudMe drive storage.

B. *Cloudo*
It is a free computer that lives on the Internet, right in the web browser. This means that one can access documents, photos, music, movies and all other files no matter where you are, from any computer or mobile phone. Cloudo is a hosted service, there is no hardware or software to setup and maintain, and the DDE is fully accessible from any internet connected device. Other advantages of utilizing hosted software include centralizing data backup, updates, and security at the data center as well as the benefits of lower cost which can be associated with the administration of a single global instance of software versus many local instances.

C. *Mint*
It is a Cloud based personal finance tool to manage the money transactions. Launched in September 2007, it has received 30+ prestigious web awards from the likes of CNN Money, Time,

Business Week, PC Mag etc. The client can create an account and access all balances and transactions together on the web or on the iPhone. It's a simply an innovative concept: All your money related accounts viz. bank accounts, credit card, loans, stock brokerage and other investments in one place. Barclays, ABN Amro and few Europe based banks are supported but one must check at Mint for the specific details.

4. PRIVACY ISSUES

Cloud computing makes use of virtualization and its services are provide using internet. Both virtualization and internet are vulnerable to different types of attacks by hackers. Hence privacy is worth discussing with respect to cloud computing.

When Mint like services is taken into considerations, they are the main interest area of hackers. So it is very important to provide privacy to such sensitive information, user use to access cloud services. Also when we think of using cloud for business applications, confidential information such as bids, passwords, Account number etc , if leaked out can be disastrous. Hence care should be taken to provide such details only to the authenticated user. To provide authentication, we proposed to make use of digital signatures. Digital signature is a proof of being an authenticated user and it will be easier for cloud service providers to recognize its users. So the characteristics feature of multi-tenancy will also be implemented easily by making use of digital signature.

5. SECURITY ISSUES

Innately, Internet is communication infrastructure for cloud providers that use well-known TCP/IP protocol which users' IP addresses to identify them in the Internet. Similar to physical computer in the Internet that have IP address, a virtual machine in the Internet has an IP address as well. A malicious user, whether internal or external, like a legal user can find this IP addresses as well. In this case, malicious user can find out which physical servers the victim is using then by implanting a malicious virtual machine at that location to launch an attack [5]. Because all of users who use same virtual machine as infrastructure, if a hacker steals a virtual machine or take control over it, he will be able to access to all users' data within it. Therefore, The hacker can copy them into his local machine before cloud provider detect that virtual machine is in out of control then the hacker with analysis the data may be find valuable data afterward[6].

6. RIJNDAEL ENCRYPTION ALGORTIHM

Rijndael is the algorithm, selected by the U.S. National Institute of Standards and Technology (NIST) as the candidate for the Advanced Encryption Standard (AES). It was selected from a list of five finalists that were themselves selected from an original list of more than 15 submissions. Rijndael will begin to supplant the Data Encryption Standard (DES) - and later Triple DES - over the next few years in many cryptography applications. The algorithm was designed by two Belgian cryptologists, Vincent Rijmen and Joan Daemen, whose surnames are reflected in the cipher's name.

The Rijndael algorithm is a new generation symmetric block cipher that supports key sizes of 128, 192 and 256 bits, with data handled in 128-bit blocks. Rijndael uses a variable number of rounds, depending on key/block sizes, as follows: 9 rounds if the key/block size is 128 bits, 11 rounds if the key/block size is 192 bits, and 13 rounds if the key/block size is 256 bits.

Rijndael is a substitution linear transformation cipher. It use triple discreet invertible uniform transformations (layers). Specifically, these are: Linear Mix Transform; Non-linear Transform and Key Addition Transform. Even before the first round, a simple key addition layer is performed, which adds to security. Thereafter, there are Nr-1 rounds and then the final round. The transformations form a State when started but before completion of the entire process [7].

7. VII. DIGITAL SIGNATURE WITH RIJNDAEL ALGORITHM TO ENHANCE DATA SECURITY IN CLOUD

Digital signatures rely on certain types of encryption to ensure authentication. Encryption is the process of taking all the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode. In Digital Signature, software will crunch down the data, document into just a few lines by a using "hashing algorithm".

These few lines are called a message digest. Software then encrypts the message digest with his private key. Then it will produce digital signature .Software will Decrypt the digital signature into message digest with public key of sender's and his/her own private key. We are using Digital signatures so that we are able to distribute software, financial transactions, over the network and in other cases where it is important to detect forgery and tampering [1].

Then, we are using Rijndael algorithm to encrypt the data, which will make it more secure, on the fly. Finally encrypted data is stored on cloud. So it will definitely enhanced security of data in cloud.

8. VIII. PROPOSED WORKING MODEL OF DIGITAL SIGNATURE WITH RIJNDAEL ALGORITHM

Now, we explain how actual the proposed system would work. Suppose, C1 is cloud service provider (csp) and C2 is its user or client. Now C2 expects C1 to provide him secured cloud services. Suppose C2 wants some data stored in cloud. Now we explain the process in stepwise manner as follows.

Step1: C1 takes the required data file from the cloud.

Step2: Now the original data file is crunched using some hash function into message digest.

Step 3: C1's software then encrypts the message digest with his private key. The result is the digital signature.

Step 4: Using Rijndael Algorithm, C1 will encrypt digitally signed signature with C2's public key and C2 will decrypt the cipher text to plain text with his private key and C1 public key for verification of signature.

9. CONCLUSION

The combination of digital signature and Rijndael algorithms will undoubtedly enhance the security of data in cloud. This may encourage the large scale companies to pave their ways towards cloud, as the biggest concerns of privacy and security associated with cloud can be deal with, this implementation hereafter.

10. REFERENCES

[1] http://en.wikipedia.org/wiki/Digital_signature

[2] Farzad Sabahi, presented "Cloud computing security threats and responses" at Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference

[3] Jianfeng Yang and Zhibin Chen presented "Cloud Computing Research and Security Issues", at Computational Intelligence and Software Engineering (CiSE), 2010 International Conference.

[4] Rich Maggiani, solari communication. “Cloud computing is changing how we communicate”.
[5] N. Mead, et ai, prepared "Security quality requirements Engineering (SQUARE) methodolgy," at Carnegie Mellon Software Engineering Institute.
[6] J. W.Rittinghouse and J. F.Ransome, Cloud Computing: Taylor and Francis Group, LLC, 2010.
[7] www.efgh.com/software/rijndael.htm