International Journal of Computer Trends and Technology- volume4Issue3- 2013

Efficient Framework for Deploying Information in Cloud Virtual Datacenters with Cryptography Algorithms

Radhika G[#1], K.V.V. Satyanarayana[*2], Tejaswi A[#3]
[1,2,3] Dept of CSE, K L University, Vaddeswaram-522502, Guntur Dist., Andhra Pradesh, India

Abstract*-- Aim of this paper is to protect the data stored on cloud by using security algorithms. The use of cloud computing has increased rapidly in many organizations, but, still there is a major problem, i.e., security threat for the data that is before uploading information into virtual data centers. Due to data security concern with cloud computing many business organizations have fear in uploading and storing their data in Cloud. So the most challenging task of the business organizations is to provide high security for their data since the data are sensible related to their business. To ensure the privacy of data, we proposed a method of providing security by implementing cryptography algorithms using Microsoft windows azure to the data that will be stored in the third party area.

Index Terms: Cloud computing, cryptography, Windows Azure, Encryption and Decryption

1. INTRODUCTION

Cloud computing, which gets its name as a representation for the Internet [1], is becoming a popular term and has been used by an increasing number of organizations. In cloud computing environment, services are not provided by a single server or a small group of servers; instead, various computing and storage services are provided by some collection of data centers owned and maintained by a third party [2].

Cloud computing service providers provide their services in a number of fundamental models. The most widely used models are software as a service, platform as a service, and infrastructure as a service.

Software as a service (SaaS) is the capability provided to consumers to use the provider's applications running on a cloud infrastructure. It delivers the applications to users over internet. Instead of installing and maintaining data, the users simply access data through internet. Users have no control over underlying infrastructures, including network, servers, operating systems, storage, or even individual application capabilities [3].

Platform as a service (PaaS) is the capability provided to consumers to deploy onto the cloud infrastructure. It supplies all the resources required to build applications and services completely from the internet. Users have no control over the underlying infrastructure.

Infrastructure as a service (Iaas) is the capability provided to user's virtual storage, virtual machines and other hardware asserts. It differs from both SaaS and Paas. It is mainly used for storage purpose. On these resources, users may organize and run other software and web and console applications, or even operating systems, such as Linux or Windows.

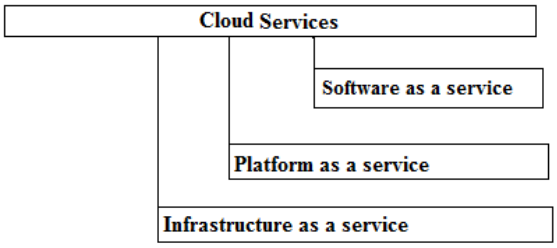

Fig 1: Types of Cloud Services

Additionally, there are some other models, including communication as a service (CaaS) and monitoring as a service (MaaS) [4].

While cloud computing is more and more popular, security becomes a great concern due to the distributed nature of cloud. For example, data in cloud is stored remotely, completely out of the

control of the data owner. Within cloud environment, users lose the control over physical security [4]. Users may have to share computing resources, including CPU time, network bandwidth, data storage space, with other users. It is possible for a user's data to be exposed to another user without their knowledge and control. To minimizing the security problem, implementing cryptography algorithms into cloud environment.

2. CRYPTOGRAPHY

Cryptography is the study of mathematical techniques for all aspects of information security. The conversion of data into a secret code for transmission over a public network, which means, the original text is turned into a coded equivalent called "cipher text" through an encryption algorithm. The cipher text is decrypted at the receiving end and turned back into plaintext. Cryptography is achieved by three methods, those are:

i. Symmetric Crypto System
ii. Asymmetric Crypto System
iii. Hash Functions

2.1 Symmetric Crypto System:

In symmetric crypto system, the encryption and decryption done by a single key i.e., shared key. Both sender and receiver share the same key and they maintained that shared key in highly confidential manner.

Ex:-DES, AES, Triple DES and Blowfish algorithms.

2.2 Asymmetric Crypto System:

In asymmetric crypto system, the encryption and decryption done by two different keys, those are

a. Public Key
b. Private Key

Public Key: The public key is identified by any person and can be used to encrypt messages and verify signatures.

Private Key: The private key is identified by only to the particular person i.e., recipient, used to decrypt messages and verify signatures.

Public key cryptography is asymmetric because, those who encrypt messages or verify signatures cannot decrypt messages or create signatures.

Ex:- RSA

2.3 Hash Function

A hash function is a function which maps an input of arbitrary length into a fixed number of output bits. In order to be functional for cryptographic applications, a hash function has to satisfy some additional requirements. One can discriminate two types of hash functions [6]. A MAC (Message Authentication Code) that uses a confidential key, and an MDC (Manipulation Detection Code) that works without a key. Hash functions can be used to protect the authenticity of large quantities of data with a short secret key (MAC), or to protect the authenticity of a short string (MDC).

Ex: SHA family, HMAC

By implementing these cryptography techniques into cloud environment, there is a chance to overcome the security problem in cloud environment. In this paper, we are using windows azure for deploying the information into cloud environment.

3. WINDOWS AZURE

Windows Azure is a platform for running Windows applications and storing data in the cloud. Microsoft Windows Azure runs on machines in Microsoft data centers instead of providing software that Microsoft customers can install and run themselves on their own computers, Azure is a service: Customers use it to run applications and store data on Internet-accessible machines owned by Microsoft. Those applications might offer services to business organizations, to consumers, or both.

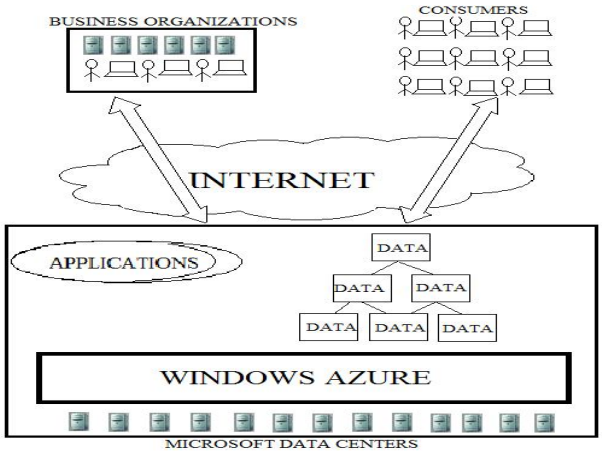

Fig 2: Windows azure applications run in Microsoft data centers and are accessed through internet.

4. IMPLEMENTATION

To implement cryptography algorithms to data before the users uploading information into virtual data centers. Here, we are implementing three cryptography algorithms (RSA, SHA1 and MD5) for providing security to information.

4.1 Algorithms

i. RSA Algorithm:

RSA algorithm is an asymmetric encryption, in which, the encryption and decryption done by two different keys i.e., Public key and Private Key

The secrecy of RSA is depends upon the size of the key[5]. If the key size is increased then security level is also increased. The minimum key size of RSA is 1024.

ii. SHA1 algorithm:

The acronym for SHA is Secure Hash Algorithm. The purpose of SHA1 is authentication not encryption. In SHA1, the user gives an arbitrary size of input and it produces a fixed size of hash function and the size of hash function for SHA1 is 160 bits.

iii. MD5:

The acronym for MD5 is Message Digest. MD5 is one way of hash function. MD5 algorithm takes an input of arbitrary length and produces a message digest i.e., 128 bits long. The size of hash function for MD5 is 128 bits.

Launch the three algorithms in Microsoft visual studio 2010.

4.2 Visual Studio2010

Visual Studio 2010 is an absolute development environment from Microsoft for creating web applications and client (Windows) applications. In contrast, Visual Studio 2010 Express is a set of free, entry-level products that features efficient interfaces and core capabilities that focus on providing the tools that you need for creating applications for a single platform. These are the steps for encrypt and decrypt of the plain text.

Step1: Create key pairs of RSA algorithm

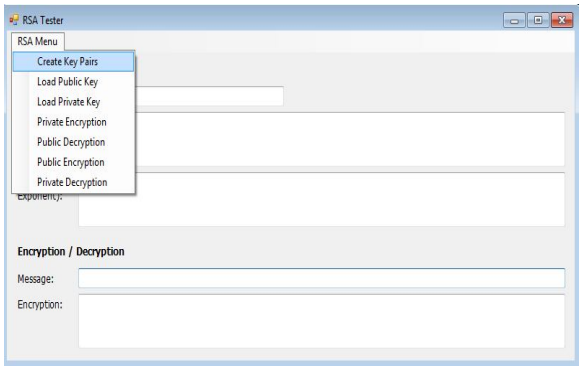

Fig 3: Menu form of RSA algorithm

Step 2: After creating the key pairs successfully, we can load the public and private keys and calculate the module and exponent values.

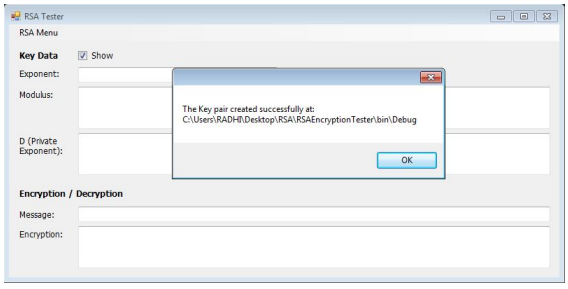

Fig 4: Successfully loaded key pairs of RSA algorithm

Step 3: After calculating the module and exponent values, the user enters the plain text and click private encryption in RSA menu.

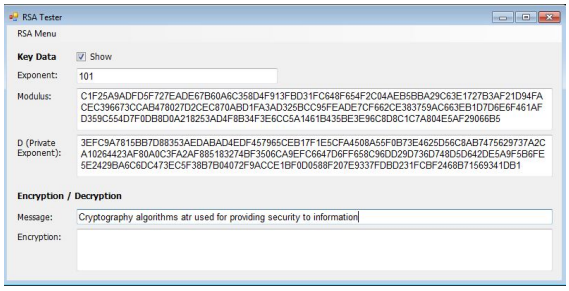

Fig 5: Enter plaintext

Step 4: After select the private encryption, the cipher text will be appears in the encryption box. Here, the encryption and decryption can be done in two ways.

i. Private encryption and public decryption
ii. Public encryption and private decryption

If we select the private encryption in RSA menu, for decryption purpose we have to choose only public decryption and if, we select public encryption in RSA menu, for decryption purpose we have to choose only private decryption.

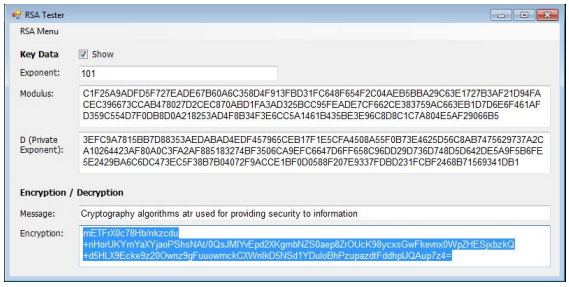

Fig 6: Encrypts the plaintext using RSA algorithm

Step 5: This is the decrypted message.

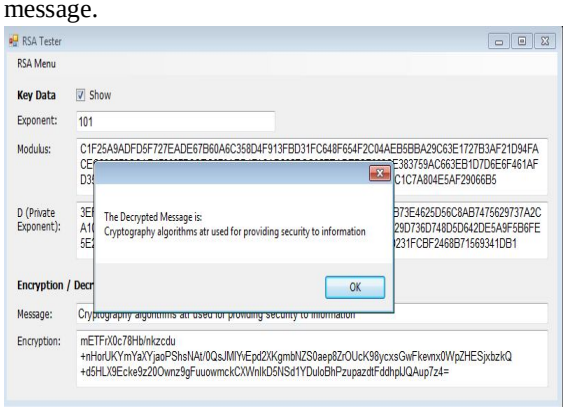

Fig 7: Decrypts the plaintext using RSA algorithm

Step 6: Enter Plaintext for SHA1 and MD5 algorithms

Fig 8: Enter plain text for SHA1 and MD5 algorithms

Step 7: This is the SHA1 algorithm. Here, we can enter the message into Enter String text box and then click SHA1 encryption. The hash function will be appears in Encrypted string textbox. In sha1, it takes input as arbitrary size and the key length is constant i.e., 28.

Fig 9: Hash Key value for SHA1 algorithm

Step 8: This is the MD5 algorithm. Here, we can enter click MD5 encryption. The hash function will be appears in Encrypted string textbox. In MD5, it takes input as arbitrary size and the key length is constant i.e. 24 bits.

Fig 10: Hash Key value for MD5 algorithm

4.3 Setting up the Development Environment

Before you can initiate developing your Windows Azure application, you need to get the tools and set-up your development environment.

1. Microsoft Visual Studio 2010
2. IIS7
3. Windows Azure SDK for .NET

Once the installation is finish, you will have everything necessary to start developing. The Software Development Kit (SDK) includes tools that let you easily develop Windows Azure applications in Visual Studio.

5. RESULTS

For enhancing privacy in cloud, we implemented three cryptography algorithms into cloud environment. For deploying application, we have to use Microsoft windows azure, launch the algorithms into visual studio2010 and execute the algorithms.

1. In RSA, it takes input size as 280 bits and key size is 172 bits. Here, the key is very strong.
2. In SHA1, it takes input as arbitrary size and gives a fixed size key i.e., 28 bits.
3. In MD5, it takes input as arbitrary size and gives a fixed size key i.e., 24 bits.

By comparing the SHA1 and MD5, SHA1 is superlative algorithm because it takes input as arbitrary size and produces a strong hash key. When compared to SHA1 with RSA algorithm, RSA provide more security than SHA1 but it only takes 280 bits as input.

ALGORITHM	MAXIMUM INPUT SIZE	KEY SIZE
RSA	280 bits	172bits
SHA1	Arbitrary Size	28bits
MD5	Arbitrary Size	24 bits

Table 1: Results for Cryptography Algorithms

6. CONCLUSION

In this paper, we have implemented RSA, SHA1 and MD5 algorithms and deploying information into cloud in secure way. From the results we obtained it is proved that Cryptography algorithms gives protection for the data, which is stored in Cloud. The users can store the information by using this security application. Even if anyone happens to read the data accidentally, the original meaning of the data will not be understood. Also we argued that the importance of security and privacy of data stored and retrieved in the cloud. We utilize Cryptography algorithms and

Windows Azure to provide efficient and secured data storage scheme.

7. REFRENCES

[1] A. Velte, T. Velte, and R. Elsenpeter, Cloud computing: a practical approach, New York: McGraw-Hill, 2010.

[2]. H. Jin, S. Ibrahim, T. Bell, L. Qi, H. Cao, S. Wu, and X. Shi, "Tools and technologies for building clouds", in Cloud Computing: Principles, Systems and Applications, N. Antonopoulos and L.Gillam, Eds, London: Springer, 2010.

[3]. National Institute of Science and Technology, The NIST Definition of Cloud Computing, 2011.

[4].J.Rittinghouse and J. Ransome, "Cloud computing: Implementation,management and security", Boca Raton: CRC Press, Taylor and Francis Group, 2010.

[5]. N. Saravanan, A. Mahendiran, N. Venkata Subramanian and N. Sairam "An Implementation of RSA Algorithm in Google Cloud using Cloud SQL" Research Journal of Applied Sciences, Engineering and Technology 4(19): 3574-3579, 2012.

[6]. William Stallings, "Cryptography and Network Security Principles and PracticSes", 4th Edition, 2005.