IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

TREM: A New Cloud Security Algorithm

V.Poongodi[1], Dr.K.Thangadurai[2]

Research Scholar, Manonmaniam Sundaranar University, Tirunelveli[1]

Head, PG & Research Dept. of Computer Science, Government Arts College, Karur[2]

Abstract: Cloud computing brings out a wide range of benefits including configurable computing resources, economic savings, and service flexibility. However, security concerns are shown to be the primary obstacles to a wide adoption of clouds. The new concepts that clouds introduce, such as multi-tenancy, resource sharing and outsourcing, create new challenges to the cloud data security. To address these challenges, it is necessary to tune the security measures developed for traditional computing systems and proposing a new security algorithms. In this paper a new cloud security algorithm is proposed by combining different cryptographic techniques in a hybrid manner.

Keywords: Cloud Computing, Cloud Computing Architecture, Data Security and issues in cloud computing, TREM.

I. INTRODUCTION

Cloud computing is an internet based computing and it is evolved from grid computing, utility computing, parallel computing, distributed computing and virtualization. As per the definition of NIST cloud computing is divided into different categories as Private, Public, Community and Hybrid cloud. This techniques offers various services like software a***s a service (SaaS):*** SaaS refers to the software available on the internet. It includes youtube, facebook, google applications. ***Platform as a service (PaaS):*** an operating system, hardware, and network are provided, and the customer installs or develops its own software applications. It include Amazon DB/S3[1], Google AppEngine. ***Infrastructure as a service (IaaS):*** provides just the hardware and network; the customer installs or develops its own operating systems, software and applications. Examples of IaaS providers include Amazon EC2, GoGrid, FlexiScale[2].

II. ESSENTIAL CHARACTERISTICS OF CLOUD COMPUTING

A. ***Self-service on Requirement:*** The user possibly will make a decision on the use of computing amenities such as server time and network storage alone, based on of their current needs, with no excess communication with dissimilar service providers [3].

B. ***Broad Network Access:*** Computing amenities possibly be accessed over the network through the use of standardized mechanism that hold up different clients, like mobile phones, tablets, laptops and work stations [3].

C. ***Location-Independent and Resource Pooling:*** Computing resources are pooled to serve multiple users using a multi-tenant model, with different physical and

D. virtual resources dynamically assigned and reassigned according to users' demand. Applications require resources. However, these resources can be located anywhere in the geographic locations physically and assigned as virtual components whenever they are needed [3].

E. ***High Elasticity:*** The consumer may easily increase or decrease the computing capacities afforded using the current requirements. The capacities are unlimited for the user [3].

F. ***Scalability:*** It enables new nodes to be added or dropped from the network like physical servers, with limited modifications to infrastructure set up and software. Cloud architecture can scale horizontally or vertically, according to users' demand [3].

III. CLOUD COMPUTING ARCHITECTURE

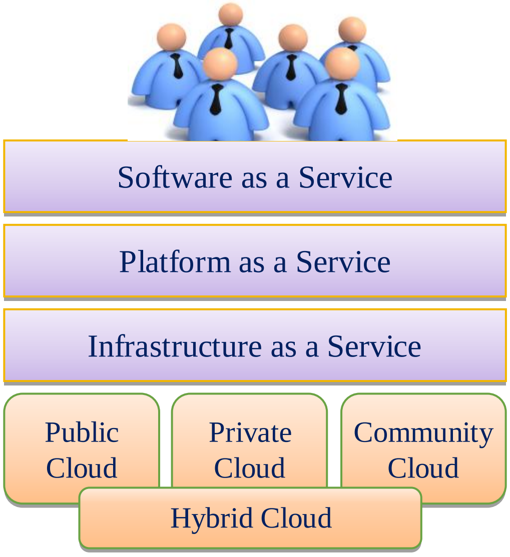

Figure 1. Cloud Computing System Architecture

The current cloud computing system consists of three layers: software layer, platform layer and infrastructure layer, as shown in Figure 1 [4]. The software layer

DOI 10.17148/IJARCCE.2016.54239

provides the interfaces for users to use CSPs' applications running on a cloud infrastructure. The platform layer provides the operating environment for the software to run using system resources. The infrastructure layer provides the hardware resources for computing, storage, and networks [5].

IV. ADVANTAGES OF CLOUD COMPUTING

1. ***Lesser Cost:*** Pay as you go, negligible hardware investments or software licenses.
2. ***Added Performance:*** on demand processing time, even HPC, if required.
3. ***Fewer Maintenance:*** somebody else manages the servers along with core software.
4. ***Extra Security:*** easily repair, enforcement of policies, centralized data.
5. ***Extra Wide Storage Capacity:*** Use it when you require it.

V. DISADVANTAGES OF CLOUD COMPUTING

1. ***Dependency on Internet Connectivity:*** Requires a regular connection.
2. ***Loss of Control:*** The trouble of someone else hosting hardware, software and data, which outcome in security concerns.
3. ***Unpredictable Cost:*** Pay as you go means that the price of computing will be differ every month.

VI. DATA SECURITY IN CLOUD COMPUTING

Major concern is security of data. Data relocation on high level has negative implications for data safety and data security as well as data availability. Thus the main apprehension with reference to safety of data residing in the Cloud is: at the rest how to safe security .Although, customers know the location of data and there in no data mobility, there are question relating to its security and secrecy of it. No confusion the Cloud Computing area has become bigger because of its wide network access [6].

VII. SECURITY ISSUES IN CLOUD COMPUTING

*A. **Privacy and Confidentiality:*** Once the client show data to the cloud there should be some security that access to that data will only be incomplete to the authorized access. The client is being provided assurance and proper practices and safe policies and procedures should be in place to guarantee the cloud users of the data safety [7].

*B. **Data Integrity:*** Cloud Service Providers should apply mechanisms to ensure data truthfulness and be able to tell what happened to a definite data set and at what point. The client should be aware by the data provider the origin and the integrity mechanisms [7].

*C. **Data Location and Relocation:*** Cloud computing offers a high amount of data mobility. Consumers do not always know location of their data. However, when an venture has some sensitive data that's reserved over a storage device in the Cloud, they will often keep asking the career than it. They will also aspiration to specify a chosen location. The cloud providers should take accountability to guarantee the security of systems (including data) and gives robust certification to protect customer's information [7].

*D. **Data Availability:*** Customer information is normally saved in chunk on different servers often residing in different locations or even in different Clouds. In such cases, data availability becomes a major legitimate issue because use of un-interruptible and seamless provision becomes relatively difficult [7].

VIII. MICROSOFT WINDOWS AZURE

Azure is Microsoft's Cloud computing[9] offering to build and deploy applications on a Pay-per-use basis. Azure is a comprehensive set of storage, computing, and networking infrastructure services that reside in Microsoft's network of datacenters. Which provides a scalable infrastructure for consumer to run and host web based applications. To support cloud applications and data, Windows Azure has five components, as shown in figure 2.

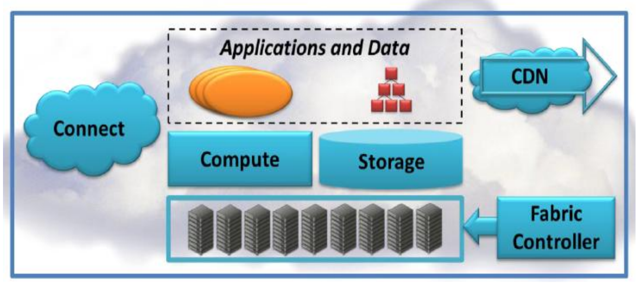

Figure2: Microsoft Windows Azure.

Compute: runs applications in the cloud. Those applications largely see a Windows Server environment, although the Windows Azure programming model isn't exactly the same as the on-premises Windows Server model.

Storage: Windows Azure provides multiple storage services that are highly durable, scalable as well as constantly available. Azure offers three types of storage services, BLOB, Table and Queues, which cater to unstructured, structured as well as transient data requirements.

Fabric Controller: deploys, manages, and monitors applications. The fabric controller also handles updates to system software throughout the platform.

Content Delivery Network (CDN): speeds up global access to binary data in Windows Azure storage by maintaining cached copies of that data around the world.

Connect: allows creating IP-level connections between on-premises computers and Windows Azure applications.

DOI 10.17148/IJARCCE.2016.54239

IX. PROPOSED WORK

TREM

The proposed TREM Security service algorithm combines two efficient cryptographic algorithms. In this service the original text is converted in to cipher text using the message digest technique. If a cryptographic algoithm use the message digest technique it is very difficult to extract the information from the cipher text. The main advantage in ths service the size of the cipher text is small. Hence it doesnot have difficult in the cloud storage. Figure 3 show the proposed security service algorithm to enhance the data security in cloud computing. The proposed algorithm is analysed in the cloud environment as a service

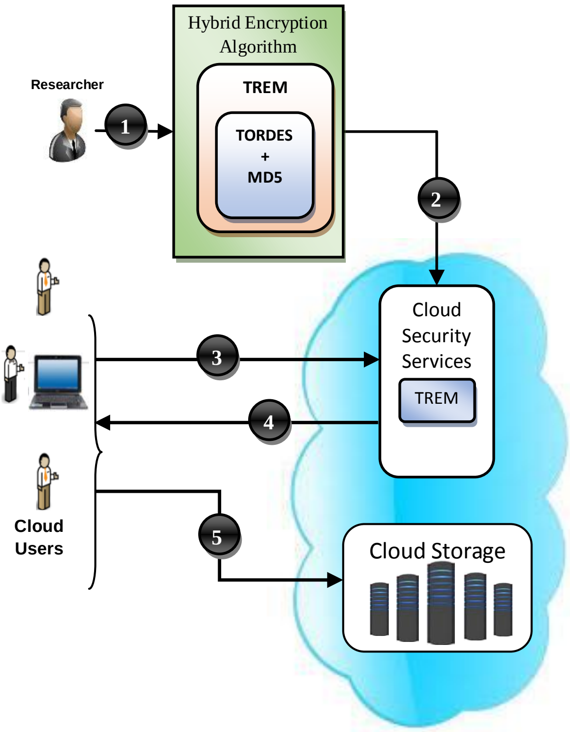

Fig 3. TREM Hybrid Security Service Algorithm

The working process of the proposed TREM algorithm is clearly explained in the following steps to know how the cloud users' data are stored in a highly secured way over the cloud storage environment.

STEP 1: *Researcher proposed security service algorithms using different hybrid cryptographic techniques.*

STEP 2: *The Proposed **TREM** algorithm is deployed in the cloud environment as security services.*

STEP 3: *The cloud users want to store their data in the cloud storage environment. For this user request any one of the cloud security services in the cloud environment.*

STEP 4: *The requested cloud security service is offered to the cloud user to encrypt or to decrypt their data.*

STEP 5: *Finally, the cloud users encrypt / decrypt or their data to store or to retrieve form the cloud storage environment.*

X. SIMULATION RESULT

The proposed algorithm is implemented using .NET. The simulation analysis is perfromend in the cloud environment(Microsoft Azure) with different data input. The time taken to Encrypt and Decrypt the given input data is calculated for the proposed TREM and Existing RSA,AES and BlowFish Algorithms. The results are compared and tabulated in table 1 and it is graphically represented in figure 4.

Table 1. Comparative Analysis based on Encryption Time

Size	**Algorithms**			
	RSA	**AES**	**Blowfish**	**TREM**
	Encryption Time(Minutes)			
1 MB	14.6754	13.9436	10.8872	4.7983
5 MB	19.7381	17.8764	13.7968	7.8257
10 MB	24.6786	21.7548	17.9647	12.9327
15 MB	27.8654	24.6979	21.6548	14.8753

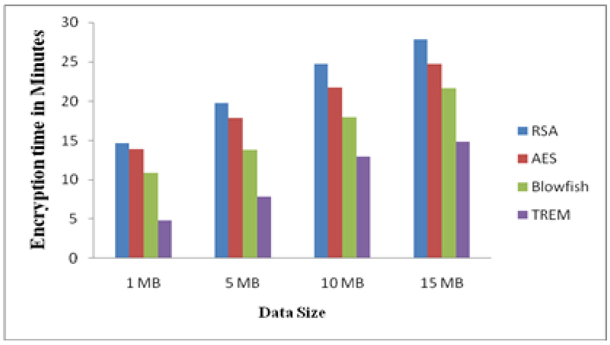

Fig 4. Comparative Analysis based on Encryption Time

Table 2 presents the performance comparison of decryption with existing techniques. The time taken by the existing and proposed decryption algorithms is calculated for different sizes of data.

Table 2. Comparative Analysis based on Decryption Time

Size	**Algorithms**			
	RSA	**AES**	**Blowfish**	**TREM**
	Decryption Time(Minutes)			
1 MB	11.9738	9.7382	7.6347	3.9627

DOI 10.17148/IJARCCE.2016.54239

5 MB	15.7357	13.8172	10.8796	6.7635
10 MB	20.6937	18.9073	15.9363	10.8214
15 MB	24.8392	20.6382	17.9826	13.6376

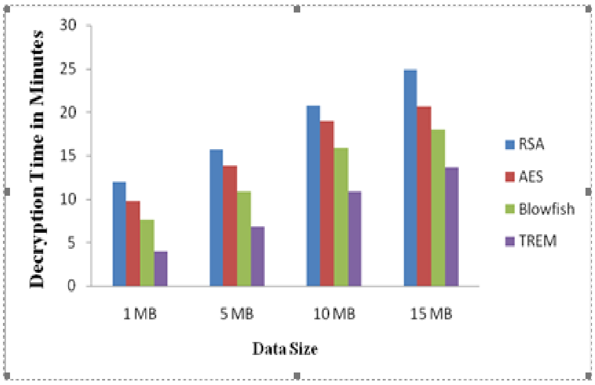

Fig 5. Comparative Analysis based on Decryption Time

Figure 5 presents the performance of existing and proposed algorithms based on the time taken for decryption process. The result shows that compared to the existing algorithms, the proposed TREM hybrid security algorithm has taken minimum time duration for decryption of different sizes of data.

Table 3 and Figure 6 represent the comparison of security levels. The result shows that compared to the existing algorithms, TREM hybrid Security algorithm produces maximum security for cloud data. Security level of TREM is 87%, RSA is 82%, AES is 79% and Blowfish is 74%. TREM shows maximum security level when compared with existing encryption techniques.

Table 3. Comparison of Security Levels of Existing and Proposed Algorithms

Algorithms	Security Level(%)
BlowFish	74
AES	79
RSA	82
TREM	87

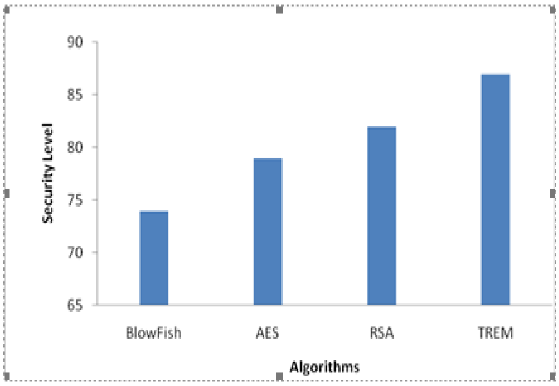

Fig 6. Comparison of Security Levels of Existing and Proposed Algorithms

XI. CONCLUSION

It is indeed that cloud computing can prove to be a boon in today's work environment hence this paper deals with data security issues related to cloud computing. This issue is overcome by proposing new data security algorithm using hybrid cryptographic technique is used. The proposed algorithm is converted into cloud security service. The proposed TREM cloud service is compared with the existing services and the result shows that the proposed algorithm improve the data security.

REFERENCES

[1] Sunil Sanka, ChittaranjanHota, MuttukrishnanRajarajan, "Secure Data Access in Cloud Computing," in IMSAA '10, 2010, p. 1-6.

[2] Jing-Jang Hwang and Hung-Kai Chuang, Yi-Chang Hsu and Chien-Hsing Wu, "A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service," in ICISA '11, 2011, p. 1-7.

[3] Peter Mell, and Timothy Grance, "The NIST Definition of Cloud Computing", The National Institute of Standards and Technology, USA, 2011.

[4] BhagyashreeAmbulkar and VaishaliBorkar, "Data Mining in Cloud Computing", MPGI National Multi Conference 2012 (MPGINMC-2012), 7-8 April 2012.

[5] Ahmad Azarnika, JafarShayana, MojtabaAlizadehb and SasanKaramizadeha, "Associated Risks of Cloud Computing for SMEs", Open International Journal of Informatics, 2012, pp. 37-45.

[6] Aiiad A. Albeshri, "Outsourcing Data Storage without Outsourcing trust in Cloud Computing", Queensland University of Technology, Australia, 2013.

DOI 10.17148/IJARCCE.2016.54239