International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 14 (2015) pp 33990-33995

An Enhanced Data Security Algorithm for Cloud Environment

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

[1]*Research Scholar, Manonmaniam Sundaranar University, Tirunelveli*
E-mail:vmpoongodi@yahoo.com
[2]*Head, PG&Research Dept. of Computer Science, Government Arts College, Karur.*
E-mail:ktramprasad04@yahoo.com

Abstract
Cloud computing is the delivery of computing services over the Internet. This technique allows the individuals and businesses users to access the 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. In cloud computing data is travelling over the internet and is stored in remote locations. The data stored in the remote location needs high security. To improve the security in cloud computing lot of security algorithms were developed. But still many research work is going on to improve the data storage security in cloud environment. In this paper an enhanced security algorithm is proposed with the hybrid cryptographic techniques. The proposed algorithm is compared with the existing algorithms. The result shows that the proposed algorithm performs better than the existing security algorithms.

Keywords: **Cloud Computing, Service & Deployment Models, Data Security, Microsoft Azure**

I. INTRODUCTION

Cloud Computing is the name given to the recent trend in computing service provision. This trend has seen the technological and cultural shift of computing service provision from being provided locally to being provided remotely and en masse, by third-party service providers [Aro, 2011].
"NIST definition of cloud computing Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." It provides computational resources like server, storage, software, memory, network etc., as on-demand services [Kam, 2010]. It helps to reduce the computational infrastructure investment and maintenance cost of IT requisite for Small and Medium scale Enterprises (SMEs) [Sun, 2012].It provides Everything(X) as a Service (XaaS),[Xia, 2010] where 'X' denotes software, OS, server, hardware, storage, etc. Cloud services are scaling up and down based on the users' demand [Wil, 2005].
The major feature of cloud computing is that it allows sharing and scalable deployment of services as needed by the users from any location. Cloud computing saves time and money during software up-gradation; cloud services are updated by the provider; so users are always working on the latest platform [Ans, 2013].
Now a day's Security of data has become a big distress. High levels of data repositioning have off-putting implications for data security and data shield as well as data availability [Sun, 2012]. Thus the main worry regarding security of data residing in the Cloud is: how to make sure the security of data which is at rest.

II. CLOUD SERVICE MODELS

Cloud Computing technique contains three different service models, namely, IaaS, PaaS and SaaS which is shown in fig1.

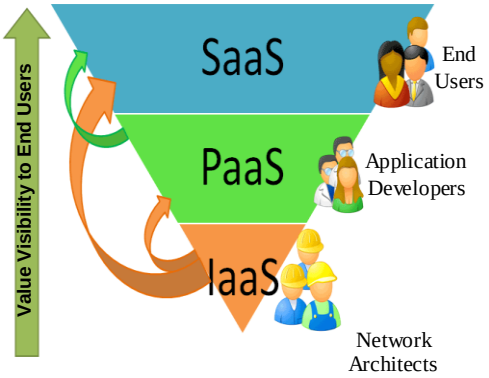

Fig 1. Cloud Service Models

Infrastructure as a Service: IaaS provide on-demand provisioning of infrastructural resources and does not manage or control the infrastructure and only manage and control the storage, application and selected network components[May, 2014].

Platform as a Service: PaaS providing software development frameworks and platform layer resources including operating system support. In PaaS user controls their application and does not manage servers and storage [May, 2014].

Software as a Service: SaaS providing on demand applications all over the Internet. In SaaS user does not control or manage the servers, storage, network and application [May, 2014].

III. CLOUD DEPLOYMENT MODELS

The deployment models in cloud computing are divided into four major components they are, Private, Public, Community and Hybrid Clouds which is illustrated in fig 2.

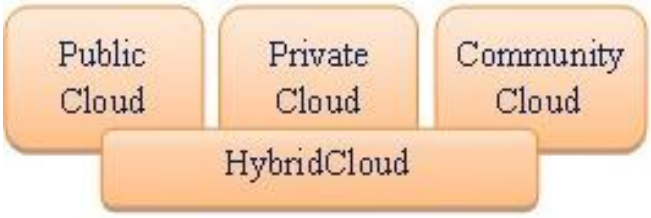

Fig 2. Cloud Deployment Models

Private Cloud is operated solely for a single organization and managed by the third party. It is also known as internal cloud. These clouds are hosted by third parties, rather than being hosted on dedicated servers. Hosting companies operate large data centres and people who require their data to be hosted, buy or lease storage capacity from providers and use it for their storage [Xia, 2010].

Public Cloud or external cloud describes cloud computing in the traditional mainstream, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications or web services. The resources are provisioned from an off-site third-party CSPs who bill on a utility computing basis [Xia, 2010].

Community Clouds are only accessible to a few numbers of clients with known features. This option of deployment is more expensive but may offer a higher level of privacy, security and/or policy compliance [Xia, 2010].

Hybrid Clouds are composition of two or more clouds (public or private). By integrating multiple cloud services, users may be able to ease the transition to public cloud services. A hybrid storage cloud uses a combination of public and private storage clouds [Xia, 2010].

IV. 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 and flexibility [Joh, 2009].

V. SECURITY ISSUES IN CLOUD COMPUTING

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 [Kev, 2010].

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 [Kev, 2010].

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 [Kev, 2010].

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 [Kev, 2010].

VI. MICROSOFT WINDOWS AZURE

Azure is Microsoft's Cloud computing 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 fig 3.

The AzureTM Services Platform (Azure) is an Internet-scale cloud computing and services platform hosted in datacenters created by Microsoft Corp., which provides an operating system and a set of developer services that can be used individually or together. The flexible and interoperable Azure platform can be used to build new applications to run from the cloud or enhance existing applications with cloud-based capabilities. Its open architecture gives developers the choice to build Web applications, applications running on connected devices, PCs, servers or hybrid solutions offering the best of both worlds(online and on-premise).

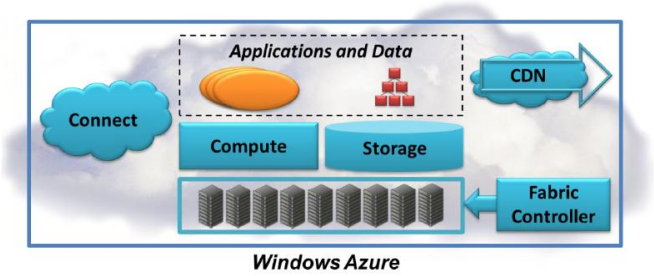

Fig 3: Windows Azure has five main parts: Compute, Storage, the Fabric Controller, the CDN, and Connect.

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.

VII. PROPOSED WORK

Cloud Computing is a new standard that provide the hardware and software resources according to the user needs. In this technology number of users stores their data on the cloud environment. Data storage security refers the security of data on the storage media. In cloud computing, data storage security has become on of the challenging task. Recent days, many researchers developed the cloud security by implementing security algorithm by combining more than one cryptographic algorithm (symmetric and asymmetric). But still the problem persists.

A. Symmetric Algorithm

TORDES Algorithm

TORDES is a block cipher algorithm. It is a unique and independent approach which uses several computational steps along with string of randomized operators and delimiter selections by using some suitable mathematical logic with transformation and mirror image operation. It is specially designed to produce different cipher texts by applying same key on same plain text. It is one of the best performing partial symmetric key algorithms particularly for the text message in its class. It also safeguard against various attacks like Brute-force because it is not fully dependent on the key and code cannot be deciphered by applying all possible combinations of keys. The following information invariably used in TORDES for encryption techniques.

1) 32 bit key.
2) Code sequence string generated from a particular process (Multithread).
3) Transformation of String.
4) Mirror image of String.
5) Lookup Table
6) Randomized delimiter string

B. Asymmetric Algorithm

RSA Algorithm

This is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption. Till now it is the only algorithm used for private and public key generation and encryption. It is a fast encryption[Uma,2010].

Algorithm:

Key Generation: KeyGen(p, q)
Input: Two large primes – p, q
Compute n = p. q
$\varphi(n) = (p - 1)(q - 1)$
Choose e such that $\gcd(e, \varphi(n)) = 1$
Determine d such that e. $d \equiv 1 \bmod \varphi(n)$

Key:

public key = (e, n)
secret key= (d, n)

Encryption:

$c = m^e \bmod n$
where c is the cipher text and m is the plain text.

C. Methodology

In this methodology an enhanced hybrid security service algorithm namely, **TOR** (***TO****rdes+****R****SA*) is proposed and this algorithm is combining by two cryptographic algorithms and the proposed TOR algorithm is deployed in the cloud environment (***Microsoft Windows Azure***) as a security services. The cloud users use this service to ensure the confidentiality in the cloud storage environment and it is illustrated in fig 4.

The proposed security services algorithm is coded using.Net and it is deployed in the cloud environment called Microsoft Windows Azure as a security service. The security measure of this algorithm is calculated by considering the time taken to encrypt and decrypt the user data in the cloud environment. The proposed TOR algorithm is compared with the existing asymmetric and symmetric algorithms namely, ***RSA, AES*** and ***BLOWFISH*** to prove that our algorithm performs better than the existing algorithms.

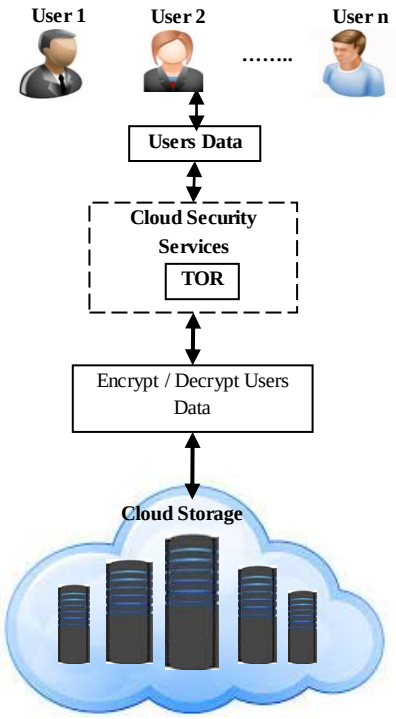

Fig 4. Methodology Diagram to enhance Data Storage Security in Cloud Environment

D. TOR Algorithm

In this security service algorithm TORDES and RSA were combined and proposed a new hybrid security service algorithm called TOR. The proposed TOR algorithm consists of both symmetric and asymmetric cryptographic algorithm. In this TORDES is a symmetric key algorithm whereas RSA is an asymmetric key algorithm. The proposed algorithm is implemented as a security service in the cloud environment. Figure 5 show the proposed security service algorithm to enhance the data security in cloud computing.

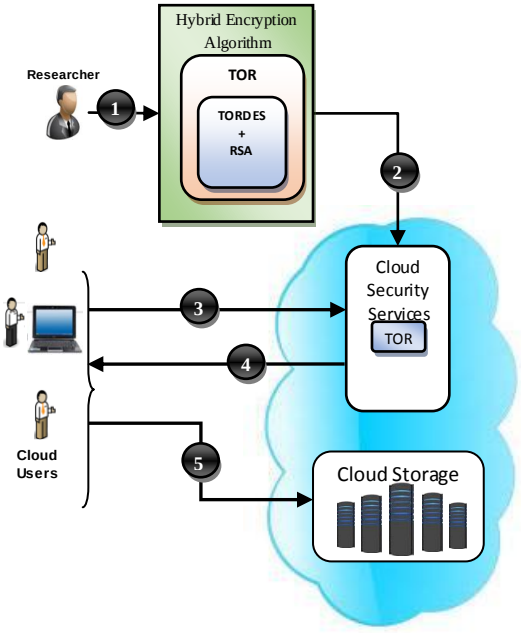

Fig 5. TOR Hybrid Security Service Algorithm

The working process of the proposed TOR 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 **TOR** algorithm is deployed in the cloud environment as security services.*

STEP 3: *The cloud users want to store their data in the cloud storge 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 from the cloud storage environment.*

E. Simulation Result

The proposed algorithm is implemented using.NET. The simulation analysis is performed 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 TOR and Existing RSA,AES and BlowFish Algorithms. The results are compared and tabulated in table 1 and it is graphically represented in figure 6.

TABLE 1 COMPARATIVE ANALYSIS BASED ON ENCRYPTION TIME

Size	Algorithms			
	RSA	AES	Blowfish	TOR
	Encryption Time (Minutes)			
1 MB	14.6754	13.9436	10.8872	5.7856
5 MB	19.7381	17.8764	13.7968	9.8798
10 MB	24.6786	21.7548	17.9647	14.6888
15 MB	27.8654	24.6979	21.6548	18.9799

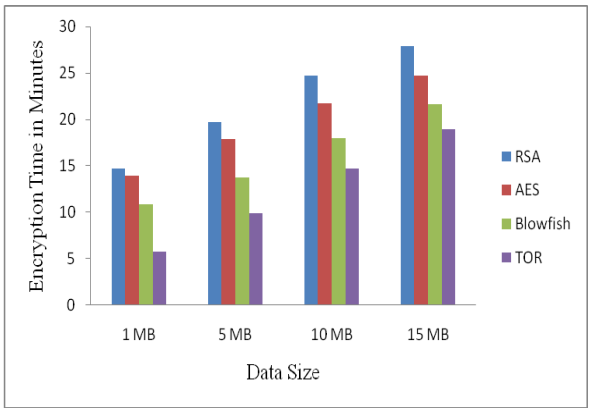

Fig 6. Comparative Analysis based on Encryption Time

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	TOR
	Decryption Time (Minutes)			
1 MB	11.9738	9.7382	7.6347	4.7454
5 MB	15.7357	13.8172	10.8796	8.6940
10 MB	20.6937	18.9073	15.9363	11.8132
15 MB	24.8392	20.6382	17.9826	16.9173

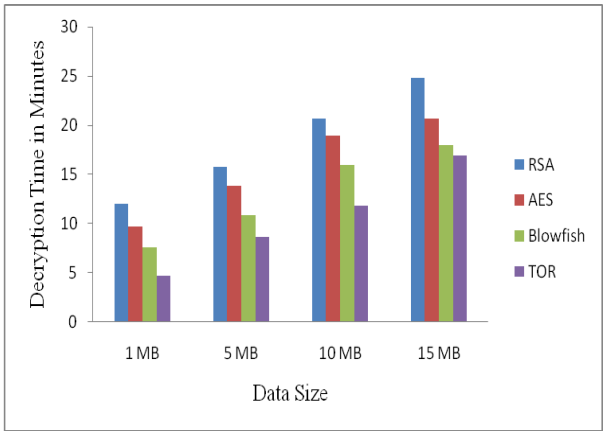

Fig 7. Comparative Analysis based on Decryption Time

Figure 7 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 TOR hybrid security algorithm has taken minimum time duration for decryption of different sizes of data.

Table 3 and Figure 8 represent the comparison of security levels. The result shows that compared to the existing algorithms, TOR hybrid Security algorithm produces maximum security for cloud data. Security level of TOR is 89%, RSA is 82%, AES is 79% and Blowfish is 74%. TOR 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
TOR	89

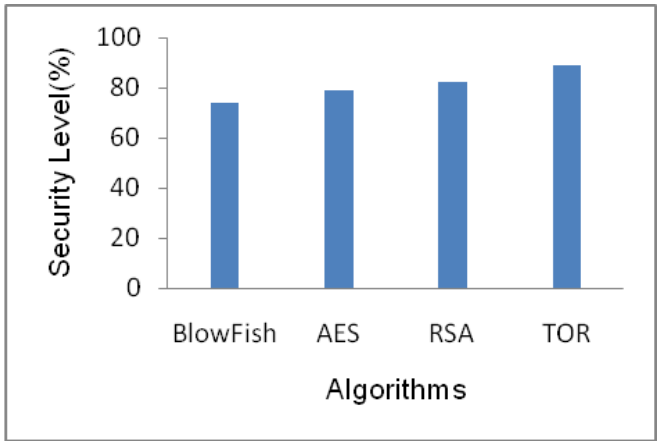

Fig 10. Comparison of Security Levels of Existing and Proposed Algorithms

VIII. CONCLUSION

Cloud data outsourcing helps to improve the business of the small enterprises at a low cost. Due to the security issue in cloud users are reluctant to outsource data in cloud storage.

Cryptographic techniques are used to ensure the confidentiality of the data in the cloud storage. In this paper an enhanced security service algorithm has proposed namely, TOR for secured cloud storage. It is one of the security services in cloud security service. TOR security service algorithm is provided through cloud security service as a security service in the cloud environment. The TOR is a hybrid encryption algorithm.

Simulation has been conducted using Microsoft Windows Azure with different sizes of data and performance has been analyzed in terms of time taken for encryption and decryption, and security level. From the results obtained, it is evident that the proposed TOR algorithm provides better security in lesser time than the existing security algorithms.

REFERENCES

1. Mayank Patwal_and Tanushri Mittal "A Survey of Cryptographic based Security Algorithms for Cloud Computing" International Journal of Technology Innovations and Research, 2014, pp. 1- 17.
2. Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen and Henghu Gong "The Characteristics of Cloud Computing", IEEE International Conference on Parallel Processing Workshops, 1530- 2016/10, 2010 pp. 275-279.
3. Sudha M., Monica M., "Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography", Advances in Computer Science and its Applications, volume 1, Issue 1, 2012, pp. 32-37.
4. John, H., L.M. Kaufman and Bruce, P., "Data security in the world of cloud computing" IEEE transactions Security & Privacy, 2009, pp. 61-64.
5. Kamara S. andLauter K., "Cryptographic cloud storage", IFCA/ LNCS 6054, Springer-verlag, Berlin

Heidelberg, 2010, pp.136-149.

6. Sunita Rani, AmbrishGangal "Cloud Security with Encryption using Hybrid Algorithm and Secured Endpoints", International Journal of Computer Science and Information Technologies, Volume 3, Issue 3, 2012, pp.4302 – 4304.
7. hManpreetKaur and Rajbir Singh, "Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing", International Journal of Computer Applications, Volume 70, Issue 18, 2013,pp.16-21.
8. AnshuParashar and RachnaArora, "Secure User Data in Cloud Computing Using Encryption Algorithms", International Journal of Engineering Research and Applications (IJERA), Volume 3, Issue 4, 2013, pp.1922-1926.
9. Kelsey Rauber, "Cloud Cryptography", International Journal of Pure and Applied Mathematics, Volume 85, Issue 1, 2013, pp.1-11.
10. Kevin Hamlen, Murat Kantarcioglu, Latifur Khan and BhavaniThuraisingham, "Security Issues for Cloud Computing", International Journal of Information Security and Privacy, Volume 4, Issue 2, 2010, pp. 39-51
11. William, S., "Cryptography and network security: principles & practices", Fifth edition, Prentice Hall, 2005, pp. 6-56.
12. Xiaojun, Y. and Qiaoyan, W., "A view about cloud data security from data life cycle", IEEE International Conference on Computational Intelligence and Software Engineering (CiSE), 2010, pp. 1-4.
13. L. Arockiam, S. Monikandan, G. Parthasarathy "Cloud Computing: A Survey" in International Conference on Computer Science and Engineering CSE-2011, October 2011, pp. 67-74.
14. L. Arockiam, G. Parthasarathy, S. Monikandan, "Privacy in Cloud Computing: A Survey" in International Conference on Advanced Computer Science & Information Technology (ACSIT-2012), ISBN:978-1-921987-04-5, July 2012, pp. 321-330.
15. ArijitUkil, Debasish Jana and Ajanta De Sarkar, "A security framework in cloud computing Infrastructure", International Journal of Network Security & Its Applications, Volume 5, Issue 5, September 2013, pp. 11-24.
16. IlangoSriram and Ali Khajehhosseini, "Research Agenda in Cloud Technologies", ACM Symposium on Cloud Computing, 2010, pp. 1-11.
17. Uma Somani, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).
18. Mr. Gurjeevan Singh,, Mr. Ashwani Singla and Mr. K S Sandha " Cryptography Algorithm Compaison For Security Enhancement In Wireless Intrusion Detection System" International Journal of Multidisciplinary Research Vol.1 Issue 4, August 2011.
19. Gurpreet Singh, Supriya Kinger"Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security "International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.