CLOUD COMPUTING A CRM SERVICE BASED ON SEPARATE ENCRYPTION AND DECRYPTION USING BLOWFISH ALGORITHM

Rajiv R Bhandari
M-Tech Student, Department of IT
NRI Institute of Information Science and Technology
Bhopal, (MP) India.
rajivbhandari@ymail.com

Prof.Nitin Mishra
Professor, Department of IT
NRI Institute of Information Science and Technology
Bhopal, (MP) India.
nitin.nriist@gmail.com

***Abstract*— Enterprises always store the data in the internal storage of the organization itself. Especially in a Customer Relationship management system all the data of the customers will be stored in the internal storage itself. In cloud computing, the data will be stored in storage provided by service providers. If a cloud system is answerable for both the tasks on storage and encryption-decryption of data, the system administrators may concurrently obtain encrypted data and decryption keys and there may be the chances of unauthorized disclosure of data. This allows them to access information without authorization and thus poses a risk to information privacy. A Customer Relationship Management service along with Blowfish Algorithm is described in this paper as an example of strong security system with higher performance to illustrate the proposed business Model.**

Keywords-CRM,ERP,CSP,KMS

*****

I. INTRODUCTION

Cloud Computing is an emerging technology in recent years. Before the development of the cloud computing generally the enterprises used to store the data in the internal storage of the organization itself. The data stored will be very confidential and even it has some security measures and it is protected from the unauthorized user. But in the cloud computing environment the storage of data is somewhere from the client workplace and the data storage and security measures will be in the service provider of the cloud computing environment. Generally the data is stored after it is encrypted. This is for the security of the client's or user's data. In Cloud computing the user data is stored followed by the encryption of the data. But if the storage and encryption of the data is in the same service provider then there is a possibility of accessing the keys and original data by the internal staffs or by administrators of the service provider.

A. Cloud Computing

The US National Institute of Standards and Technology (NIST) has published a definition of cloud computing that has been adopted and referred internationally as "*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.".* [3]

B. The Proposed Objective

This paper proposed a model to encrypt the data in one service provider and store the data in the different service provider. So once the data is stored in the application it is get encrypted and the encrypted data will not be present in the encryption service provider. Thus the storage of the data will be in the encrypted format and the administrators and the staffs have no knowledge about the encrypted keys and the service providers of the encryption and decryption.

C. Proposed Objective Discussion

In cloud computing, the data will be stored in storage provided by service providers. Service providers must have a viable way to protect their clients' data, especially to prevent the data from disclosure by unauthorized insiders. Storing the data in encrypted form is a common method of information privacy protection. If a cloud system is responsible for both tasks on storage and encryption/decryption of data, the system administrators may simultaneously obtain encrypted data and decryption keys. This allows them to access information without authorization and thus poses a risk to information privacy.

D. Applied Methodology

To implement the proposed solution of the problem that is being taken care of in this thesis work, the following methodology is used:

- To analyze the various existing Security Algorithm and find their strengths and weakness by the literature survey.
- To compare the existing techniques.
- A business model for cloud computing based on the concept of separating the encryption and decryption service from the storage service.

II. LITERATURE REVIEW

Cloud computing is one of the fastest growing segment of IT industry today .Companies are increasingly using cloud computing for their business. Cloud Computing has become a major part in today's IT sector.

They need to trust the cloud provider that their information will not be misused. With cloud computing users and companies are frequent victims of hacking and data loss. Hence It is necessary to analyze the security issues in cloud computing and make cloud computing secure and safe. [4]

Table: 1 Top concern regarding Security in Cloud Computing

Concern	Explanation
80% of enterprises consider security the #1 inhibitor to cloud adoptions	"How can we be assured that our data will not be leaked and that the vendors have the technology and the governance to control its employees from stealing data?"
48% Of enterprises are concerned about the reliability of clouds	"Security is the biggest concern. I don't worry much about the other "-cities" – reliability, availability, etc."
33% Of respondents are concerned with cloud interfering with their ability to comply with regulations	"I prefer internal cloud to IaaS. When the service is kept internally, I am more comfortable with the security that it offers."

A. Related Work

Data security system in cloud computing can be implemented using different Security algorithm. The below section represents the comparisons between different security algorithms.

In Figure 1 respondents marked out various information categories that can be risky if kept in the cloud, almost 70% people responded with risk of putting intellectual property over the cloud, followed by financial data at 62% and other categories of data were at an average of 40 – 55%, which included credit card information, noncommercial information and employee data. It is evident from the response of the surveyors that "Intellectual Property" followed by "Financial Data" are the two of the major categories of information that are at high risks in the cloud computing space.[1][11]

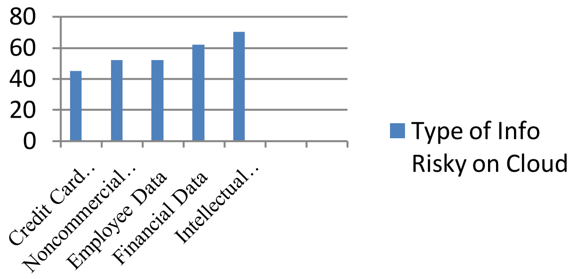


Figure 1 Type of Information Risky on Cloud

Hence this survey shows why cloud is not adaptable as per security is concern and how blow fish shows better result in different computing environment that's why this paper proposed and implemented better technique.

III. SURVEY ON SECURITY ISSUES IN CLOUD COMPUTING

A. Security Issues in Service Model:

Cloud computing having three delivery models through which services are delivered to end users. These models are SaaS, IaaS and PaaS which provide software, Infrastructure and platform assets to the users. They have different level of security requirements.

i) **Security issues in SaaS:** Software as service is a model, where the software applications are hosted slightly by the service provider and available to users on request, over the internet. In SaaS, client data is available on the internet and may be visible to other users, it is the responsibility of provider to set proper security checks for data protection. This is the major security risk, which create a problem in secure data migration and storage.

ii) **Security issues in PaaS:** PaaS is the layer above the IaaS. It deals with operating system, middleware, etc. It provides set of service through which a developer can complete a development process from testing to maintenance. It is complete platform where user can complete development task without any hesitation. In PaaS, the service provider give some command to customer over some application on platform. But still there can be the problem of security like intrusion etc, which must be assured that data may not be accessible between applications.

iii) **Security issues in IaaS :**IaaS introduce the traditional concept of development, spending a huge amount on data centers or managing hosting forum and hiring a staff for operation. Now the IaaS give an idea to use the infrastructure of any one provider, get services and pay only for resources they use. IaaS and other related services have enable set up and focus on business improvement without worrying about the organization infrastructure.

The IaaS provides basic security firewall, load balancing, etc. In IaaS there is better control over the security, and there is no security gap in virtualization manager. The main security problem in IaaS is the trustworthiness of data that is stored within the provider's hardware. [12],[13]

IV. INSIGHT OF SECURED ENCRYPTED CLOUD STORAGE

A. Key Management

Based on the Segregation of Duties security principle, key management should be separated from the cloud provider hosting the data. Described below are three different scenarios which depict the possible configurations. Organizations should elect the appropriate scenario for them, based on the classification of the data and their risk tolerance level

The scenario illustrated in Figure 2 (in which the customer maintains the KMS or Enterprise Key Management (EKM) solution on-premise and the encryption keys are stored on-premise) is the optimal scenario. It allows the customer to leverage the benefits of migrating sensitive data to a CSP for storage and processing while maintaining control and ownership over the keys and therefore the data. Hosting a Key Management Service (KMS) in a multi-tenant environment (Figure 2) can be a costly proposition for a cloud provider [16]

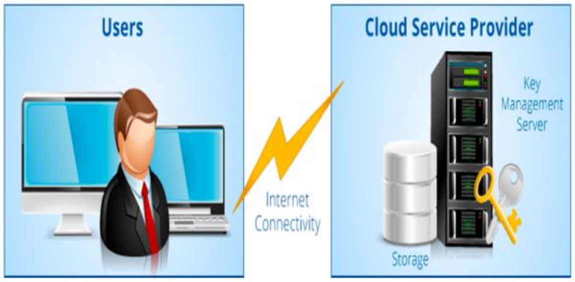


Figure 2: Key Located at Server Side

Remote Key Management Service where the customer maintains the KMS or Enterprise Key Management (EKM) solution on-premise, as illustrated in Figure 2. The ideal scenario is enterprises owning, maintaining and supporting their own KMS, leaving the ownership and control to the customer while the hosting and the processing are sourced out to the cloud provider.

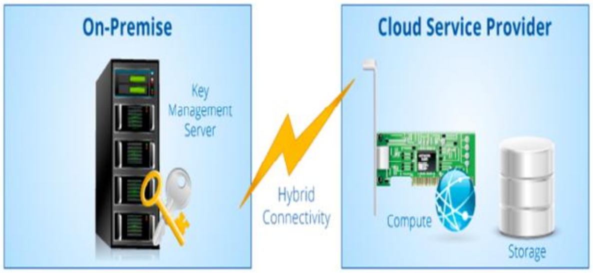


Figure 3: Key at User Side and Computation at Provider Side

A similar decentralized approach puts the customer in complete control of encryption/decryption keys. As shown in Figure 3, almost all processing and control is done on the customer side. The cloud provider does not hold keys, has minimal knowledge of users, cannot decrypt customer data, and facilitates the storage of encrypted data. The KMS is provided and run by the cloud provider, but the KMS resides on customer's premise and the keys are generated and held by the customer. This type of solution can be used by cloud storage and SaaS providers. [16]

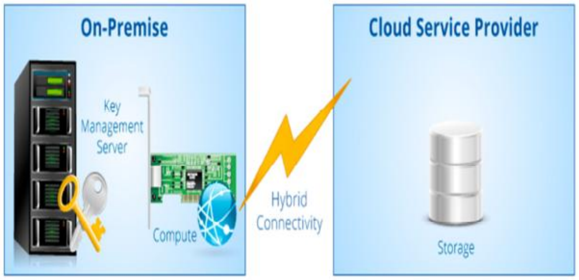


Figure 4: Key and Computation both are at User Side

B. BlowFish algorithm

Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish was designed in 1993 by Bruce Schneider as a fast, free alternative to existing encryption algorithms.

Description of the Algorithm

Blowfish uses a large number of subkeys. These keys must be precomputed before any data encryption or decryption. The P-array consists of 18 32-bit subkeys : P1, P2,..., P18. There are four 32-bit S-boxes with 256 entries each:

S1,0, S1,1,..., S1,255;
S2,0, S2,1,..,, S2,255;
S3,0, S3,1,..., S3,255;
S4,0, S4,1,..,, S4,255.

The exact method used to calculate these sub keys will be described later.

Encryption:

```
Blowfish is a Feistel network consisting of 16 rounds
 The input is a 64-bit data element, x.
Divide x into two 32-bit halves: xL, xR
For i = 1 to 16:
xL = xL XOR Pi
xR = F(xL) XOR xR
Swap xL and xR
Swap xL and xR (Undo the last swap.)
xR = xR XOR P17
xL = xL XOR P18
Recombine xL and xR
```

Function F ():

Divide xL into four eight-bit quarters: a, b, c, and d
F(xL) = ((S1,a + S2,b mod 232) XOR S3,c) + S4,d mod 232
Decryption is exactly the same as encryption, except that P1, P2,..., P18 are used in the reverse order.
Implementations of Blowfish that require the fastest speeds should unroll the loop and ensure that all sub keys are stored in cache.
The subkeys are calculated using the Blowfish algorithm.
The exact method is as follows:
Initialize first the P-array and then the four S-boxes, in order, with a fixed string. This string consists of the hexadecimal digits of pi (less the initial 3).
For example:
P1 = 0x243f6a88
P2 = 0x85a308d3
P3 = 0x13198a2e
P4 = 0x03707344
XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to P14). Repeatedly cycle through the key bits until the entire P-array has been XORed with key bits. (For every short key, there is at least one equivalent longer key; for example, if A is a 64-bit key, then AA, AAA, etc., are equivalent keys.)
Encrypt the all-zero string with the Blowfish algorithm, using the subkeys described in steps (1) and (2). Replace P1 and P2 with the output of step (3).
Encrypt the output of step (3) using the Blowfish algorithm with the modified subkeys.
Replace P3 and P4 with the output of step (5) Continue the process, replacing all entries of the P- array, and then all four S-boxes in order, with the output of the continuously-changing Blowfish algorithm. In total, 521 iterations are required to generate all required subkeys. [17]

V. IMPLEMENTATION OVERVIEW

A. *Business Model for Cloud Computing Based on an Encryption and Decryption service using Blowfish Algorithm:*

The concept is based on separating the storage and encryption/decryption of user data, as shown in Figure 5. In this business model, Encryption/Decryption as a Service and Storage as a Service (SaaS) are not provided by a single operator.

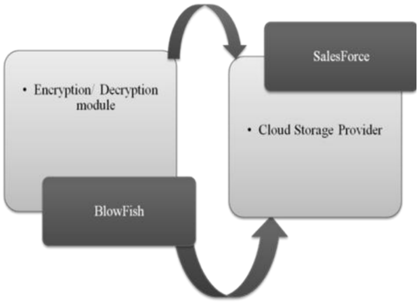


Figure 5: Encryption/Decryption as an independent service

Data retrieval from Cloud Service Provider:

When a user wants to access the CRM Cloud Service, must first execute the Login Program as shown in Step 1. This step can use current e-commerce or other services which have already securely verified the user's registration, such as symmetric key-based challenge and reply login verification, or through a One-Time Password. After the user's login has been successfully verified, if the CRM Service System requires client information from the user, it sends a request for information to the Storage Service System, as shown in Step 2. In this step, the CRM Service System transmits the user ID to the Storage Service System where it searches for the user's data. This data is encrypted so, once found, a request must be sent to the Encryption/Decryption Service System along with the user ID. Step 3 shows the Storage Service System executing the transmission of encrypted client data and the user ID to the Encryption/Decryption Service System. Since the Encryption /Decryption Service System can serve multiple users and the encryption/decryption for each user's data requires a different key, therefore each user's unique ID and keys are stored together. Therefore, in Step 4, the Encryption/Decryption Service System uses the received user ID to index the user's data decryption key, which is then used to decrypt the received data.

Using the correct decryption key to decrypt the data is critical to restoring the data to its original state. After the Encryption/Decryption Service System has decrypted the client's data, in Step 5 the decrypted client data is provided to the CRM Service System which then displays the client data to the user in Step 6, completing the Data Retrieval Program. Prior to sending the decrypted client data, the Encryption/Decryption Service System and the CRM Service System can establish a secure data transmission channel (e.g., a Secure Sockets Layer connection) to securely transmit the decrypted client data. [8]

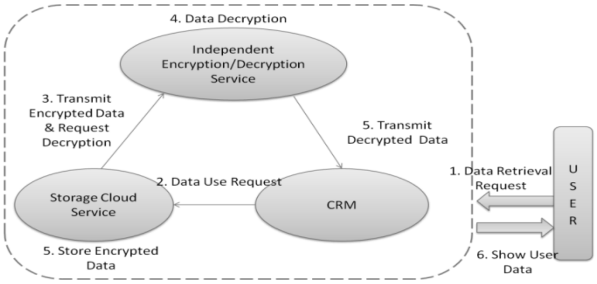

4. Data Decryption
Independent Encryption/Decryption Service
3. Transmit Encrypted Data & Request Decryption
5. Transmit Decrypted Data
2. Data Use Request
Storage Cloud Service
CRM
1. Data Retrieval Request
U S E R
5. Store Encrypted Data
6. Show User Data

Figure 6: Data Retrival from Cloud Service Provider

Next, we describe the Data Storage Program, as shown in Fig. 7. This program also involves the collaboration of three cloud service systems: CRM Service System, Encryption/Decryption Service System, and Storage Service System.

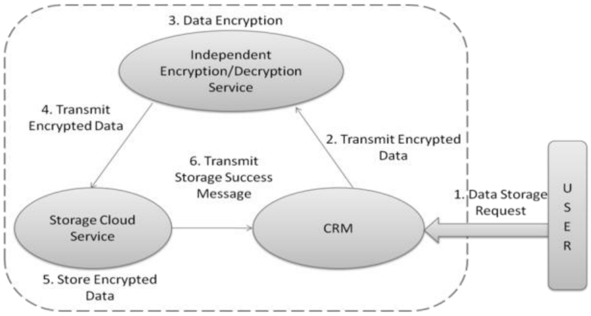

3. Data Encryption
Independent Encryption/Decryption Service
4. Transmit Encrypted Data
2. Transmit Encrypted Data
6. Transmit Storage Success Message
Storage Cloud Service
CRM
1. Data Storage Request
U S E R
5. Store Encrypted Data

Figure 7: Data storage diagram

Step 1 of Fig. 7 shows the client sending a Data Storage Request to the CRM Service System which then initiates the Data Storage Program, requesting data encryption from the cryption/Decryption Service System as shown in Step 2. In Step 2, the CRM Service System and the Encryption/Decryption Service System establish a secure data transfer channel to transmit the user ID and the data requiring storage from the CRM Service System to the Encryption/Decryption Service System.

As the encryption of data from different users requires different keys, in Step 3 the Encryption/Decryption Service System initiates data encryption, which involves using the received user ID to index the user's encryption key which is then used to encrypt the received data. Following this study's emphasis on the principle of divided authority, once the client data is encrypted by the Encryption/Decryption Service System it must be transferred to the Storage Service System where the user ID and encrypted data are stored together. Therefore, when the Encryption/Decryption Service System executes Step 4, it must transfer the user ID and encrypted client data to the Storage Service System.

Step 5 shows the Storage Service System receiving the user ID paired with the data for storage. In this business model, the following the completion of Step 4 at the Encryption /Decryption Service System, all unencrypted and decrypted user data must be deleted. Step 6, the final step of the Data Storage Program, transmits a Data Storage Complete message from the Storage Service System to the CRM Service System, at which point the CRM Service System may confirm that the client data has been stored. If it doesn't receive a Data Storage Complete message, it can re-initiate the Data Storage Program or, after a given period of time, proceed with exceptional situation handling.

VI. END RESULTS & UPSHOT

This section illustrates the End results & upshots which are obtained by running the system using different data loads. The results show how data is secure in Cloud Service Provider side Environment. Following figure illustrate graphical user interface for customer relationship management and inserting a record in CRM system.

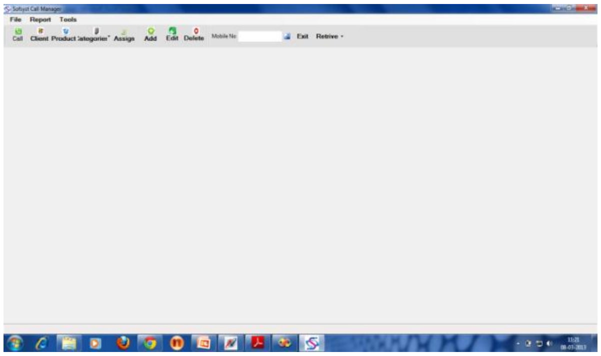
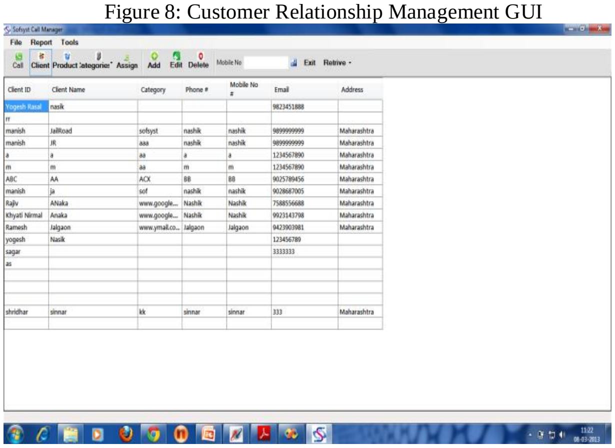

Sofsyst Call Manager
File Report Tools
Call Client Product Categories Assign Add Edit Delete Mobile No Exit Retrive

Figure 8: Customer Relationship Management GUI


Sofsyst Call Manager
File Report Tools
Call Client Product Categories Assign Add Edit Delete Mobile No Exit Retrive

Client ID	Client Name	Category	Phone #	Mobile No #	Email	Address
Yogesh Rasal	nasik				9823451888	
rr						
manish	JailRoad	sofsyst	nashik	nashik	9899999999	Maharashtra
manish	JR	aaa	nashik	nashik	9899999999	Maharashtra
a	a	aa	a	a	1234567890	Maharashtra
m	m	aa	m	m	1234567890	Maharashtra
ABC	AA	ACX	BB	BB	9025789456	Maharashtra
manish	ja	sof	nashik	nashik	9028687005	Maharashtra
Rajiv	ANaka	www.google...	Nashik	Nashik	7588556688	Maharashtra
Khyati Nirmal	Anaka	www.google...	Nashik	Nashik	9923143798	Maharashtra
Ramesh	Jalgaon	www.ymail.co...	Jalgaon	Jalgaon	9423903981	Maharashtra
yogesh	Nasik				123456789	
sagar					3333333	
as						
shridhar	sinnar	kk	sinnar	sinnar	333	Maharashtra

Figure 9: Customer Information

Once the customer information is inserted then encryption algorithm is applied and all data get stored in cloud service providers physical storage as illustrated in figure

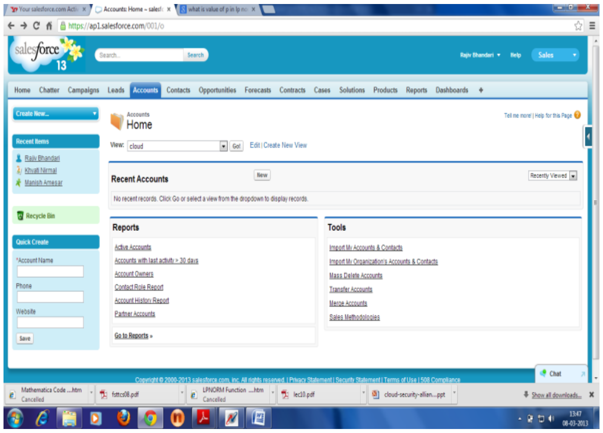


Figure 10: Saleforce Cloud Service Provider

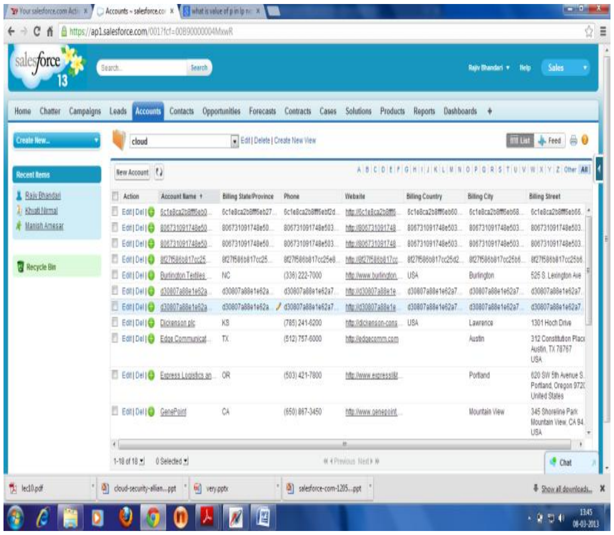


Figure 11: Customer Information Storage in Encrypted Format

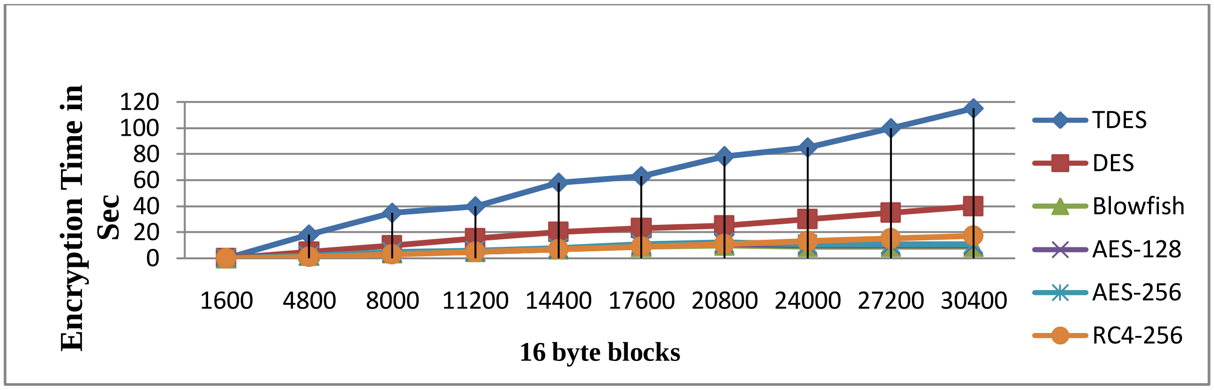


Figure 12: Comparison of encryption times for various common symmetric encryption algorithms for Cloud Computing

Table 2: Comparison of Blow-Fish with different Algorithm in Cloud Computing

Algorithm	Data	Time(In Seconds)	Average MB/Sec	Performance
DES	256 MB	10-11	22-23	Low
3DES	256 MB	12	12	Low
AES	256 MB	5	512	Medium
Blowfish	256 MB	3.5-4	64	High

VII. CONCLUSION

For cloud computing to spread, users must have a high level of trust in the methods by which service providers protect their data. This study proposes a Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service, emphasizing that authorization for the storage and encryption/decryption of user data must be vested with two different service providers. The privileges of Storage as Service provider include storing user data which has already been encrypted through an Encryption/Decryption Service System, but does not allow this service provider access to the Decryption Key or allow for the storage of decrypted data.

Furthermore, the privileges of the Encryption/Decryption as Service provider includes management of the key required for the encryption/decryption of user data, but not the storage of decrypted or encrypted user data. In this new business model, user data in the Storage Service System is all saved encrypted.
Without the decryption key, there is no way for the service provider to access the user data. Within the Encryption/Decryption Service System there is no stored user data, thus eliminating the possibility that user data might be improperly disclosed. After establishing "Independent Encryption/Decryption Services" in cloud computing environments, users of cloud computing services

(e.g., CRM, ERP, etc.) will use the services of at least two cloud computing service providers, so agreements between these service providers are required to establish a model for cooperation and division of responsibilities in providing a common service to clients. The core concept of this paper is consistent with division of management authority to reduce operational risk, thus avoiding the risk of wrongful disclosure of user data.

A. *Future Expectation*

The data storage security in Cloud Computing, an area full of challenges and of paramount importance, are still in its infancy now, and many research problems are yet to be identified is to enhance the more security features by using other enhanced techniques of data security through cryptosystems and other techniques. cloud computing does provide us with tangible benefits but today we still have no definite answers on a proper security platform for cloud computing, only suggestions and theories are being formed but we are yet to see a practical security measure for cloud computing to be a safer platform for organizations and individuals. The paper suggests the use of SSL to secure Cloud computing however this technology is still under the radar for practical usage and may serve as a security checkpoint for cloud computing security issues as of this moment, but cannot be used a sole tool to safeguard cloud computing, as the time progresses different technologies shall be discovered to safeguard cloud computing in the future.

ACKNOWLEDGMENT

At the outset, I would like to thank my guide, Prof. Nitin Mishra, Department of information Technology, NIIST, Bhopal, for giving me an opportunity to work on this challenging topic and providing me ample and valuable guidance through the course of this research.

I wish to thank Dr. Samidha Dwivedi Sharma, HOD, Department of Information Technology, NIIST, Bhopal for the innumerable hours spent with the early editing of the manuscript and the continuing moral support.

Above all, I would like to Special thanks to Ms.Khyati Nirmal and My Parents for their continuous support and encouragement that no amount of thanks can suffice.

REFERENCES

[1] Abhishek Goel , Shikha Goel ,“ Security Issues in Cloud Computing” International Journal of Application or Innovation in Engineering & Management Volume 1, Issue 4, pp 121-124, ISSN 2319 – 4847, December 2012

[2] Bupesh Mansukhani, Tanveer A. Zia, ”An empirical study of challenges in managing the security in cloud computing” in Proceedings of the 9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th - 7th December, pp 172-181, 2011

[3] Torry Harris, ”Cloud Computing – An Overview” , Retrieved from http://www.thbs.com/downloads/cloud-computing-overview.pdf

[4] “Cloud security An enterprise perspective” Hewlett-Packard Development Company, L.P. The information, 2012. Available from https://h30613.www3.**hp**.com/media/files/.../BB237 _Nielson.pdf

[5] “Cloud Security Survey Global Executive Summary Corporate Marketing Trend Micro“, August 2012. Available from http://www.trendmicro.com/cloud-content/us/pdfs/about/2012 _global_cloud_security_survey_executive_summary.pdf

[6] Elminaam, D S Abd; Kader H M Abdual and Hadhoud, M Mohamed, “Evaluating the Performance of Sysmmetric Encryption Algorithms”, International Journal of Network Security, Vol. 10, No. 3, pp. 216-222, May 2010.

[7] Jawahar Thakur, Nagesh Kumar, AES, DES, .Blowfish: Symmetric key algorithm Simulation based performance analysis”, ,International Journal of Emerging Technology and Advanced Engineering ,Volume 1, Issue 2, pp 6-12, ISSN 2250-2459, December 2011.

[8] 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”, IEEE Conference on Information Science and Applications (ICISA), April 2011.

[9] I.Golda Selia, S.K. Madhumithaa , “CRM System in Cloud Computing with Different Service Providers “International Journal of Computational Engineering Research National Conference on Architecture, Software system and Green computing, pp 46-49, ISSN:2250-3005

[10] Aamer Nadeem, Dr M. Younus Javed, " A Performance Comparison of Data Encryption Algorithms ", IEEE Conference on Information and Communication Technologies ICICT, pp 84-89, 2005

[11] Neha Jain and Gurpreet Kaur, “Implementing DES Algorithm in Cloud for Data Security” VSRD-International Journal of Computer Science and Information Technology, Vol. 2 (4), pp 316-321, ISSN No: 2231-2471, 2012.

[12] Priyanka Arora, Arun Singh, Himanshu Tyagi , “Evaluation and Comparison of Security Issues on Cloud Computing Environment” World of Computer Science and Information Technology Journal (WCSIT), Vol. 2, No. 5, pp 179-183, ISSN: 2221-0741, 2012

[13] Rejoice Paul, Mansi Talreja, Aman Sahu and K. John Singh, ”Security issues in Cloud Computing” International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 11, pp 1863-1867, ISSN : 0975-3397, November 2012

[14] “Security in Cloud Computing A Microsoft Perspective” Retrieved 2010 from http://www.microsoft.com/en-us /download/ details.aspx?id=5288

[15] Uma Somani, Kanika Lakhani,Manish Mundra, ”Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing” International Conference on Parallel, Distributed and Grid Computing PDGC IEEE– 2010

[16] “secaas- category- 8- encryption- implementation”, Retrieved 2012, from https://cloudsecurityalliance.org/download/secaas-category-8-encryption implementation- guidance

[17] Atul Kahate “Cryptography and Network Security”, Tata Mc-graw Hill, 3rd Edition 2008