A CRM Based Cryptography Service for Ensuring Security in Cloud Computing

K.V.S.Prasad M.Babu Rao

Abstract- Cloud Computing is more than a technology. It is more than a platform. It is more than just a hosting provider. It is more than just an application hosted as a service. It is more than providing storage services on the Internet. It is a combination of all the above. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth. A simple example of cloud computing is Yahoo email, Gmail, or Hotmail etc. You don't need software or a server to use them. All a consumer would need is just an internet connection and you can start sending emails, The server and email management software is all on the cloud (internet) and is totally managed by the cloud service provider Yahoo , Google etc. But in data privacy protection and data retrieval control is one of the most challenging research work in cloud computing, because of users can store their confidential data in storage cloud which is provided by the service provider. Service provider must provides the authentication for valid user otherwise the security must reduce and the cloud computing system may collapse. It's service provider's responsibility that saves the end users data with security. For these issues regarding security and privacy this paper implies some efficient ways to overcome the limitations and drawbacks of cloud computing. This Paper mainly focus on the core concept of secured cloud storage i.e. it suggests separating the encryption and decryption process from storage process for achieving more security measures. This paper introduces a user interface model i.e. Customer Relationship Management (CRM). The CRM is actually a connecting application which connects user to any system. So we purposefully uses CRM for user interface. A CRM service is described in this paper as an example to proposed business model and usability for end user. This service consists of three cloud systems, which are an encryption, and decryption system, a storage system, and a CRM application system. One service provider operates the encryption and decryption system while other providers operate the storage Even for security and data integrity we supposed to implement the One Time Password Authentication (OTP) including email updates and application systems, according to the core concept of the proposed computing model.

General Terms: Private Key, Public Key, SaaS, PaaS, IaaS, Authentication ID, cipher text.
Keywords: Cloud computing; Encryption and Decryption cloud services; Data privacy protection; One Time Password (OTP), Service Level Agreements (SLA).

1 INTRODUCTION

The constant growth of Internet usage has created new challenges. Largest online companies, such as Amazon and Google, were forced to change their attitude towards data storage and resource allocation. That caused computing revolution, which is just beginning. The revolution, called "Cloud computing". Cloud computing represents the new understanding of computing power as a service, not as a product. In other words, you should pay for what you use instead of for what you own. However, it is a lot more than lower costs. The money could not be saved without balancing resources – and that is what cloud computing does. Most people do not use their computers 24 hours a day, 7 days a week, as well as the vast majority of servers are not fully employed all the time. Consequently, a good portion of computing resources goes unused. Cloud computing uses those resources.

Nevertheless, it is important to note, that most of the technologies used in cloud computing have been around for ages (Reese, 2009). Therefore, the changes are more related with the different usage of existing computing devices than with the creation of new physical machines.
This essay will state the promises of cloud computing to both users and developers. However, the main aim is to analyse the problems which this technology faces in the way of global acceptance. That should answer the question, why cloud computing is only the future, but not the present of the Internet.

2. RELATED WORK

In late 90s or even now, ask any web developer, solution architect or anyone involved in web application development in any capacity:
Which symbol do you use to represent Internet on numerous white-board meetings? Obviously the most widely used metaphor for Internet was/is cloud. Cloud computing has derived its name from the same line of thinking.
Cloud Computing is a style of computing which must cater to the following computing needs:

- Dynamism
- Abstraction

- *K V S Prasad is currently pursuing masters degree program in computer science engineering in Guglavalleru Engineering College, India. E-mail: kvs998@gmail.com*
- *Prof.M Babu Rao is currently working as professor in computer science engineering in Gudlavalleru Engineering College, India. E-mail: baburaompd@yahoo.co.in*

- Resource Sharing

A. Dynamism

Your business is growing exponentially. Your computing need & usage is getting bigger with every passing day. Would you add servers & other hardware's to meet the new demand? Assume, Recession is back & your business is losing customers. The servers & hardware's you added during last quarter's peak season is now idle. Will you sale them? Demand keeps on changing based on world/regional economy, sometimes seasonal traffic burst as well. That's where Cloud Computing comes to your rescue! You just need to configure & your provider will take care of fluctuating demand

B .Abstraction

Your business should focus on your core competency & should not worry about security, OS, software platform, updates and patches etc. Leave these chores to your provider. From an end users perspective, you don't need to care for the OS, the plug-ins, web security or the software platform. Everything should be in place without any worry.

C. Resource Sharing

Resource Sharing is the beauty of Cloud Computing. This is the concept which helps the cloud providers to attain optimum utilization of resources. Say, a company dealing in gifts may require more server resources during festive season. A company dealing in Payroll management may require more resources during the end or beginning of the month. The cloud architecture is implemented in such a way that it provides you the flexibility to share application as well as other network resources (hardware etc). This will lead to a need based flexible architecture where the resources will expand or contract with little configuration changes.

Using Applications in the Cloud

If people can access a service using any computer, without preference of operating system, browser and other software, that service is cloud-based. In general, the only thing you need – is a browser. Cloud computing does not require a single piece of software to be installed in the user's computer.The most common example of cloud computing could be Google Mail. For a long time such programs as Microsoft Outlook were used for working with email. Currently, the freedom of accessing data from any computer, as well as the improved functionality of online applications, has encouraged people to move into the cloud.

Firstly, as application runs in the cloud, not on the desktop PC, the PC does not need the processing power or hard disk space demanded by traditional desktop software (Miller, 2008). Therefore, users can choose lower-cost computers. For this purpose, the whole class of small, light and inexpensive laptop computers, called net books, was created. According to market forecaster Display Search (displaysearch.com), in the second quarter of 2009, net books accounted for 32.9 percent of all portable computer shipments in Europe, and it is expected to grow constantly in the future. This data proves that more and more people become independent of personal computer resources.

Secondly, it means increased computing power and unlimited storage. Distributed computing shares resources between many servers in the cloud. Therefore, a user has the power of the entire cloud at his disposal and can store whatever he needs.

Thirdly, one of the most interesting benefits of cloud is online collaboration. A user does not have to carry a copy of every file with him when he moves from one location to another. Instead, all documents are hosted in the cloud and are available to any authorized user. That makes an opportunity for multiple users to access and edit the same document in real time.

Finally, it encompasses data safety. Files in the cloud are automatically duplicated. In addition, they are not affected by crashes of the user's computer or application. Nevertheless, it is still important to store backups in more accessible place than the cloud (Miller, 2008).

Cloud computing for business and developers

Currently, the vast majority of companies build their own IT infrastructure or choose managed services provider. These options have significant costs and limited flexibility, unlike data storage in the cloud.

Using cloud computing, files can be just "thrown" into the cloud without worrying how they are stored or backing them up. In addition, you do not need to take care about software licenses and upgrades, which are done for you automatically. Furthermore, there is nothing to do with hardware, as you do not own it. In other words, you do not need to take care about any hardware failures or purchases. In the world, where machine's value is reduced every month it is in use until it is worth nothing, that means a lot.

There are three main types of cloud services.

1. IaaS – Infrastructure as a service.
2. PaaS -platform as services.
3. SaaS- software as service

2.1. Infrastructure as a Service: (IaaS)

This is the base layer of the cloud stack. It serves as a foundation for the other two layers, for their execution. The keyword behind this stack is Virtualization.

Let us try to understand this using Amazon EC2. In Amazon EC2 (Elastic Compute Cloud) your application will be executed on a virtual computer (instance). You have the choice of virtual computer, where you can select a configuration of CPU, memory & storage that is optimal for your application. The whole cloud infrastructure viz.

servers, routers, hardware based load-balancing, firewalls, storage & other network equipments are provided by the IaaS provider. The customers buy these resources as a service on a need basis.

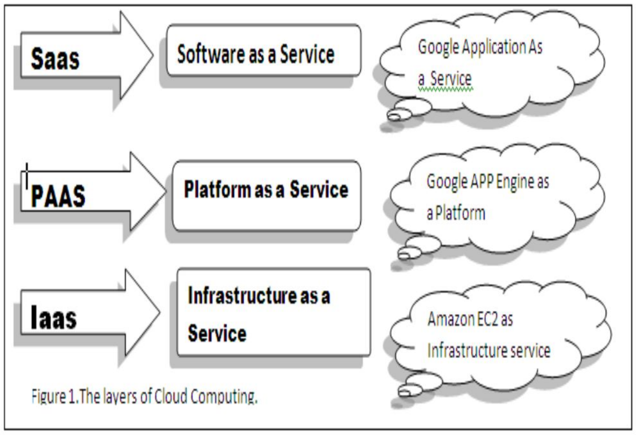

Saas
Software as a Service
Google Application As a Service
PAAS
Platform as a Service
Google APP Engine as a Platform
Iaas
Infrastructure as a Service
Amazon EC2 as Infrastructure service
Figure 1.The layers of Cloud Computing.

Figure 1:Layers of Cloud Computing

2.2. Platform as a Service (PaaS)

Now you don't need to invest millions of $$$ to get that development foundation ready for your developers. The PaaS provider will deliver the platform on the web, and in most of the cases you can consume the platform using your browser, i.e. no need to download any software. It has definitely empowered small & mid-size companies or even an individual developer to launch their own SaaS leveraging the power of these platform providers, without any initial investment.

- PaaS Layers
- Cloud OS
- Cloud Middleware

2.3. Software as a Service (SaaS)

This is the Top most layer of the cloud computing stack - directly consumed by end user – i.e. SaaS (Software as a Service). On-Premise applications are quite expensive, affordable only to big enterprises. Why? Cause On-Premise applications had a very high upfront CapEx(Capital Expenditure); which results in a high TCO (Total Cost of Ownership). On-Premise apps also require a higher number of skilled developers to maintain the application. In its current avatar SaaS is going to be the best bet for SMEs/SMBs (Small & Mid size businesses). Now, they can afford best software solution for their business without investing anything at all on the infrastructure or development platform or skilled manpower. The only requirement for SaaS is a computer with browser, quite basic. SaaS is a recurring subscription based model delivered to customer on demand – Pay as you use.

Best SaaS Examples

- Sales Force CRM
- Google Apps
- ZOHO Support
- Desk away
- Impel CRM
- Wipro w-SaaS

3. LITERATURE REVIEW

3.1. Origin and Core Concept of Cloud Computing

In a cloud computing environment, the service content offered by service providers can be adjusted according to the needs of the user. For example, the applicant can request different amounts of storage, transmission speeds, levels of data encryption and other services. In addition to defining the service items, the agreement normally also notes the time, quality and performance requirements provided with the service. Generally, these service agreements are referred to as Service Level Agreements (SLA) [4]. By signing an SLA, the user shows that he has understood and agreed to the contents of the application service, and agrees with the provider's data privacy and protection policies.

A common approach to protect user data is that user data is encrypted before it is stored. In a cloud computing environment, a user's data can also be stored following additional encryption, but if the storage and encryption of a given user's data is performed by the same service provider, the service provider's internal staff (e.g., system administrators and authorized staff) can use their decryption keys and internal access privileges to access user data. From the user's perspective, this could put his stored data at risk of unauthorized disclosure.

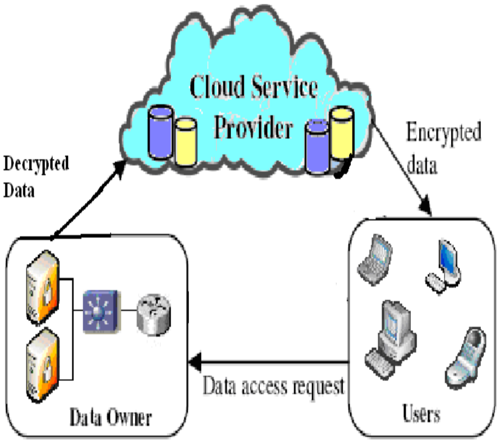


Figure.2.Basic of Cloud Computing

Creating user trust through the protection of user's data content is the key to the widespread acceptance of the cloud computing. This study proposes a business model for cloud computing based on the concept of using a separate encryption and decryption service. In the model, data storage and decryption of user data are provided separately by two distinct providers. In addition, those working with the data storage system will have no access to decrypted user data, and those working with user data encryption and decryption will delete all encrypted and decrypted user data after transferring the encrypted data to the system of the data storage service provider.

4. PREVIOUS METHODALOGY FOR PROTECTING DATA IN CLOUD COMPUTING

The cloud computing methods are actually based on the concept of cryptography. Encryption and decryption these are the some processes involved in the cloud computing which help to leads for data integrity and data security.

Encryption Method: -

Symmetric and asymmetric cryptography is the part of common data encryption methods. Example of a encryption method, it is used in the us. federal conformation processing standard's (FIPS).46-3, 197 Advanced Encryption Standard (AES) and others or Triple Data Encryption Algorithm (TDEA, also known as Triple-DES or 3DES). This type of encryption and decryption process uses as a secret key. Asymmetric cryptography having two different keys-

- "public key" for encryption
- "Private Key" for decryption:

Examples include RSA cryptography and Elliptic Curve Cryptography (ECC). According to the user, "symmetric cryptography is more efficient, and is suitable for encrypting large amount of data. Asymmetric cryptography requires more computation time and is used for the decryption keys required for symmetric cryptography."The use of passwords as an authentication process is more familiar to users, but data sent by the user can be easily hacked.

5. A CRM BASED CRYPTOGRAPHY SERVICE FOR ENSURING THE SECURITY IN CLOUD COMPUTING

Here we are going to clear more ideas about the actual motives of cloud computing. As we already know about the cloud computing till yet. But now we will focus more on how the exact working of cloud computing undergoes for doing the encryption and decryption service for data security and data integrity. This concept is fully and conveniently described in figure 3. As shown in the figure we are going to separate both the service storage and the encryption decryption services so through that we will be getting more security to protect our confidential data from getting hacked by someone. Here for implementing we are using a concept of Software as a Service (SaaS).

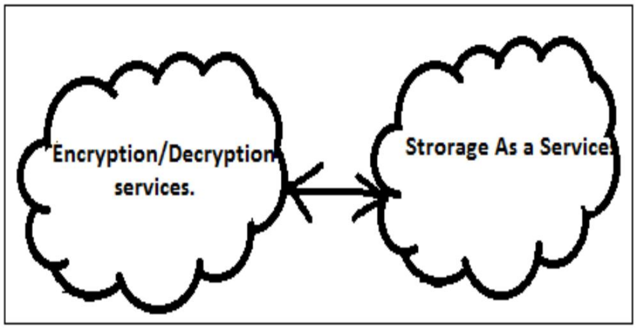


Figure.3:Security Services for cloud Computing

When the required data will get encrypted or decrypted depending upon the user request, then the Encryption or Decryption Service will first of all assign the respective result to the CRM application. But now the data which is sent to Encryption or Decryption Services for doing encryption or decryption is stored in that service only. This will create a risk factor for getting leakage of data. This provider will automatically delete the encrypted and decrypted data from the Encryption and Decryption Service System. As here data will get stored in one place and gets encrypted in another place so due to this dividing authority data integrity is prevented. In that two functions say accountant and cashier are related to each other regarding providing funds. But these would not interact with each other. These two functions should be kept separately for providing safety. As cashier won't be able to do any frond in the billing provided by the accountant. In this manner we can efficiently and properly maintained our confidential data from getting leaked by someone. Here are some examples of effective cloud computing, Salesforce.com's CRM service [11], SAP□s ERP services [12], etc. Data generated while

5.1.Data Retrival From Cloud Service Using Security Service

Now we will focus on how user will do interaction with the CRM to encrypt and decrypt the data. For that purpose, users have to undergo the login procedure in order to do the encryption and decryption procedure as shown in figure 4. The Data Retrieval Program is illustrated in Fig.4 and is elaborated below. By observing figure we will firstly understand the concept of data retrieving concept. As shown in the figure user will do login where the user's registration is securely verified through login verification or say a One-time Password.

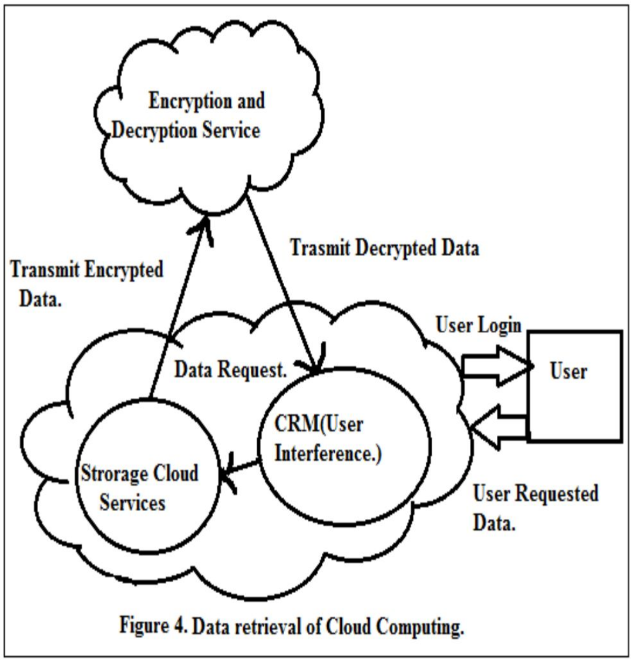


Figure.4 Data retrival of Cloud Computring

After this authentication process is completed and user had been successfully completed the login procedure, he or she will send the request for the data retrieval to the CRM. Then the CRM will send the user ID to the Storage system. By sending that Id, it becomes convenient for the storage system to found the data which exactly user wants to retrieve. But here the data is stored in the encrypted form. So it is not readable by the user or say client. Hence, this encrypted data is then transmitted to the Encryption and Decryption by the Storage System with the user ID. In our cloud computing services there are n number of users or say multiuser who are performing the encryption and decryption which creates complexity for the CRM, storage systems which data specifically user requires. As the data is stored on the large manner in the form of tokens. So for identifying that we require a unique user ID which helps us out to fulfill the user requirement to secure their confidential data.

Now, further, the data when transmitted to the encryption and decryption service it should be sent with the unique user ID for indexing the decryption data. By matching that send user ID with the stored decrypted data, the decryption of that particular file or data is done with the help of decrypted key. And finally that decrypted data is send back to the CRM Service. Further this decrypted data is send to the user or client, completing the data retrieval program. For doing this we are using the public and the private key to provide security. But when the encrypted data is transmitted to the CRM then there are a chance of getting data hacked by some unauthorized person. For avoiding this we may used a Secure Sockets Layer Connection to securely transmit it. Once the decrypted data has been send to user then the unencrypted data had been deleted from there so as to prevent the creation of the same data at some another place. It means that the data and the encrypted key should not be copied by someone during that process. This would become a critical and major factor for ensuring data integrity and privacy. In this manner, we are ensuring a better and enhanced way for data retrieval of the system.

5.2. Data Storage system

Now we will understand the concept of how the data should get stored in the storage system. The Data Storage System diagram is as shown in figure 5. Here also we require the three cloud service systems which seem to mainly focus on storage system. It has following some implementing steps.

Step 1. As per the figure 5 sending the request to store the data which is then acquire by CRM system.

Step 2. Then the CRM system and Encryption / Decryption Services established the security path to transmit user ID and data which is have to be store.

Step 3. The Encryption / Decryption Service then involves in conversion of both user ID and Data with use of encryption key which mainly used to encrypt the received data. Finally data can be store successfully. Data Storage System is a actually exactly reversed process of Data Retrieval System.

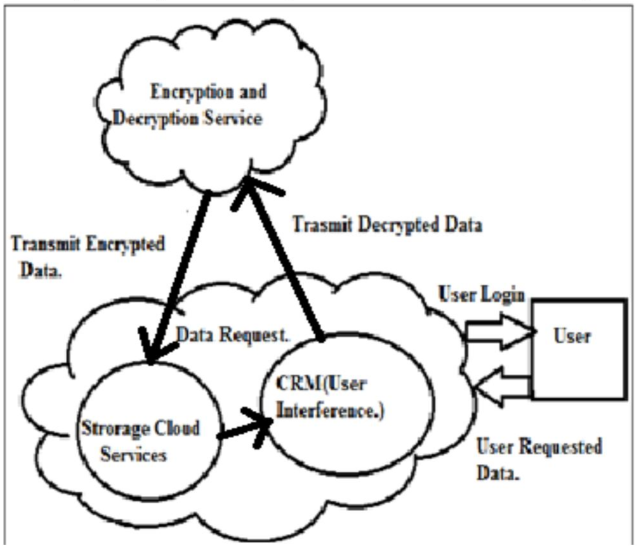


Figure.5.Data Storage System

5.3 BLOWFISH ALGORITHM:

Blowfish is a variable-length key block cipher. It does not meet all the requirements for a new cryptographic standard discussed above: it is only suitable for applications where the key does not change often, like a communications link or an automatic file encryptor. It is significantly faster than DES when implemented on 32-bit microprocessors with large data caches, such as the Pentium and the PowerPC.

Descryption of Algorithm:

Blowfish is a variable-length key, 64-bit block cipher. The algorithm consists of two parts: a key-expansion part and a data-encryption part. Key expansion converts a key of at most 448 bits into several subkey arrays totaling 4168 bytes. Data encryption occurs via a 16-round Feistel network. Each round consists of a key-dependent permutation, and a keyand data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round.

Sub keys:

Blowfish uses a large number of subkeys. These keys must be precomputed before any data encryption or decryption.

1. The P-array consists of 18 32-bit subkeys:P1, P2,..., P18.

2. 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

1). 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.

Generating the Sub keys:

The sub keys are calculated using the Blowfish algorithm. The exact method is as follows:

1. 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

2. 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.)

3. Encrypt the all-zero string with the Blowfish algorithm, using the sub keys described in steps (1) and (2).

4. Replace P1 and P2 with the output of step (3).

5. Encrypt the output of step (3) using the Blowfish algorithm with the modified sub keys.

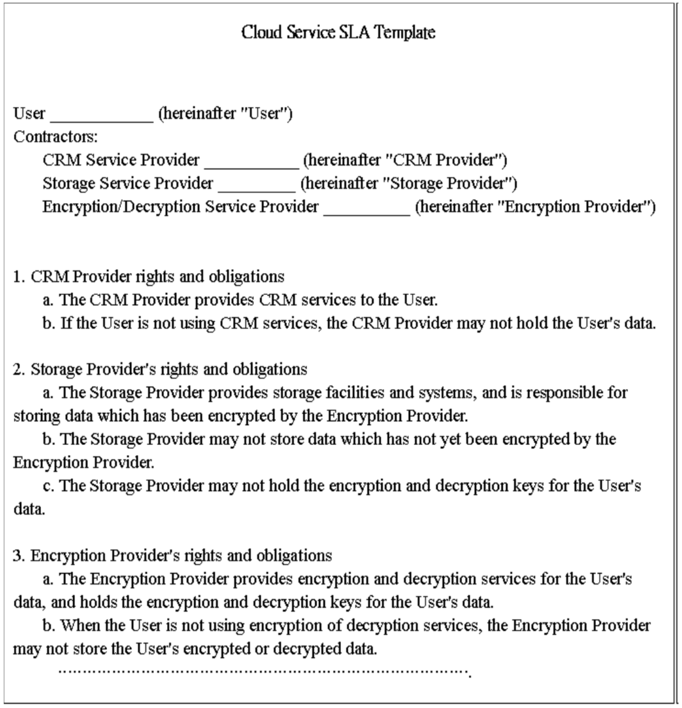
6. Replace P3 and P4 with the output of step (5).

7. 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. Sub- keys. Applications can store the sub keys rather than execute this derivation process multiple times.

5.2.Recommended Service Level Agreement Content

This CRM based Cloud computing model consists the multiple Service providers for providing the efficient CRM Cloud Service. The data handling and the coopearation among the opearators will provide the effectiveness with which users use the service. Unlike conventional Service Level Agreements (SLA), any SLA between the user and the service provider must consider the rights and obligations of the collaborating operators, and operators should sign contracts between themselves to establish the division of responsibilities and cooperation model for providing common services to clients.

The Proposed CRM based Cloud Service includes a template for multy-party opearators SLA for the user CRM Service provider, encryption / decryption Service provider, Storage Service provider, This SLA is based on policies for ensuring data privacy, as shown in Fig.6



Cloud Service SLA Template

User ___________ (hereinafter "User")
Contractors:
CRM Service Provider __________ (hereinafter "CRM Provider")
Storage Service Provider ________ (hereinafter "Storage Provider")
Encryption/Decryption Service Provider _________ (hereinafter "Encryption Provider")

1. CRM Provider rights and obligations
a. The CRM Provider provides CRM services to the User.
b. If the User is not using CRM services, the CRM Provider may not hold the User's data.

2. Storage Provider's rights and obligations
a. The Storage Provider provides storage facilities and systems, and is responsible for storing data which has been encrypted by the Encryption Provider.
b. The Storage Provider may not store data which has not yet been encrypted by the Encryption Provider.
c. The Storage Provider may not hold the encryption and decryption keys for the User's data.

3. Encryption Provider's rights and obligations
a. The Encryption Provider provides encryption and decryption services for the User's data, and holds the encryption and decryption keys for the User's data.
b. When the User is not using encryption of decryption services, the Encryption Provider may not store the User's encrypted or decrypted data.
…………………………………………………………………………….

Figure.6.Cloud Service SLA template
(based on policies to ensure data privacy)

6. CONCLUSION AND FUTURE WORK

This system effectively identifies security laws in the CRM applications using Blowfish algorithm clearly .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. This study provides a draft of a multi-signatory Service Level Agreement (SLA) in which the signatories can include cloud computing rental users, application service providers, encryption/decryption service providers, storage service providers, etc., with content including the rights and obligations between operators and also includes data security policies between each operator and clients.

In future this system is extended to implement in commercial applications like Amazon aws in order to give more security cloud services to the end users.

7. REFERENCES

[1]A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service. http://www.techrepublic.com/whitepapers/a-business modelfor-cloud-computing-based-on-a-separate-encryption-anddecryption-service/3500091

[2] David S. Linthicum, Cloud Computing and SOA Convergence in your Enterprise, Pearson, 2010.

[3] R.Buyya, C. S. Yeo, and S. Venugopa, "Marketoriented Cloud Computing: Vision, hype, and reality for delivering it services as computing utilities", in Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications (HPCC-08, IEEE CS Press, Los Alamitos ,CA, USA) 2008.

[4] Mehrdad Mahdavi Boroujerdi, Soheil Nazem, Cloud Computing: Changing Cogitation about Computing, World Academy of Science, Engineering and Technology 58 2009.

[5] Amazon web service, [Online]. Available: http://aws.amazon.com/

[6] Top Threats to Cloud Computing V1.0, Cloud Security Alliance, March 2010.

[7] L. M. Vaquero,L. Rodero-Merino,J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50-55, January 2009.

[8] C. Weinhardt, A. Anandasivam, B. Blau, N. Borissov, T. Meinl, W. Michalk, and J. Stößer, "Cloud computing – a classification, business models, and research directions," Business & Information Systems Engineering (BISE), vol. 1, no. 5, pp. 391-399, 2009.

[9] N. Hawthorn, "Finding security in the cloud," Computer Fraud & Security, vol. 2009, issue 10, pp. 19-20, October 2009.

[10] A. Parakh and S. Kak, "Online data storage using implicit security', Information Sciences, vol. 179, issue 19, pp. 3323-3333 ,September 2009.