ABSTRACT

Cloud computing is a distributive computation task on the resource pool which consists of massive computers. LMS experiences with Cloud and Managed Cloud Service provider are due to numerous factors. Availability means that the services are available even when quite a number of nodes fail. Cloud services are provided by many IT companies like Google, Amazon, Microsoft, and Salesforce.com. An enterprise usually store data in local storage and then tries to protect the information from other external source. They also provide authentication at certain fixed level. To overcome this limitation, we are presenting some approaches that do not require full dependency on the external security provider.

Storing the data in encrypted form is a common method of data privacy security. If a cloud system is responsible for both tasks on storage and encryption/decryption of data, the system administrators may simultaneously hold encrypted data and decryption keys. This allows them to access information without authorization and thus poses a threat to information privacy[1].

A LMS (Learning Management System) service is described in this project using Blowfish algorithm. It promotes more accessibility to LMS service providers to send their training modules and syllabus via Internet at any point of the hour much more efficiently. This gives rise to reduced cost of hardware and software tools, which in return would scale-up the e-learning environment. In the existing system RSA algorithm used. It requires more computation time for large volumes of data. To reduce this computation time we are using Blowfish algorithm. The LMS Service utilizes three cloud systems, including an encryption and decryption system, a storage system, and LMS application system.

I. INTRODUCTION

Cloud computing” is a term, which involves virtualization, distributed computing, Networking, software and web services. A cloud consists of several elements such as clients, datacenter and distributed servers. It includes fault tolerance, high availability, scalability, flexibility, reduced overhead for users, reduced cost of ownership, on demand services etc. Central to these issues lies the establishment of an effective load balancing algorithm. The load can be CPU load, memory capacity, delay or network load. Load balancing is the process of distributing the load among various nodes of a distributed system to improve both resource utilization and job response time while also avoiding a situation where some of the nodes are heavily loaded while other nodes are idle or doing very little work. Load balancing ensures that all the processor in the system or every node in the network does approximately the equal amount of work at any instant of time. This technique can be sender initiated, receiver initiated or symmetric type (combination of sender initiated and receiver initiated types).

Cloud computing is a distributive computation task on the resource pool which consists of Massive computers. The storage space and software service according to its demand. Cloud computing can be categorized in to two High scalability and high availability. Availability means that the services are available even when quite a number of nodes fail. Cloud services are provided by many IT companies like Google, Amazon, Microsoft, and Salesforce.com. In this project as per their services we categorized services in to Software as a Service (SaaS), Platform as a Service (PaaS), Network as a Service (NaaS) and Infrastructure as a Service (IaaS). Detailed analysis to these services are provided and adopting the cloud services to a basic system which can be used by organization.

Types of services provided by cloud computing:-

Infrastructure as a Service (IaaS):- means you’re buying access to raw computing hardware over the Net, such as servers or storage. Since you buy what you need and pay-as-you go, this is often referred to as utility computing. Ordinary web hosting is a simple example of IaaS, you pay a monthly subscription or a per-megabyte/gigabyte fee to have a hosting company serves up files for your website from their servers.

Software as a Service (SaaS):- means you use a complete application running on someone else's system. Web-based email and Google Documents are perhaps the best-known examples. Zoho is another well-known SaaS provider offering a variety of office applications online.

Platform as a Service (PaaS):- means you develop applications using Web-based tools so they run on systems software and hardware provided by another company. So, for example, you might develop your own ecommerce website but have the whole thing, including the shopping cart, checkout, and payment mechanism running on merchant’s
2. RELATED WORK

Open-source software has been on the rise at many businesses during the extended economic downturn, and one of the areas where it is starting to offer companies a lot of flexibility and cost savings is in cloud computing. Cloud deployments can save money, free businesses from vendor lock-ins that could really sting over time, and offer flexible ways to combine public and private applications. The following are 11 top open-source cloud applications, services, educational resources, support options, general items of interest, and more.

**Eucalyptus:**
Ostatic broke the news about UC Santa Barbara’s open-source cloud project last year. Released as an open-source (under a FreeBSD-style license) infrastructure for cloud computing on clusters that duplicates the functionality of Amazon’s EC2, Eucalyptus directly uses the Amazon command-line tools. Startup Eucalyptus Systems was launched this year with venture funding, and the staff includes original architects from the Eucalyptus project. The company recently released its first major update to the software framework, which is also powering the cloud computing features in the new version of Ubuntu Linux.

**AWS Compatibility**

Eucalyptus is fully compatible with the AWS API, which means you can use or reuse any of your existing AWS-compatible tools, images (AMIs), and scripts to manage your own on-premise Infrastructure as a Service (IaaS) environments. We implement the AWS API on top of Eucalyptus, so any tool in the cloud ecosystem that communicates with AWS can communicate with Eucalyptus IaaS.

Eucalyptus will provide compatibility to the most popular Amazon Web Services including:

- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic Block Storage (EBS)
- Amazon Machine Image (AMI)
- Amazon Simple Storage Service (S3)
- Amazon Identity and Access Management (IAM)

Common data encryption methods include symmetric and asymmetric cryptography algorithms. Symmetric cryptography is used in the U.S. Federal Information Processing Standard’s (FIPS) 46-3 Triple Data Encryption Algorithm (TDEA, also known as Triple-DES or 3DES) or 197 Advanced Encryption Standard (AES) and others. This type of encryption and decryption process uses a secret key. Asymmetric cryptography, on the other hand, uses two different keys, a “public key” for encryption, and a “private key” for decryption. Examples include RSA cryptography and Elliptic Curve Cryptography [12]. Generally speaking, symmetric cryptography is more efficient, and is suitable for encrypting large volumes of data. Asymmetric cryptography requires more computation time and is used for the decryption keys required for symmetric cryptography.

3. PROPOSED APPROACH

This study proposes a Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service. The concept is based on separating the storage and encryption/decryption of user data, as shown in Fig. 1. In this business model, Encryption/Decryption as a Service and Storage as a Service (SaaS) are not provided by a single operator. In addition, the SaaS provider may not store unencrypted user data and, once the provider of Encryption/Decryption as a Service has finished encrypting the user data and handed it off to an application (e.g. a CRM system), the encryption/decryption system must delete all encrypted and decrypted user data.

![Fig 1: Encryption/Decryption as an independent service](image-url)
To illustrate the concept of our proposed business model, Fig. 2 presents an example in which the user uses separate cloud services for CRM, storage and encryption/decryption. According to the user’s needs, CRM Cloud Services could be swapped for other function-specific application services (e.g., ERP Cloud Services, Account Software Cloud Services, Investment Portfolio Selection and Financial Operations Cloud Services)[2].

Fig 2: Business model concept integrating separate cloud services for data encryption/decryption, CRM and storage

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.

DESCRIPTION OF THE 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 key- and 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.

Subkeys:

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 subkeys will be described later.

Encryption:

Blowfish is a Feistel network consisting of 16 rounds (see Figure 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 2^32) XOR S3,c) + S4,d mod 2^32

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 subkeys are stored in cache.

Generating the Subkeys:

The subkeys 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 Pi 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 subkeys 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 subkeys.

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
Applications can store the subkeys rather than execute this derivation process multiple times.

4. EXPERIMENTAL RESULTS

All experiments were performed with the configurations Intel(R) Core(TM)2 CPU 2.13GHz, 2 GB RAM, and the operation system platform is Microsoft Windows XP Professional (SP2).

Home page of Cloud Security:

LMS home page: If the cipher server is alive

Cloud Service Login Page:

Error Status page in LMS:

Cloud Services after login:

If Cloud System is Hacked:
5. CONCLUSION AND FUTURE WORK

This system effectively identifies security laws in the CRM applications using Blowfish algorithm effectively. 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.

6. REFERENCES