International Journal of Recent Research and Review, Vol. IV, December 2012
ISSN 2277 – 8322

Data Security & Privacy Protection: Primary Inhibitor for Adoption of Cloud Computing Services

Vidhi Agarwal[1], Raj Yadav[2]
Depatment of SE[1] &CSE[2],
PCE[1] & KITE[2], Jaipur (Rajasthan)
Email: vidhiagarwal31@gmail.com, yadavrajc@gmail.com

***Abstract* - In cloud computing, the data will be stored in storage provided by CSP.Service providers must have a viable way to protect their user's data, especially to prevent the data from disclosure by Malicious Insiders. Storing the data in encrypted form is a popular and common method of protecting user's data . If a cloud is responsible for storage and encryption/decryption of data, then *Malicious Insiders* may simultaneously obtain encrypted data and decryption keys. This allows them to access information without authorization and thus poses a risk to user's data. This paper proposes a Solution for cloud computing based on the concept of separating the encryption and decryption service from the storage service.**

Furthermore, the Server responsible for the data storage must not store data in plaintext, and the Server responsible for data encryption and decrryption must delete all data after the computation of encryption or decryption tasks. A CRM service is described in this project as an example to illustrate the Security Solution, which deals with a unique ID among all the servers.

A CRM (Customer Relationship Management with Information Centric Authority) service is described in this project as an example to illustrate the business model.

***Keywords*- CRM, Malicious Insiders, CSP, API.**

I. INTRODUCTION

Cloud computing could be defined as the integration of virtual resources according to user's requirements, flexibly combining resources including hardware, development platforms and various applications to create services. The special features of cloud computing include the storage of user data in the cloud and the lack of any need for software installation on the client side. As long as the user is able to connect to the Internet, all of the hardware resources in the cloud can be used as client-side infrastructure.

II. TYPES OF CLOUDS

Cloud providers typically centre on one type of cloud functionality provisioning: Infrastructure, Platform or Software / Application, though there is potentially no restriction to offer multiple types at the same time, which can often be observed in PaaS (Platform as a Service) providers which offer specific applications too, such as Google App Engine in combination with Google Docs[8]. Due this combinatorial capability, these types are also often referred to as "components" Literature and publications typically differ slightly in the terminologies applied. This is mostly due to the fact that some application areas overlap and are therefore difficult to distinguish. As an example, platforms typically have to provide access to resources indirectly, and thus are sometimes confused with infrastructures [4]. Additionally, more popular terms have been introduced in less technologically centered publications.

The following list identifies the main types of clouds (currently in use):

*A) Infrastructure as a Service***:** (IaaS) also referred to as Resource Clouds, provide (managed and scalable)

resources as services to the user – in other words, they basically provide enhanced virtualization capabilities. Accordingly, different resources may be provided via a service interface: Data & Storage Clouds deal with reliable access to data of potentially dynamic size, weighing resource usage with access requirements and / or quality definition.
*Examples***:** Amazon S3, SQL Azure.
Compute Clouds provide access to computational resources, i.e. CPUs. So far, such low-level resources cannot really be exploited on their own, so that they are typically exposed as part of a "virtualized environment" (not to be mixed with PaaS below), i.e. hyper visors. Compute Cloud Providers therefore typically offer the capability to provide computing resources (i.e. raw access to resources unlike PaaS that offer full software stacks to develop and build applications), typically virtualized, in which to execute cloudified services and applications. IaaS (Infrastructure as a Service) offers additional capabilities over a simple compute service.
Examples: Amazon EC2, Zimory, Elastichosts.

*B) Platform as a Service***:** (PaaS), provide computational resources via a platform upon which applications and services can be developed and hosted. PaaS typically makes use of dedicated APIs to control the behaviour of a server hosting engine which executes and replicates the execution according to user requests (e.g. access rate). As each provider exposes his / her own API[4]according to the respective key capabilities, applications developed for one specific cloud provider cannot be moved to another cloud host – there are however attempts to extend generic programming models with cloud capabilities (such as MS Azure).
Examples: Force.com, Google App Engine, Windows Azure (Platform).

*C) Software as a Service***:** (SaaS), also sometimes referred to as Service or Application Clouds are offering implementations of specific business functions and business processes that are provided with specific cloud capabilities, i.e. they provide applications / services using a cloud infrastructure or platform, rather than providing cloud features themselves. Often, kind of standard application software functionality is offered within a cloud.
*Examples***:** Google Docs, Sales force CRM, SAP Business by Design.

III. TOP THREATS TO CLOUD COMPUTING

Customers are both excited and nervous at the prospects of Cloud Computing. They are excited by the opportunities to reduce capital costs. They are excited for a chance to divest themselves of infrastructure management, and focus on core competencies[2]. Most of all, they are excited by the agility offered by the on-demand provisioning of computing and the ability to align information technology with business strategies and needs more readily. However, customers are also very concerned about the risks of Cloud Computing if not properly secured[7], and the loss of direct control over systems for which they are nonetheless accountable.

Following threats after Reviewing (Security Guidance for Critical Areas in CC) are identified:

Abuse and Nefarious Use of Cloud Computing

Impact: Criminals continue to leverage new technologies to improve their reach, avoid detection, and improve the effectiveness of their activities. Cloud Computing providers are actively being targeted, partially because their relatively weak registration systems facilitate anonymity, and providers' fraud detection capabilities are limited.

Insecure Application Programming Interfaces

Impact: While most providers strive to ensure security is well integrated into their service models, it is critical for consumers of those services to understand the security implications associated with the usage, management, orchestration and monitoring of cloud services. Reliance on a weak set of interfaces and APIs exposes organizations to a variety of security issues related to confidentiality, integrity, availability and accountability.

Malicious Insiders

The risk of malicious insiders has been debated in the security industry. While the level of threat is left to

debate. (I stated “If user will pay, user will use the service then why he will take tension”)

CERN defines an insider threat as such:

“A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.”

Shared Technology Vulnerabilities

Impact: Attacks have surfaced in recent years that target the shared technology inside Cloud Computing environments. Disk partitions, CPU caches, GPUs, and other shared elements were never designed for strong compartmentalization. As a result, attackers focus on how to impact the operations of other cloud customers, and how to gain unauthorized access to data.

Data Loss/Leakage

Impact: Data loss or leakage can have a devastating impact on a business. Beyond the damage to one’s brand and reputation, a loss could significantly impact employee, partner, and customer morale and trust. Loss of core intellectual property could have competitive and financial implications. Worse still, depending upon the data that is lost or leaked, there might be compliance violations and legal ramifications.

Account, Service & Traffic Hijacking

Impact: Account and service hijacking, usually with stolen credentials, remains a top threat. With stolen credentials, attackers can often access critical areas of deployed cloud computing services, allowing them to compromise the confidentiality, integrity and availability of those services. Organizations should be aware of these techniques as well as common defense in depth protection strategies to contain the damage (and possible litigation) resulting from a breach.

IV. EXISTING CLOUD SERVICES

The hardware and architecture required for providing cloud computing environment services is similar to most computer hardware and software systems. The hardware in a modern personal computer (i.e., CPU, HDD, optical drive, etc.) performs basic functions such as performing calculations and storing data. The operating system (e.g., Windows XP) is the platform for the operations of the basic infrastructure, and text processing software such as MSWord and Excel are application services which run on the platform. The architecture of cloud services can be divided into three levels: infrastructure, platform, and application software. Application software constructs the user interface and presents the application system’s functions[4]. Through the functions of the operations platform, the application can use the CPU and other hardware resources to execute calculations and access storage media and other equipment to store data. Building a cloud computing application as a service requires infrastructure, platform and application software which can be obtained from a single provider or from different service providers. If the revenue for cloud services primarily comes from charging for infrastructure, this business model can be referred to as Infrastructure as a Service (IaaS). If revenue comes primarily from charging for the platform, the business model can be referred to as Platform as a Service (PaaS). If revenue primarily comes from charging for applications or an operating system, the business model can be referred to as Software as a Service (SaaS).

Summarizing fig1. existing cloud services[7].

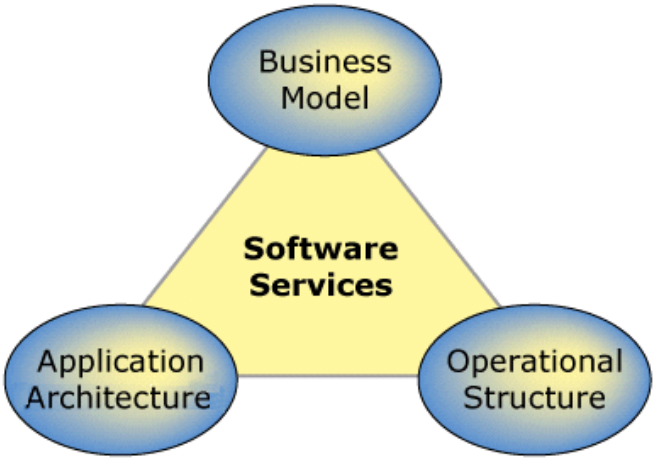

Figure 1. Existing Architectural Strategies.

Cloud computing business operations structure presents a hierarchical structure, with Platform as a Service as the value-added infrastructure service. The Application is built on the infrastructure and computing platform, and requires a specific user interface.

A. User data privacy concerns in a cloud computing environment

In a cloud computing environment, the equipment used for business operations can be leased from a single service provider along with the application, and the related business data can be stored on equipment provided by the same service provider. This type of arrangement can help a company save on hardware and software infrastructure costs, but storing the company's data on the service provider's equipment raises the possibility that important business information may be improperly disclosed to others. Some researchers have suggested that user data stored on a service-provider's equipment must be encrypted. Encrypting data prior to storage is a common method of data protection, and service providers may be able to build firewalls to ensure that the decryption keys associated with encrypted user data are not disclosed to outsiders. However, if the decryption key and the encrypted data are held by the same service provider, it raises the possibility that high-level administrators within the service provider would have access to both the decryption key and the encrypted data, thus presenting a risk for the unauthorized disclosure of the user data.

B. Existing methods for protecting data stored in a cloud environment

Common methods for protecting user data include encryption prior to storage, user authentication procedures prior to storage or retrieval, and building secure channels for data transmission. These protection methods normally require cryptography algorithms and digital signature techniques, as explained below:

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 (ECC). 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.

The use of passwords as an authentication process is more familiar to general users, but messages sent by the user are vulnerable to surreptitious recording by hackers who can then use the data in the message to log into the service as the user. In more advanced authentication systems, the system side will generate a random number to send the user a challenge message, requesting the user to transmit an encrypted response message in reply to the challenge message, thus authenticating that the user has the correct encryption key. Without this key, the user will not be allowed access. In the process of challenge and response the client's encrypted key uses the client's password to convert a derived value and. In this program, each communication between the client and server is unique, and a hacker using an old message would fail to access the system. In addition, the One-Time Password (OTP) authentication system differs from most peoples' conception of a password. Most people

understand a password to be a password chosen by the user to be meaningful, and can be used again and again. The emphasis of OTP, however is the single-use nature of the password.

After receiving authentication from the user, the system side must create a secure transmission channel to exchange information with the user. The Secure Sockets Layer (SSL) is a common method of building secure channels, primarily using RSA encryption to transmit the secret keys needed for the both sides to encrypt and decrypt data transmitted between them. When using cryptographic technology to protect user data, the keys used for encryption and decryption of that data must be securely stored. In particular, cloud computing service providers must have specific methods for constraining internal system management personnel to prevent them from obtaining both encrypted data and their decryption keys – this is critical to protecting user data. Operator policies for protecting user data must be clearly laid out in the Service Level Agreement (SLA) and must explain how special privilege users are prevented from improperly accessing user data.

Kandukuri, Paturi and Rakshit offer six recommendations for SLA content, including (1) special privilege user data access must be controlled to prevent unauthorized storage or retrieval, (2) cloud computing services must comply with relevant laws, (3) user data must be properly stored and encrypted, (4) a reset mechanism must be provided in case of service disruption or system crash, (5) service must be sustainable and guaranteed against service discontinuation due to change or dissolution of the provider and (6) if cloud computing services are used for illegal purposes, the provider must be able to provide records to assist with investigations.

Related Work

In our proposed system, the authorization for the storage and encryption/decryption of user data must be vested with two different service providers[1]. As our 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 Propose Solution, 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.

In this project Advanced Encryption Standard (AES) algorithm is used to encrypt/decrypt the data.

Features of AES Encryption Algorithm:

- Advanced Encryption Standard (AES) algorithm works on the principle of Substitution Permutation network.
- AES doesn’t use a Feistel network and is fast in both software and hardware.
- AES operates on a 4×4 matrix of bytes termed as a state
- The Advanced Encryption Standard cipher is specified as a number of repetitions of transformation sounds that convert the input plaintext into the final output of cipher text.
- Each round consists of several processing steps, including one that depends on the Encryption key.
- A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key.

Advantage in Proposed System

- Advanced Encryption Standard not only assures security but also improves the performance in a variety of settings such as smartcards, hardware implementations etc.
- AES is federal information processing standard and there are currently no known non-brute-force direct attacks against AES.

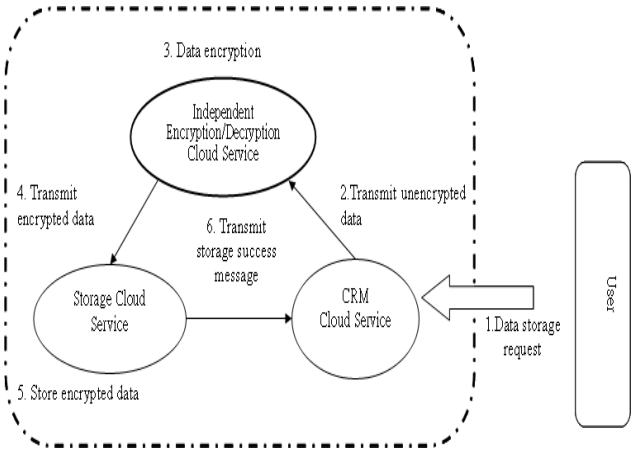

Fig.2 Data Storage Diagram

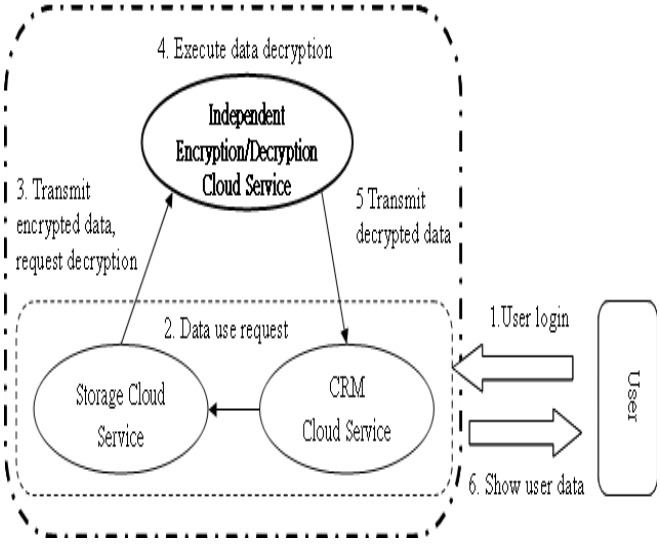

Fig. 3 :Data Retrieval Diagram

V. CONCLUSION

This system effectively identifies security laws in the CRM applications using Advanced Encryption Standard 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 Cloud Flare in order to give more security cloud services and less trafficking to the end users.

VI. REFERENCES

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

[2] B. R. Kandukuri, V, R. Paturi and A. Rakshit, "Cloud security issues," in Proceedings of the 2009 IEEE International Conference on Services Computing, pp. 517-520, September 2009.

[3] R. Sterritt, "Autonomic computing," Innovations in Systems and Software Engineering, vol. 1, no. 1, Springer, pp. 79-88. 2005.

[4] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility," Future Generation Computer Systems, vol. 25, issue 6, pp. 599-616, June 2008.

[5] 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.

[6] 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.

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

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

[9] R. Rivest, A. Shamir, and L. Adleman, "A method

for obtaining digital signatures and public key cryptosystems", Communications of the ACM, vol. 21, no. 2, pp.120-126, 1978.

[10] V. Miller, "Uses of elliptic curves in cryptography," Advances in Cryptology - CRYPTO '85, Lecture Notes in Computer Science, pp. 417-426, 1986.