International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 03, Issue 09, September 2014 ISSN 2319 - 4847

A Review of Cloud Security Issues and Data Protection Techniques

Pallav Sharma[1], Dr. Varsha Sharma[2]and Dr. Sanjeev Sharma[3]

[1]Research Scholar, School of Information Technology, Bhopal, M.P.

[2]Professor, School of Information Technology, Bhopal, M.P.

[3]HOD, School of Information Technology, Bhopal, M.P.

ABSTRACT

Cloud Computing is an emerging technology that has practically opened the space for virtualization by providing many computing and storage services over the Internet. Cloud computing has at its core services like platform, infrastructure and software as a service. The recent boom in cloud computing is driven by its simplest economical benefits. It helps by reducing capital expense and operating expenses. Even with its features cloud computing, introduces a new headache of less data security and control over data as the data resides on third party's premises to which the cloud service provider and the cloud user have no control. This paper mainly focuses on several security issues that have been introduced as a by-product of cloud computing and also discusses some of the security techniques that have been proposed to protect the user data over the cloud by reviewing some of the prior works.

Keywords: Cloud Computing, Security Issues, Data Storage, Encryption.

1. INTRODUCTION

For many years internet is shown in form of a cloud symbol in a network diagram until in the year 2008 a vast number of services started to merge the permitted computing resources to be accessed over the internet which then came to be known as cloud computing. A cloud computing model in simple words refers to access to a pool of resources provisioned via internet for rent. However, the definition of cloud proposed by National Institute of Standards and Technology(NIST) U.S. states that, "Cloud Computing is model to enable convenient, uninterrupted, on-demand network access to a pool of shared configurable computing resources (like storage, application, networks, servers, services) that can rapidly provisioned and released with minimum management effort or service provider interaction"[1]. The main driving force towards cloud computing is cost reduction, hassle free startup for small business organization, or increasing computing resources by renting them instead of buying new hardware or software. A move towards cloud seem cost effective, it unfortunately increased an overhead and major concern for privacy and security. In this paper we not only discuss various security issues raised because of cloud but also some of the security techniques that have been proposed in the past to deal with security concerning data storage over the cloud. In this paper we discuss in-depth details of various security issues rising mostly with public cloud and might need a little extra looking into. In this paper we provide a vivid demonstration of security issues by using multi-level approach. Also this paper is divided in a way that it gives a brief introduction to cloud and various issues regarding security. Irrespective of all the hype surrounding the cloud it is still not as much popular among the customer because of the security issues raised by the cloud features like 3rd party data storage centers, less control of your own data. In fact, security was ranked top among many surveys that were conducted as shown in figure 1.

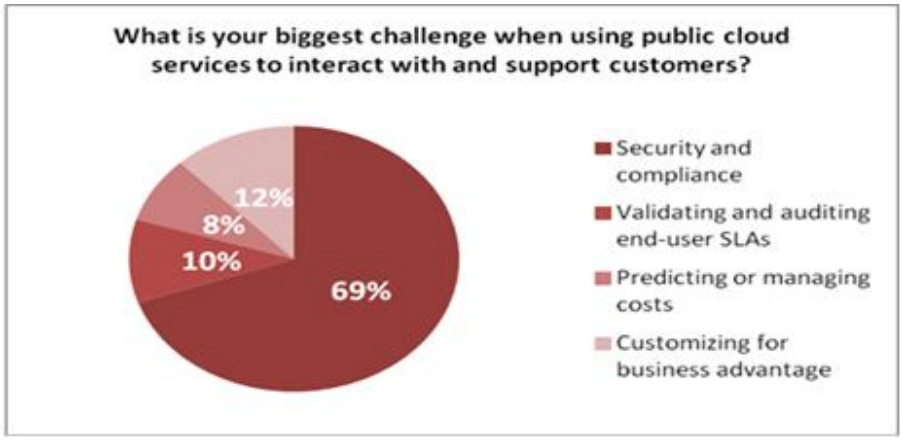

Figure 1: Result of Survey conducted by CA Technologies in March, 2012[2]

1.1 Cloud Computing

Cloud computing is a technology that takes virtualization to new heights. It allows one to break the barriers of space i.e. storing the data somewhere and accessing it from another location. Although this is one of the many features of the cloud, some others are like – application services, storage space, servers, processors etc. One of the most important feature of cloud is that instead of buying, one is allowed to rent these services or hardware and pay only for the service that you. For example, if one has to rent space of around 10 GB then they only pay a rent for that space, this allowed the user to get extension of space for their personal needs instead of buying a new Hard Drive. The above feature of cloud computing can be best understood by this another example, suppose a user is working on a Linux based and they have to perform some task or project that requires them to shift to another operating system like windows. Now for working on single project it would be considered a waste to buy a whole operating system. However because of cloud a user is allowed to rent an instance of such OS from a Cloud Service Provider (CSP) and pay only for the period of time they use it. Cloud computing models as proposed by NIST consists of two basic types of models –

- Deployment Model
- Service Model

1.1.1 Deployment Model

Deployment model is referred to as a model which describes the nature of a cloud based on its deployment. There are only three types of deployment models which are as follows:

1.1.1.1 Public Cloud

A public cloud is defined as a cloud in which the infrastructure and the computational resources that it contains are available to general public over the internet. It is owned by a cloud service provider (CSP) giving cloud services to the user. Public cloud by definition is external to a consumer organization.

1.1.1.2 Private Cloud

Private cloud as described by NIST is a cloud in which the computing environment is operated only for a single organization. It may or may not be managed by the organization itself and it can either be located on the primes of the organization or it may be located outside it. A private cloud allows for a greater potential to the organization by providing greater control over cloud consumers, computing resources, infrastructure than a public cloud can offer.

1.1.1.3 Community Cloud

A community cloud can be said to exist between the boundaries of private cloud and public cloud, since a community cloud targets a particular set of customers. It is more or less similar to private cloud deployment model but the computational resources and infrastructure may be exclusive to two or more organization that have similar regulatory, privacy and security considerations rather than a single organization.

1.1.1.4 Hybrid Cloud

Hybrid clouds are more complex when compared to other cloud deployment models as they are made up of two or more clouds (like public, private or community), in which all clouds retains their discrete identity but are brought together by some technology that allows data and application portability between them.

1.1.2 Service Models

Service Models are equally as important as the deployment models. A service model actually dictates the type of service a cloud will provide. A service model can be formed by either of the deployment models. There are three service models that are described by NIST which are as follows:

1.1.2.1 Software as a service (SaaS)

Software as a Service is a service delivery type of model that provides a user with one or more applications and also the computational power needed to run them to be used on demand. The main objective of this model is to reduce the total cost of software and hardware development, operations and maintenance etc. Security is carried by cloud service provider and the user has no control over the underlying architecture except for limited admin control and some preference selections.

1.1.2.2 Platform as a Service (PaaS)

Platform as a service is a service delivery type of model where on consumers' demand he/she is provided with a complete computing platform on which applications can be build and deployed. The main purpose of PaaS is to decrease the cost and the underlying hardship to buy, house and manage the hardware and software components required by the platform inclusive of any programs or database tools. The environment for development is determined by cloud provider. In this model the consumer has the environment of applications and their setting of the platform. Security is managed by both cloud consumer and cloud provider.

1.1.2.3 Infrastructure as a Service (IaaS)

Infrastructure as a service is a service delivery type of model where on consumers' demand an infrastructure comprising of network equipments, servers and software are provided upon which a platform to develop and execute applications can be created. The main goal of this model is to avoid buying, storing and managing hardware, software components and instead obtain them on rent basis as virtualized objects that can be controlled using service interface. Security provision is maintained by cloud consumer except for the infrastructure which is secured by the cloud service provider.

2. SECURITY ISSUES

Cloud computing is now gaining more and more popularization because of its virtualization feature and ease of access from anywhere through the internet. So, it also important to point out area concerning the security as much as possible by briefly studying research that had been done by many scholars or researchers experiment the current technologies. This section depicts the security issues that are considered to be the most important areas of cloud computing by organizing them in different categories such as issues in service model, service level agreement, governance, trust, network security, data security etc.

2.1 Issues in Service Models

As we have already discussed earlier that the cloud computing model consists of different delivery model, for various types of services provided to a cloud consumer. These models basically provide services like platform, infrastructure and hardware as demanded by the cloud consumer. The security and control depends on the type of the model that is being used.

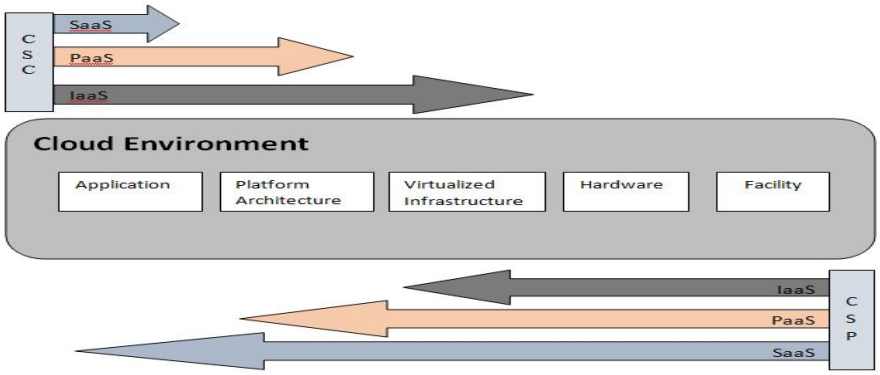

Figure 2: Scope and Control among Cloud Service Models.[3]

Figure 2 shows the various components used by the service Modes. We can see from the figure that more the servies from the CSP the less control and scope of Cloud Service Consumer (CSC). It is the duty of CSP to implement and manage securities as data cofridentiality and security is more important especially to a business critical organisation. But the guarantee of security is difficult as the CSP provides different types of services like XaaS (where X refers to the type of service provided by CSP). Infrastructure as a Service (IaaS) allows for developers or small or medium scale organizations that cannot afford to spend more money for new sets of hardware or specialized personal to meet the new trends in technological advancement. Instead of buying these resources they just rent such machines in form of Virtual Machines (VMs) and network storage that can accessed through a wide area network over the internet. But the problem in IaaS lies that they do have no idea how the VMs allotted by them are utilized by the consumer. This can understood by the fact that some hackers used the VMs they rented from Amazon EC2 to gain access to user data of other consumers and then also data of Sony PS3 from the cloud [4].So, the security is a major concern in IaaS as CSP has no way of knowing anything about the program that is running on the CSC side. Platform as a Service (PaaS) is the second service delivery model used by the cloud computing environment. PaaS provides platforms that allow the cloud consumer to build and deploy applications. Even though cloud consumer has more control in PaaS but the security apart from application level like host intrusion or network security are still associated with CSP. Hence, it is the job of CSP to make sure that the applications do not access data from other applications. PaaS can be seen as extension of the Software as a Service (SaaS) as this model allows user to develop applications with features designed by them. PaaS also increases feature and security capabilities as the inbuilt security and capacity are not much flexible. Software as a Service (SaaS) is the cloud computing environment where the cloud consumer is provided with the applications developed by various developers. The consumer then uses the software application via the internet by demanding it from the CSP. SaaS allows the cloud consumer to access many applications on various hand held devices. It also reduces cost and improves the overall efficiency. However many of the organizations and general public is not satisfied with SaaS as it lacks transparency i.e. the cloud consumer has no knowledge of data locality and data security. Hence it

is a very big task for CSP to provide with a way to increase the trust among consumers as well data security, so that the data remains protected.

2.2Issues in Service Level Agreement

Service Level Agreement (SLA) isan agreement between CSP and CSC that decides the nature of type of service provided. Here the nature of service depicts the mutual understanding between the CSP and CSC about what to expect from the service and how will the CSC be compensated in case of failure to deliver the said quality of service. SLA in general is an agreement that decides licensing, suspension and termination, terms of service, privacy policy and security policy that will be implemented. There are two types of SLA that are already defined [5] they are Non-Negotiable SLA and Negotiable SLA. Non-Negotiable SLA are much more bend towards CSP as they allow them to change terms of services without notifying the CSC [5]. On the other hand Negotiable SLA are very much like nowadays IT outsourcing contracts. They deal with the privacy policy and security policies. They also address issues like control over employees, data encryption, data ownership and use of products is in compliance with national and international standards. The non-negotiable SLAs can be considered as a rough move towards CSC as these type of SLAs give almost all power and control to CSP because the CSP has the right to change the agreements without notifications. This causes insecurities in CSCs as they have no control over their assets. Therefore to increase a trustable security more and more negotiable agreements should be formed between CSP and CSC.

2.3Issues in Identity and Access Management as a Service (IDaaS)

As the security concerns with the identity of a consumer and the access of data by its right owner increased, the cloud came up with a new group Identity and Access Management as a Service (IDaaS) which is a part of XaaS. We know that the SaaS handles a large amount of user data and the identification of correct user was becoming more of a problem that raised the issue of data access management. On the other hand IaaS has to handle multiple VMs that should be accessed only by the intended user. Security issues raised in IDaaS are different than those of IaaS, PaaS or SaaS as they also depend on the fact whether the identity is externalized to or managed by the cloud [6]. The users handled by IDaaS can be either 'internal' or 'external' to an organization or may not even belong to any organization and simply be consumer of a service. The security issues pertaining to each scenario is completely different and impact different stakeholders within an organization. Here the problem faced by the consumer is having their identities serviced in cloud environment, which may give rise to issue of reputation that should be considered by both CSCs and CSPs.

2.4 Issues in Governance

Any service that starts needs some form of governance. A governing association is one which has the responsibilities like procedure and standards for storage, control over policies, applications, and they also have the task of monitoring the deployed services. Since cloud computing environment provides many services and applications, a need for governance is mandatory. Lack of this might lead to problem arising in future uses. Even though cloud computing environment provides many platforms at different levels but to be able to manage such platforms skilled workers are needed.

Well it is true that cloud computing provides for some of the cheapest solutions and also decreases the overall capital investment and allows for such expenses to be projected into development of applications. Here the CSP is deploying the same environments to different clients as it is providing the same infrastructure via different VMs. But poor governance from CSPs might result in the loss of the client and thereby decreasing the credibility of the CSP. Therefore it is very important for CSPs and CSCs that the provider implements good governance to look after its policies, security risk and privacy procedures.

2.5 Issues in Compliance

Compliance refers to the appearance of laws, regulations and standards. The laws, regulations and rules for privacy and security are different for different locations. Every country, state and local bodies have their own rules and regulations. Compliance is very important issue when it comes to cloud computing.

- Regulations and Laws: As we discussed earlier that laws and regulations are different for different places. Governments need special acts that they can use to control the privacy and security issues. Like the Payment Card Industry Data Security Standards (PCIDSS), will apply to a particular industry. CSPs are more sensitive towards regulatory and legal concerns and may be willing to agree to process or store data in a particular jurisdiction and may apply protection for privacy and security. Although the extent to which they might accept liability to exposure of data under their control is still to be seen. Irrespective of this the organizations are still held responsible for the privacy and security of data that is under their control. In INDIA the first law regarding Information Technology was drafted in 1999 and came into force in 2000. Later this law was amended and came in force in 2009. The law allowed the government right to read organizational data but still the law does no deal with the data that is stored outside country boundaries. So, if any problems arise to a consumer regarding his/her data then the current law does not provide much help if the data center used by the CSPs resides in another country. Therefore, there is a

need to form regulations specifically for cloud computing environments that protects the interest of cloud consumers. This can be done by forming a committee that should comprise of representatives from different countries and drafting rules and regulations that can be accepted and applied globally.

2.6 Trust

Any type of consumer-provider system that exists requires trust. Consumer always has to trust the service provider. Cloud computing is no exception to such trend. Since, in cloud computing environment the cloud consumer provides the CSP with their digital assets that the CSPs have total control over.

2.6.1 Malicious Insider

A malicious insider is a threat to an organization in form of a current or former worker, business partners or contractors who have or had access to the company's network, data, or system and they intentionally used that access in such a way that it affected the organizations integrity, confidentiality, or availability of organizations' information or systems. Following are some vulnerability due to malicious insider:

- Rogue Administrator [7]: An attack often related to this insider is theft of important and sensitive data, which can result in data confidentiality loss or loss of data integrity. The rogue admin is usually motivated financially.
- Exploit Weakness Introduced as by-product of Cloud usage [7]: Insider within the organization can use the vulnerabilities that are introduced by the usage of cloud and use them to access confidential and private data.
- Using cloud to conduct malicious activity [7]: Another type of cloud related insider is the one who uses the cloud for the purpose of carrying out an attack on his/her own employer.
- Lack of transparency in Management Process: Due to lack in CSPs procedure and process, insider often gain privileged access. Insider activities are often bypassed by Intrusion Detection system (IDS) or firewall assuming that these are legal activities.

2.6.2 Composite Service

This issue can be described as the more than two CSPs. It means that one SaaS provider can build their application on the services provided by PaaS which in turn may be using the services of an IaaS provider. Hence in here the renting or hiring is done on a multilevel. Here the services are basically rented or outsourced to a third party which can raise serious trust because of multiple parties involved.

2.6.3 Visibility

Visibility here refers to the transparency provide by the CSPs that controls the vital parts for a very effective oversight of the system privacy and system security. Security issues must be transparent to the cloud consumers. There should be a detailed and effective monitoring of the network, systems and storage.

2.7 Architecture

The architecture of cloud comprises of both software and hardware. The software that usually works on the hardware are VMs. So in general an IaaS supports VMs which are loosely attached to the underlying hardware and the whereabouts of the location of these hardware is only known to CSPs. Attack Surface in the cloud can be done on both the hardware and software level. The security of hardware against physical theft is handled by CSPs and cannot be considered irrelevant. But the most important security issue is on the virtual layer that serves a common layer to both hardware and software. VMs are deployed on this middle layer. However the complexity that arises in deployment of the VMs is a major security concern. As we know virtualization is the key to cloud computing environment. But if someone has sufficient privileges to access the middle layer, then they can alter or observe any data or process. Image sharing is one of the most common practice in CSPs. These image storages should be controlled and monitored to detect for attempts on security breach.

2.8 Data Protection

In cloud the applications that are deployed and managed on the CSPs premises, the data is under the protection and control of the organization as data resides on the same site as the CSP. However this may not will always the case as there are cases where the data resides outside of the CSPs boundaries. Such a case is of the public cloud. Here the CSPs must enable more security checks and protection techniques as the data resides on the premises of a third party and the CSPs have no physical access or control over that data. Therefore adequate data protection techniques must be implemented to protect the data. Some of these issues regarding data protection are discussed as follows:

2.8.1 Data Breach

Data Breach is referred to as an incident regarding data that involve accessing information which is sensitive, confidential or protected for the purpose of copying, theft, transmission that is used by an unauthorized personal. Data breaches may involve financial information like bank details or credit card, personal health information (PHI), personally identifiable information, trade secrets of a corporation or intellectual property. Following are the vulnerabilities that may result in data breach:

- Loss of Personally Identifiable Information (PII): A cloud consumer has to provide sensitive information regarding themselves (like name, credit card number, home address, phone number etc.) for being able to use the cloud services. But if this precious information is mishandled by the CSPs, it can lead to exposure of identity of the cloud consumer by people with malicious intent.
- Loss of Encryption Keys: This refers to the loss of secret keys to other parties or password disclosure to unauthorized personal, or loss or corruption of those keys or their unauthorized use for non- repudiation or authentication. If a key is lost the user might not be able to read their own data as it will be unreadable encrypted form that requires a key to decrypt it.
- Brute Force Attacks: A brute force attack is a technique which is used to crack password. This technique uses combinations of dictionaries and software programs to test hundreds of thousands of password combination per second and cracking passwords in a few minutes taking advantage of computing ability of cloud.

2.8.2 Data Loss

Data loss is referred to as the permanent unavailability of data. Data loss was the second most leading threat in 2013 as the hackers would gain access to sensitive data and delete it. While implementing securities those data sets should be considered that are heavily accessed. Following are some vulnerability that might result in data loss:

- Loss of Encryption Keys: If the key used to encrypt the data or the passwords are disclosed somehow, then there may be chance that a malicious person might use this information to gain access to the data and delete it. If there is no backup available the user might loose the data permanently.
- Cloud Service Termination: It refers to risk of user loosing their data in case the CSPs run out of business. On September 2013, a CSP Nirvanix announced that they will be shutting down their services due to lack of sufficient funds and the users have two weeks to migrate their data from the cloud or the data will be lost permanently.
- Hardware or Software Failure: Hardware or software failure may result in data loss. Data specially the data in transit have a great chance of being lost in event of a system crashing because of a software or hardware fault.
- Natural Disaster: Natural disasters such as floods, hurricane, earthquakes etc. are problems pertaining to a particular region. So if the cloud storage is located physically in one such region then there are chances that the data might get lost in event of such disasters, if the data is not backup regularly.

2.8.3 Data Locality

In cloud environment, the cloud consumers use the various applications provided by CSPs and process their business data. However, the cloud consumer has no idea whatsoever about the whereabouts of the location of the data storage facility. This can raise many issues. However there are many countries like European Union and South American countries that have laws which prohibit a particular type of information for leaving the countries as it may be potentially sensitive information [8]. A secure SaaS model is required which allows the CSC to be sure of the location of their data in order to increase reliability among CSPs.

2.8.4 Data Integrity

Data integrity refers to certainty that the data stored is truth and correct to the best available knowledge. Data Integrity is one of the most critical security issue in cloud computing environment. Data integrity in a standalone system with single database is easy as they use ACID properties to keep integrity of the data. But the complexity of data storage increases quite a bit when it comes to cloud environments. Cloud environment supports many different types of databases. So the integrity control is a little loose in order to allow some relaxation because of heterogeneity of the environment. However this loose control may allow direct access to databases thereby bypassing integrity controls. This can result in some big profound problems if not paid attention to.

2.9 Web Security

With more than 70% of attacks taking place through the web, it makes a critical piece in the overall cloud decision making process. XSS, SQL Injection, Session Hijacking etc. are some of the security issues in cloud web security and they are discussed in details as follows:

- Session Hijacking: Session hijacking attack [8] can only be performed if https is not used at all or only used during the login process. The problem with this is that if a cloud email process is affected them the malicious user might get additional information or even more passwords.
- SQL Injections [9]: Hackers exploits the vulnerabilities of web servers and inject malicious codes in order to bypass login and gain unauthorized access to backend database. When successful hackers are free to manipulate data or delete them or misuse them.
- Cross-site Scripting: This attack occurs when a cloud application sends data containing user information without validation. Hackers inject harmful scripts in such pages using VBScript, ActiveX, JavaScript, HTML and flash into vulnerable dynamic objects to gain access to user information.

3. Data Protection Techniques

As we have seen in the previous section that there are many security issues pertaining to cloud computing. However, we can see that issues regarding data are more serious and require more attention. The cause of this is the new technological trend that has changed the view of the people thereby making them more and more bend towards digitized world. The digital revolution has led to the digitization of almost all the data in todays' world. Even before the trending of cloud environment most of the organizations around the globe started doing their work in digital form. But the introduction of cloud increased this trend exponentially. The reason for this being that cloud allows for cheaper ways to store data, rather than buying a new storage and then buying another after the previous one is full. But as we have seen that cloud has also introduced some security issues of which the issue regarding data protection is discussed here. Here we discuss about some of the data encryption or protection techniques created by some research scholars. We will briefly see the working of these techniques and at the end we will create a table to compare these techniques.

3.1 Multimedia Security in Cloud Computing Environment Using Crossbreed Algorithm[22]

This technique was proposed by Sonal et al to increase the security of the multimedia data by using crossbreed algorithm. This work proposes a reference ontology framework for access control in a cloud environment to aid the design of security system and thereby reducing the complexity surrounding system design and implementations. This work exploits the ability of RSA to support public key cryptography and digital signatures. The idea behind the technique was to design algorithm based on the combination of both RSA and DES which will be provide for more and better security than either DES or RSA alone. This technique enhanced the data security and successfully prevented replay attacks. After this the result of the security service can be delivered to the designated service model and they can perform actions based in this security checking process. RSA algorithm is a public key cryptography which involves a private key and a public key. The public key is known to everyone and is used to encrypt the data, whereas the private key is known only to the user and is used to decrypt the data.

RSA generally three steps –

- First the key is generated before the encryption of the data. This is done between cloud user and CSP.
- After key generation the user data is encrypted by the CSP using the public key and stored in the cloud.
- When user accesses their data they use their own private to decrypt the data.

Data Encryption Standards (DES) is a block cipher encryption technique that divides the data into blocks of 64 bits and performs the encryption technique on each block separately. Decryption process is carried out in the same manner.

Limitation: However the combination of two cryptography technique increases the strength of the encryption technique, but the DES is the most oldest of the encryption techniques it dates back to at least 4 decades.

DES suffers from two major drawbacks –

- This technique breaks data into blocks of 64 bits and then applies encryption on each block separately. So if there is a repetition of data in plaintext it will allow two or more encrypted blocks to be identical, thereby easing the process of determining the key.
- The DES is not as strong now as it was in the good old days because now the computing power of today's system allows the brute force attack on DES to take less time thereby decreasing the safety of data secured using DES.

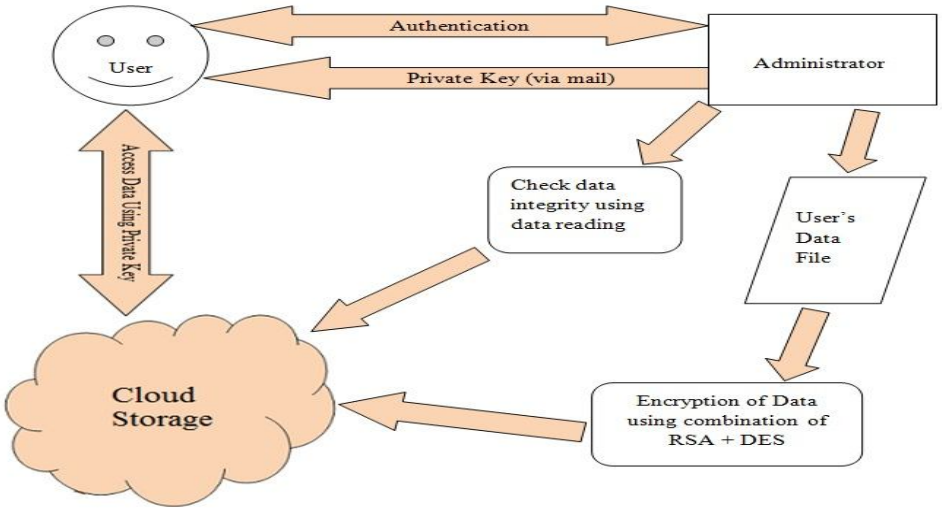

Figure 3: Flow diagram of the above method.

3.2 Multimedia Content Storage with Hybrid Encryption over Cloud Server[23]

This technique was proposed by Priyanka et al in form of a secure cloud framework. This technique proposed a security on the cloud side and also to make client data safe. For this they proposed a architecture. By using this architecture they provided security to the cloud and the user data. They divided the whole process in three modules that are described as follows:

- First they created a role based control for administrator to assign roles to authenticated users only. Only authorized users will be able to access files on the cloud. The authentication process will take place online on cloud itself.
- A technique based on combination of RSA and AES is used to encrypt data before storing it on the cloud.
- When the authorized user will try to access the file on cloud, the private key will be generated on runtime for decrypting the files. This key will be sent to the user via email. User will be required to enter the private key to access the data which will be valid for that particular session only.

RSA is public key cryptography algorithm designed by Rivest, Shamir and Adleman. It is also known as asymmetric cryptography technique, as the data is encrypted using a public key which is known to all whereas the data can only be decrypted using the private key which is known only by the intended user. AES stands for Advanced Encryption Standards which uses Rjindael designed by Rijmen and Daeman. AES is a block cipher encryption technique that divides the data into blocks of 128 bits each. AES generally have three variants that are used, 128 bits block with 128 bits key, 128 bits block with 256 bits key or 128 bits block with 192 bits key. AES is currently the most secured algorithm and takes the least time to encrypt the data. Limitation: Although a strong technique such as AES is used along with RSA thereby making the encrypted data more secure but the problem with the proposed work is that it requires the user to have access to their email to be able to receive the private key that is generated at runtime. This may not always be the case and might deny the user to access their own due to lack of private key that was delivered to mail which the user is unable to access.

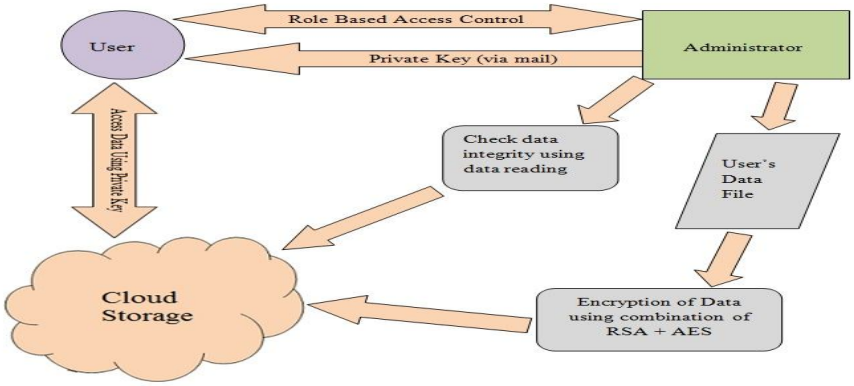

Figure 4: Flow diagram depicting the above method.

3.3 Cloud computing a CRM Service Based on Separate Encryption and Decryption using Blowfish Algorithm[24]

This technique was proposed by Rajiv et al. It proposed a model to encrypt the data in one service provider and store the data at another service provider. So as soon as the data is encrypted it is moved from the encryption service providers' side to the storage providers' side. Therefore the storage of data will be in the encrypted form and the administrators and the employees will have no knowledge of keys or the service provider for encryption and decryption. The concept is based on separating the encryption/decryption of user data and the storage. The steps for the whole process are as follows:

- First the user access CRM Cloud Service where they are verified for their credentials. After the clients 'successful login the CRM sends a request to the storage service.
- The storage system based on the users' ID received from the CRM identifies the user data which is in encrypted form. After successfully finding the data the encryption/decryption process must be invoked.
- The Storage service transmits user's encrypted data along with the user ID to the encryption/decryption service.
- After receiving the users' data and ID the encryption/decryption service the user's ID to index the users' data decryption key, which is then used to decrypt data.
- After the decryption process is completed successfully the client data is handed over to CRM which then displays this data to the user.

Blowfish was designed by Bruce Schneider in 1993 as a fast, free alternative to existing encryption algorithms. The Blowfish algorithm is a symmetric block cipher algorithm. It takes a variable length key from 32 bits to 448 bits making it ideal to secure data. Blowfish uses a large number of sub keys. These keys must be computed before the start

of the encryption or decryption process. The P-array consists of 18 sub keys with each key of 32 bits from P1-P18. There are four 32 bits S-boxes with each containing 256 entries. Limitation: Although no effective cryptanalysis has been found till date, the blowfish algorithm suffers from speed degradation during changing of keys because each new key requires pre-processing equivalent to encrypting 4 KB of text which is very slow compared to other block ciphers.

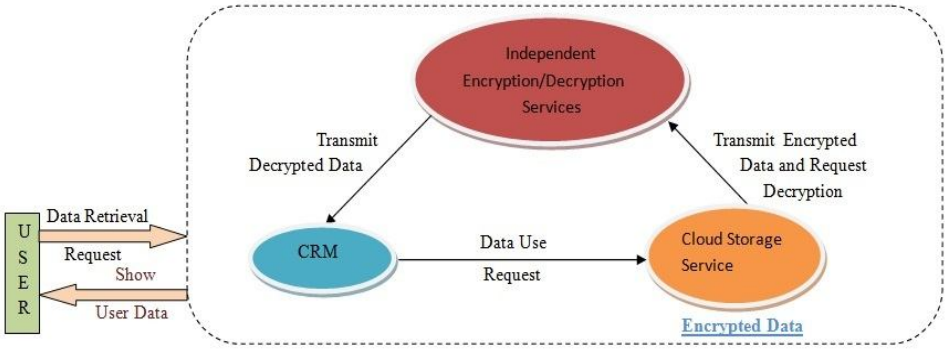

Figure 5: Flow diagram showing the working of above technique.

Table 1: Comparison of the techniques discussed above.

S.No.	Proposed Methodology	Algorithm(s) Used For Encryption/Decryption	Advantage	Limitation
1	Multimedia Security in Cloud Computing Environment using Crossbreed Algorithm	RSA in combination with DES	Increased encryption power. Hard to decrypt.	DES is outdated and suffers from brute force attacks.
2	Multimedia Content Storage using Hybrid Encryption over Cloud Server	RSA in combination with AES	More strength in encryption because of AES.	Private Key is sent to user via email and is valid for a single session only.
3	A CRM Service based on Separate Encryption/Decryption using Blowfish Algorithm	Blowfish	Blowfish is a fast block cipher that still has no effective cryptanalysis.	Speed degrades during key change phase as each new key requires pre-processing before continuation.

4. Conclusion

The arising need of cost cutting for resources or expenditure has spiked the interest of many in clouds. Specially the service delivery model that allow a cloud consumer to deploy applications or a small business without much of a hassle by doing the hard work of buying hardware or space. Now they just have to choose the right delivery model thereby saving manpower and money. Although the cloud from afar may seem like a golden goose but it actually also introduced some new issues. In this paper we discussed many of the issues that arise because of a move towards the clouds. We also discussed in detail some of the techniques proposed by various research scholars for the protection of data over the cloud. As we have shown, the numerous threats to the cloud computing environment that requires in-depth analysis and we still do not know what will be the impact of these issues in real world analysis of cloud environment.

References

[1] Wayne Jansen, Timothy Grance, “Guidelines for security and privacy in pubic cloud”, Draft Special Publication 800-144, September 2011.

[2] Sumner Blount, “CloudSecurity is still the biggest concern for adoption. But, is it valid?”, blogs.ca.com, April 11, 2012

[3] Yashpal Kadam, “Security Issues in cloud computing a transparent view”, International Journal of Computer Science and Emerging Technologies (IJCSET), E-ISSN: 2044-6004, Vol. 2, Issue 5, October 2011.

[4] Neal Leavitt, “Is Cloud Computing Really Ready for Prime Time?”, IEEE Computer, January 2009.

[5] Simon Bradshaw, Christopher Millard, Ian Walden, “Contracts for Clouds: Comparison and Analysis of terms and Condition of Cloud Computing Services”, Queen Mary School of Law Legal Studies, Research Paper No.63/2010, September 5, 2010.

[6] Jon Brodkin, "Loss of Customer Data Spurs Closure of Online Storage Services 'The Linkup'", Network World, August 11, 2008.
[7] William R Claycomb, Alex Nicoll, "Insider Threats to Cloud Computing: Directions for new Research Challenges", 36thIEEE International conference on Computer Software and Applications, 2012.
[8] E-week.com.Epsilon data breach, <URL: http://www.eweek.com/c/a/Security/Epsilon-Data-Breach-a-Training-Opportunity-on-Recognizing-Phishing-845929 .
[9] Christof Kauba, Stefen Mayer, "When the cloud disperse data confidentiality and privacy in cloud computing", University of Salzburg.
[10] Te-shun Chou, "Security Threats on Cloud Computing Vulnerabilities", International Journal of Computer Science and Information Technology (IJCSIT), Vol.5, No. 3, June 2013.
[11] Brin Hay, Kara Nance, "Storm cloud rising: security issues for IaaS cloud computing", Proceedings of the 44th Hawaii international conference on system science,2011
[12] Wayne A Jansen, "Cloud hooks: security and privacy issues in cloud computing", Proceedings of the 44th Hawaii international conference on system science,2011
[13] S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing", <URL: http://www.elsevier.com/locate/jnca
[14] http://www.cloudsecurityalliance.org/topthreats
[15] Rohit Ranchal, Bharat Bhargava, Lotfi Ben Othmane,Leszek Lilien, Anya Kim, Myong Kan, Mark Linderman, "Protection of Identity Information in Cloud Computing without Trusted Third Party," 29th IEEE International Symposium on Reliable Distributed System, 2010.
[16] Takahiko Kajiyama, "CLOUD COMPUTING SECURITY: HOW RISKS AND THREATS ARE AFFECTING CLOUD ADOPTION DECISIONS," San Diego State University.
[17] Kazi Zunnurhain and Susan V. Vrbsky, "Security Attacks and Solutions in Clouds," The University of Alabama.
[18] Dr. Ananthi Seshasaayee, Sreevidya Subramanian, "Review of Potential Threats on Cloud Computing".
[19] Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Avi Patel, Muttukrishnan Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," Springer Science+Business Media New York 2012.
[20] R. Kumar, **"**Reducing the Impact of Code Injection Vulnerabilities for Cloud Offerings", Volume 3, Issue 6, June 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.
[21] Harshal Mahajan, Dr. Nupur Giri, "Threats to cloud computing security", VESIT, International Technological Conference, January 03-04, 2014.
[22] Sonal Guleria, Dr. Sonia Vatta, "To Enhance multimedia security in cloud computing environment using crossbreed algorithm", International Journal of Application or Innovation in Engineering and Management (IJAIEM), Vol. 2,Issue 6, June 2013.
[23] Priyanka Gupta, Amandeep Kaur Brar, "Multimedia Content Storage with Hybrid Encryption over Cloud Server", International Journal of Advance and Innovative Research (IJAIR), Vol.2, Issue 7, July 2013.
[24] Rajiv R. Bhandari, Prof. Nitin Mishra, "Cloud Computing A CRM Service Based on Separate Encryption and Decryption Using Blowfish Algorithm", International Journal on Recent and innovation Trends in Computing and Communication (IJRITCC), Vol.1, Issue 4, April 2013.
[25] 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.
[26] 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.
[27] Atul Kahate "Cryptography and Network Security", Tata Mc-Graw Hill, 3rd Edition 2008
[28] Priyanka Arora, Arun Singh, "Evaluation and Comparison of Security Issues on Cloud Computing Environment" World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 2, No. 5, 179-183, 2012.
[29] Neha Jain and Gurpreet Kaur, "Implementing DES Algorithm in Cloud for Data Security" VSRD-IJCSIT, Vol. 2 (4), 2012, 316-321.

[30] N. Saravanan, A. Mahendiran, N. Venkata Subramanian, "An Implementation of RSA Algorithm in Google Cloud using Cloud SQL**",** Research Journal of Applied Sciences, Engineering and Technology 4(19): 3574-3579, October 01, 2012.

[31] R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public key Cryptosystems", Communications of the ACM, 21(2), 120-126, February 1978.