ISSN 2047-3338

Security Threat and Challenges Analysis of Cloud Computing with Some Solutions

Jihad Qaddour
School of Information Technology, Illinois State University Normal, USA
jqaddou@ilstu.edu

***Abstract*– Cloud Computing extends shared services to the businesses worldwide. It provides access to software and hardware resources to individuals and business without having to know the actual underlying infrastructure. It has evolved greatly as an industry inviting more and more users using services available from within their realm. Cloud computing has enormous benefits like Multi-tenancy, Massive scalability, Elasticity, pay as you go, Self-provisioning of resources. While there are so many benefits there are always risks involved with sharing resources, which leads to privacy and security concerns. In this paper we are going to investigate some of the security challenges faced in Cloud Computing and propose measures to overcome these. This paper focuses on various technical security issues like data security, authenticating users, host security and many more arising from the usage of Web Service in the Cloud Environment. Using AES encryption technique, we can encrypt the already modified data and store on cloud, as well as decrypt the data in a similar fashion on the receiving end.**

***Index Terms*- Cloud Computing, Service Models, Scalability, Elasticity, Security, Encryption and Decryption**

I. INTRODUCTION

THE present available high-capacity networks, cost-effective computers, and storage devices along with hardware virtualization have played a vital role in the evolution of cloud computing. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, application, and services) that can be rapidly provisioned and released with minimal management effort or services provider interaction [23]. It is an amazing concept that encapsulates the complexity and details of the infrastructure from users and applications by providing a very simple Graphical User Interface (GUI). It delivers computing resources over the Internet whereby individuals and businesses can use software and hardware managed by third parties at remote locations. In addition, the cloud-computing platform also provides on-demand services, anywhere, anytime.

Cloud computing provides economics of scale, professional network management, and professional security management. These features are so attractive to companies large and small, government agencies, and individual PC and mobile users. Those users only need to pay for services and storage they use. Moreover, those users do not have the hassle of setting up a database system, acquire the hardware, securing the network, doing the maintenance, and backing up their data, all these are part of the cloud service. Cloud computing includes a cloud networking, which refers to the networks and network management functionality that must be in place to enable cloud computing. More generally, cloud networking refers to collection of network capabilities required to access a cloud, including making use of specialized services over the Internet, linking enterprise data centers to cloud, and using firewalls and other network security devices at critical points to enforce access security policies. We can also think of cloud storage as cloud computing. In essence, cloud storage consists of database storage and database applications hosted remotely on the cloud servers [23].

Virtualization is the main enabling technology for cloud computing. It generalizes the physical infrastructure, which turns out to be the most rigid component, and makes it a soft component easy to use manage. It is based on Service-oriented Architecture (SOA), Utility Computing and Grid Computing. Cloud computing lends us the tools and technologies to build data or computation intensive applications with manageable prices when compared to traditional parallel computing techniques. Cloud model is composed of five essential characteristics, three of service models, and four deployment models.

This rest of the paper is organized in four sections: Section II covers an overview of cloud computing, Section III presents case studies related to different encryption methods. Section IV discussed security challenges of cloud computing and presenting some solution to these challenges. Lastly, we have the conclusion and the future work of cloud computing challenges.

II. OVERVIEW OF CLOUD COMPUTING

In this section, a brief overview of the basic concept of cloud computing (CC) will be explored. The overview is divided into three parts, cloud service models, essential

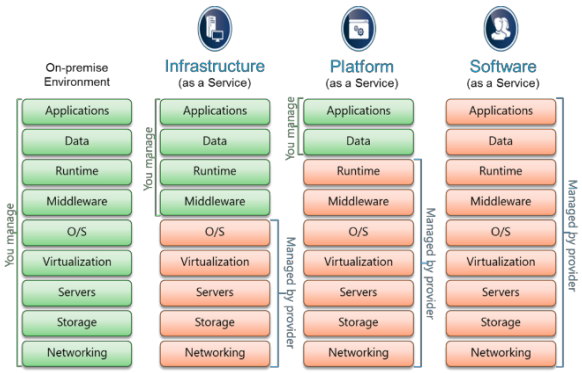

Fig. 1: Cloud Service Models

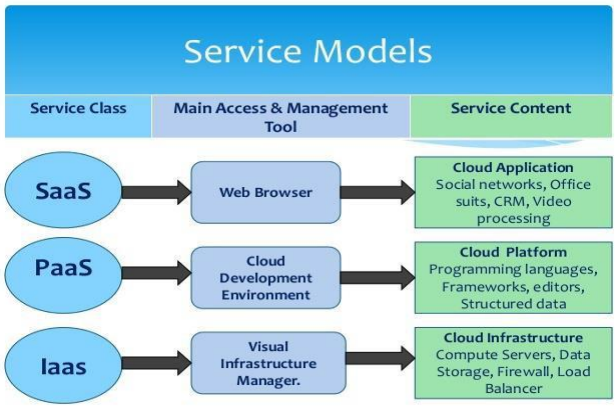

Fig. 2: Service Model Access and Contents

characteristics of CC, and deployment models of the cloud computing.

A) Cloud Service Models

NIST defined three types of services for the cloud model as shown in Fig. 1.

a) Software as a Service (SaaS)
b) Platform as a Service (PaaS)
c) Infrastructure as a Service (IaaS)

1) Software as a Service (SaaS)

SaaS is an ever-increasingly popular option for software distribution. Cloud provider (CP) provides service to customers in form of software, specifically application software running on and accessible in the cloud. The applications are accessible from various client devices through simple interface such as web browser. The use of SaaS avoids complexity of software installation, maintenance, upgrading, and patches. Example of services are Google Gmail, Microsoft 365, and Cisco WebEx. CP provides automatic backup and data sharing between the subscribers.

2) Platform as a Service (PaaS)

PaaS cloud provides service to the customer in the form of a platform on which the customer's application can run. A PaaS cloud provides useful software building blocks, and a number of development tools that assist in deploying new applications. In effect, PaaS is an operating system in the cloud. This model allows the user to have virtualized servers that they use for development and testing. For example Google (SaaS, PaaS), Google PaaS offers to build and host web applications on the Google infrastructure and SaaS offers business email and collaboration services. Big data as a service, database, business intelligence, and development and testing are examples of PaaS services.

3) Infrastructure as a Service (IaaS)

With IaaS, the customer has access to the resources of underlying cloud infrastructure. IaaS cloud provides virtual machines and other abstracted hardware and operating systems. IaaS offers customers processing, storage, networks, and other fundamental computing resource so that the customer can deploy and run arbitrary software. It is a standardized and highly automated, where a firm outsources the equipment used to support operations, including storage, hardware, servers and networking components. Example of IaaS are Amazon Elastic Compute Cloud (Amazon EC2), Microsoft Windows Azure, Google Compute Engine (GCE). IaaS services examples are backup and recovery, cloud broker, content delivery networks service management, and storage [23]. Fig. 2 depicts the service classes, access and management tools, and service contents for the service models.

B) Other Cloud Services

ITY-T-Y.3500 provides a number of other cloud services in addition to SaaS, PaaS, and IaaS as follows:

Communication as a Service (CaaS):

This service provides a unified interface and consistent user experience across multiple devices. Examples included video teleconferencing, web conferencing, instant messaging, and voice over IP.

Compute as a Service (CompaaS):

CompaaS may be though as simplified IaaS, with focus on providing compute capacity.

Data Storage as a Service (DSaaS):

DSaaS describes a storage model where the client lease storage space from a third-party provider. Customer transferred the data to the storage and use software for backup and data transfer.

Network as a Service (NaaS):

NaaS involves the optimization of resource allocation by considering network and computing resources as a unified whole. NaaS can include a virtual private network (VPN), bandwidth on demand, custom routing, multicast protocols, security firewall, intrusion detection and prevention, wide area networks (WAN) content monitoring and filtering, and antivirus.

Y .3500 distinguishes between cloud capabilities and cloud services. The tree capabilities are application, platform, and infrastructure corresponding to the basic service types of IaaS, PaaS, and IaaS. A cloud service category can include capabilities from one or more cloud capabilities types. Table I shows the relationship of the seven cloud services categories and the three cloud capabilities types [23].

TABLE I: RELATION OF CLOUD SERVICES AND CAPABILITIES

Cloud Service Categories	Cloud capabilities Types		
	Infrastructure	Platform	Application
Compute as a Service	X		
Communication as a Service		X	X
Data Storage as a service	X	X	X
Network as a service	X	X	
Infrastructure as a Service	X		
Platform as a Service		X	
Software a a Service			X

Finally, XaaS is the latest development in providing cloud services. The acronym has three interpretation, all of the them mean the same as follows: Everything as a Service, Anything as a Service, and X as a service, where X can present any possible cloud service option.

XaaS provides package of SaaS, PaaS, and IaaS together

so that the customer can do one stop shopping for any cloud service. In addition, can provides a wider range of IT department services including maintenance, patch, upgrade of verity of common application and services, single point of contact for resolving problems, and lower the cost and innovation is increased by a regular status genuine two-way real time exchange of information.

C) Essential Characteristics of Cloud Computing

National Institute of Standards and Technology (NIST) defined five characteristics of cloud computing (CC). Essential characteristics include:

1) Broad Network Access and Shared Infrastructure

CC provides access to thin or thick client platform (for example, mobile phone, laptops, and others) through standard mechanisms. As a part of doing business, cloud providers invest in and build the infrastructure necessary to offer software, platforms or infrastructure as a service to multiple consumers. Capabilities are available through shared networks with multitenant customers. Provider's resources are pooled to serve multiple consumers using multitenant model.

2) On-Demand Self-Service

On-demand self-service is the cloud customers will be able to purchase and use cloud services as and when the need arises. In some cases, cloud vendors provide an Application Programming Interface (API) that enables the consumer to program automatically (or automatically through a management application) consume a service.

3) Elastic and Scalable

From a consumer point of view, cloud computing ability to expand and reduce resources according to their specific service requirement. This service capability provides an elastic and scalable IT resource. Consumers pay for only the IT services they use. Although no IT service is infinitely scalable, the cloud service provider's ability to meet the consumer's IT needs creates the perception that the service is infinitely scalable and increases its value. Consumption- based pricing model: Providers charge the consumer per units consumed. For example, cloud vendors may charge for the service by the hour or gigabytes, stored per month.

4) Dynamic and Virtualized

The need to leverage the infrastructure across as many consumers as possible typically drives cloud vendors to create a more agile and efficient infrastructure that can move consumer workloads, lower overheads and increase service quality. Many vendors choose server virtualization to create this dynamic infrastructure.

5) Measured Services

CC automatically controls and optimizes resource use by leveraging a metering capacity at some level of abstraction appropriate to the type of service.

D) Cloud Deployment Models

An increasingly prominent trend in many organizations is to move IT operations totally to enterprise cloud computing. This section looks at the six most prominent deployment models for the CC.

1) Public Cloud

Public cloud infrastructure is made available to general public and is owned by organization selling cloud service and responsible for infrastructure, maintenance, control the data, and for operation of CC. It is an IT capability as a service that cloud providers offer to any consumer over the public Internet. Examples of the public cloud: Google App Engine, Microsoft Azure, and Amazon EC2. All major component are outside the enterprise firewall, located in a multitenant infrastructure and access the cloud through secure IP. The major advantage of public cloud is the cost. A customer pays only for the services and resources they used. The customer has no visibility at all and no control over where the computing infrastructure is hosted. The computing infrastructure is shared between all organizations.

2) Private Clouds

This cloud infrastructure is operated solely by internal IT of the organization; The organization may choose to manage the CC in house or contracted to a third party. The computing infrastructure may exist in premises or off premises. Private clouds are more expensive and more secure when compared to public clouds. Examples of private cloud are hospitals or universities. Private clouds are of two types, on premise private clouds and externally hosted private clouds.

3) Community Clouds

The community cloud shares the characteristics of both the public and private cloud. It has restricted access like the private and share its resources among many organizations like the public. A good example is the health care industry cloud. Infrastructure is a composition of two or more clouds (private and public). Community cloud involves sharing of computing infrastructure in between organizations of the same community. For example, all Government

organizations within the state of California may share computing infrastructure in the cloud to manage data related to citizens residing in California.

4) Hybrid Cloud

The hybrid cloud infrastructure is a composition of two or more cloud (public, private, or community). This is very attractive to smaller business for which the security is important and big concern to them. Hybrid cloud Organizations may host critical applications on private clouds and applications with relatively fewer security concerns on the public cloud. The usage of both private and public clouds together is called a hybrid cloud. A related term is Cloud Bursting. In Cloud bursting organization uses their own computing infrastructure for normal usage, but access the cloud for high/peak load requirements. This ensures that a sudden increase in computing requirement is handled gracefully.

5) Internal Cloud

A subset of a private cloud type, an internal cloud is an IT capability offered as a service by an IT organization to its business. For example, IT organizations building highly virtualized environments can become infrastructure providers to internal application developers. In a typical IT organization, application developers are required to work through the IT infrastructure operations team to procure and provision the development and production application platform (e.g., hardware, OS, and middleware) necessary to house a new application. In this model, the infrastructure team provides a cloud-like IT infrastructure to the application development team (or any other IT team) thereby allowing it to provision its own application platform.

6) External Cloud

An IT capability offered as a service to a business that is not hosted by its own IT firm. An external cloud can be public or private, but must be implemented by a third party.

TABLE 2. COMPARISON OF MAJOR THREE DEPLOYMENT MODELS

Delivery Model	Benefits	Risks	Best Fit
Public	• Costs • Time-to-Market • Elasticity • Self-Service • Simplicity	• Lack of Control • Security • Regulatory & Compliance • Data Migration • Application Development • Software Licensing • Vendor Lock-In • Limitations	• Applications and Data that can be publicly hosted • Applications that can be easily moved or ported to commodity virtual platforms
Private	• Control • Security • Compliance	• Scale • Management Tools • Charge-back • Adoption • ROI	• Applications and data that can not be hosted publicly for security or compliance reasons • Applications and data the require a high-level of control
Hybrid	• Flexibility • Security • Efficiencies	• Multiple Points of Failure • Same risks as public and private clouds	• When it is required to separate applications and data between private and public clouds • When public clouds can not accommodate requirements • When public cloud resources are only required temporarily and workloads can be migrated between clouds

III. CASE STUDIES RELATED TO SHARE FILE, SPLIT AND MERGE FILE WITH ENCRYPTION

The scheme proposed [1] has two main elements to take care of: the sender side and receiver side. Each one of them performs a specific task to ensure data security in cloud computing. The first one is the sender side, which has the ability to do several operations. The sender actually can shares a locked file with strong encryption and split the file before sending it. The shared file operation provides access control to the authenticate user to allow only genuine users to see the locked file and read it. Encryption can be used to protect data from granting access from cloud providers and attacker. Encrypted data will be saved in a receiver hard disk and uploaded to the cloud server. Finally, the sender can do a split operation to divide data into parts; where each part contains a jumbled text from the original text, and each part will be uploaded to cloud server after the split operation.

At the receiver side, the receiver can perform share file (unlock) to open a locked file which is locked by the sender. In addition, on this side the receiver can do the reverse operation of encryption to enable the user to download encrypted data from the cloud server and decrypt it to enable the user to understand the content of the file. The last operation is enabling the user to merge different parts to get the original text file.

In this section, two different practical cases will show the how to split the data at the sender side and merge text files at the receiver passing through different cloud with encrypting the data. We will present two cases using a simple text file of the word “RESEARCH”.

A) Case One; Spliting the File to two Parts

In this case, we will split the text file “RESEARCH” to only two parts. First part includes the even numbers “EERH” from the text file and the second part includes the odd numbers “RSAC” in the above text file as second part at the sender side. The two parts sent separately through the cloud and the receiver will merged them to recover the sent text file “RESEARCH” as shown in figure 3. Detail is as follows:

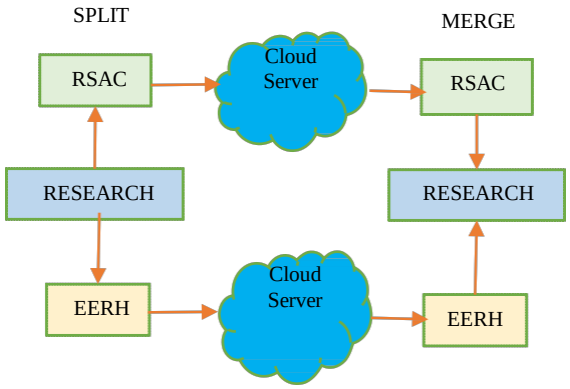

Fig. 3: Split and Merge Operation.

1) Sender Side

The sender can perform share file (lock), encryption and split operation as you can see in the above figure to part "RSAC" and "EERH" to be sent separately through the cloud. Each part meaning less by itself in the cloud, which represent the encryption of the data for more security as shown in Fig. 4.

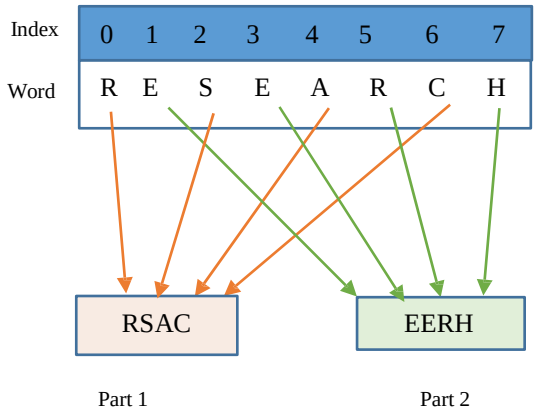

Fig. 4: Case one - Two Parts Split

2) Share File (Lock Operation)

Currently, there are many ways to make authentication. Some of them are biometric recognition and others use secret keys between the sender and receiver, where only the sender and receiver know this secret key and some of them use a token. The lock operation is done on either side to protect the communications between the two parties in order to prevent attackers from getting access to the data they are not authorized to see it. Executing this operation by generating a random number in Sender side and this number will be used to lock a file as password and send it to Receiver through the cloud or via email. The locked file will be done before uploading it to the cloud server.

3) Encryption Operation

In the proposed approach, data is encrypted before it uploaded to the server. This operation guarantees more protection to the data in a cloud server. The user selects to perform encrypt operation in the text file or image that is picked by the user. A text file or image files will be encrypted before uploading them to cloud server.

B) Case Two: Spliting The File to Four Parts

In this case, the text file will be split to four parts as shown the figure 5, where the selection splits to four, we did it in two stages. First divide the text to two halves then take the first character from the first half with the first character from the second half, which is the first part, the second part will contain the second characters from the first half and second half. The third and fourth parts are likewise. Split file operation performs also before uploading file.

These parts are done in user hard disk at the sender side. Similar to the above case, all four parts go through the cloud then will be merged at receiver side. The encryption in this case is more secure than the first case, which indicate that it is harder to recall and the four parts to recover the text file "RESEARCH".

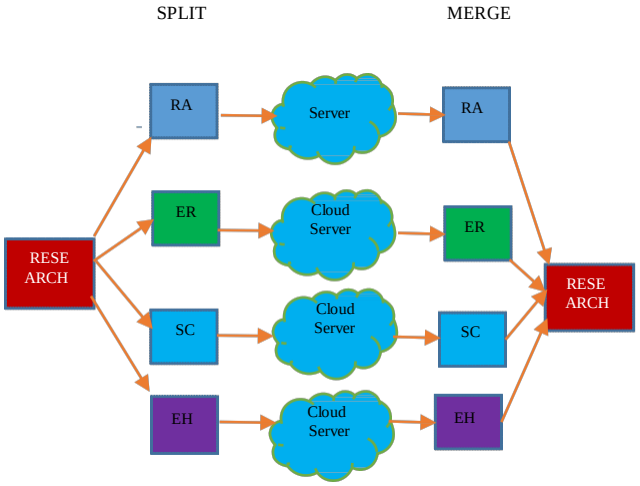

Fig. 5: Splitting and Merging into Four Parts

In both cases, we chose this way rather than encrypt data in the same cloud to ensure the security of data in cloud server and be protected from the cloud owners and hackers. The encryption algorithm proposed is AES algorithm, which is by far the best algorithm when compared to *Triple DES*, *RSA*, *Blowfish*, and *Twofish*. AES Algorithm is an acronym for Advanced Encryption Standard. The structure of AES has four basic steps used:

1. Byte substitution; 2. Shift rows

3. Mix Columns; 4. Add Round Key

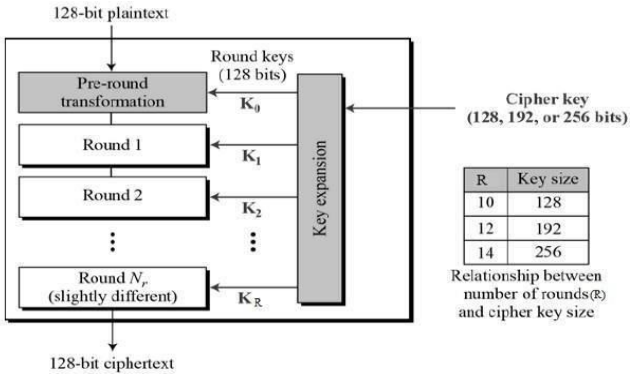

Fig. 6: AES Algorithm [22]

The 'Honey Encryption' is an upcoming encryption scheme that might prove to be better when it comes to authentication and data security. It is an encryption technique beats attackers by presenting them with fake data. When a hacker tries to hack into the network, instead of informing the unsuccessful hacker that they have been

denied access, the system shows them they are successful and give them some bogus data. One limitation to the technique is that you need to know what a genuine password or encryption key would look like for the relevant site or service (and the encryption method it uses) otherwise hackers will be able to easily tell they have been given bogus data.

C) Case Three; General case- Spliting the File to n Parts

The user can split required file into parts. Each part contains a fraction of the original file. These parts are unreadable. Because the procedure used in the split operation depends on dividing content in an incomprehensive way. The user can select a number of parts such as two, four, …n. Fig. 7 shows the general case and can be summarized as:

D) Receiver Side

As we can see, the receiver can perform share file, decryption and merge operation and how the action will be taken by the receiver to complete this operation.

1) Share File (Unlock Operation)

We run share file in the receiver side to enable Receiver to access locked file, which is locked by Sender. This operation allows only authorized users to access the file by entering random number generated by the sender.

2) Decryption Operation

Decryption is a reverse operation of encryption. To enable the receiver to understand the content of encrypted text file. We can apply it on any form of data. However, in our implemented system, we did it only for text and image files.

3) Merge Operation

In this operation, we enable the user to merge different parts that are generated by a split operation to get original file. These parts will be store on a cloud server. Therefore, when the user wants to merge them, they will need to download several parts from cloud server before performing the merge operation. The user will be able to know how many parts will be selected to download depending on the name of the part, as we mentioned it in the previous split operation.

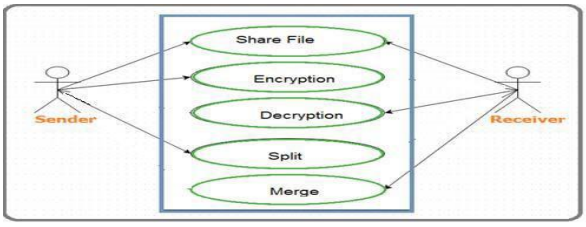

Fig. 7: Use case of the system [1]

IV. Security challenges Analysis concerning Cloud Computing and some solution

Looking at the benefits cloud provides, there are privacy and security concerns too that need attention. Data is shared over the Internet and is stored in remote locations serving multiple customers at the same time. There are Vulnerable security breaches either accidental or deliberate that require immediate attention. The security problems could be caused due to loss of control over the data, lack of trust on the mechanism used to store data or from multi-tenancy which is why the cloud is so popular.

The data, applications, and resources are taken care of by the provider. Therefore, identity management, security policies, access control etc. are also managed by the cloud provider. As the very physical infrastructure is shared with multiple users, the chances of the security threat from within is also a great threat if there are no proper security measures in place.

According to the research conducted cloud computing security challenges fall into four broad categories:

- Security Provided to Data
- Authenticating Users
- Data Breach Contingency Planning
- Technical Failures
- Cloud Infrastructure Security

A) Security Provided to Data

Implementing a cloud computing strategy means giving the critical data to a third party, so ensuring the data remains secure both on storage media as well as when in transit is important. Data needs to be encrypted every time, with clearly defined roles when it comes to who will be handling the encryption key.

Solution to the Problem: Enterprises should ask providers to provide access paths to only the physical servers that must have access to maintain the desired functionality. In most cases, the only way to truly ensure confidentiality of encrypted data that resides on a cloud provider's storage servers are for the client to own and manage the data encryption keys. When it comes to public, private, and hybrid cloud solutions, the thought of compromised information creates great risk. Organizations expect cloud providers to manage the infrastructure but feel uneasy about sharing the critical data.

B) Authenticating Users

Identity and Access Management has focused on the attributes of a person's identity. Firms still use User ID and passwords as the only form of authentication. Traditional forms of multi-factor authentication were a hindrance in the way of massive growth in devices connected to the internet and online activity and are a total failure when it comes to meet the needs of scalability, ease of use, and mass-deployment that the online-connected world requires.

Solution to the Problem: Cloud service environments require tight integration with enterprise policies around individual and group access, authentication and auditing. Data stored in the cloud needs to be accessible only by those authorized to do so, making it difficult to both restrict and monitor who will be accessing the company's data. In order to ensure the integrity of user identity, companies need to be able to view data access logs and audit trails to make sure that only authorized users are having access to the data. These access logs and audit trails need to be secured and maintained for as long as the company or legal purposes need them to. As with all cloud computing security challenges, it's the full responsibility of the customer to ensure that the cloud provider has taken all necessary security measures to protect their data and the access to that data.

C) Data Breach Contingency Planning

In the event of an unwanted disaster, the focus is on getting the business back on track. Whether the disaster is natural or human induced, it's all about recovering business operations as fast as possible. Information security is usually not part of the contingency plans. Businesses should overlook data protection provisions in their recovery post-disaster or plans to continue business.

Solution to the Problem: With the cloud serving as a single centralized repository for a company's critical data, the risks of having that data compromised due to a data breach or temporarily made unavailable due to a natural disaster are real concerns. Much of the liability for anything happening to the data in a cloud ultimately rests with the company whose critical operations depend on that data, although liability should be negotiated in a contract with the services provider prior to any commitment. An intense security assessment from a neutral third-party is strongly recommended as well.

Companies need to know how their data is being secured and what measures are taken to ensure the integrity and availability of that data in case the unexpected occurs.

D) Technical Failures

Network downtime in the Amazon Simple Storage Service (S3). In early February 2008, the entire datacenters' network froze up, leaving the majority of users to the cloud service denied access for around four hours automated set of processes should have kick-started the cloud service again, but this system also failed. This isn't the first time Amazon has had difficulties with its cloud storage system, when just over a year ago the entire service suffered multiple faults which caused many to reconsider the offerings of the technology giant.

Google's cloud services and applications suffer a series of technical difficulties. Over the course of the last year, Google had been hit by numerous different outages, which caused a ruckus in the online social media scene. Although some of the outages had only lasted approximately 45 minutes, the simple fact of an essential service to many had been partly offline caused enough disruption for many to be angry about. Gmail, a rival email service to Microsoft's Windows Live Hotmail and Yahoo Mail, also suffered downtime a month later, due to a technical error which caused an automated error message to be displayed. Because of the nature of these two products, there was never any 100% downtime; many different aspects of the services worked just as well as they did before the technical issue, but some areas of service were affected.

E) Cloud Infrastructure Security

1) Network Level

Network level infrastructure security need to be designed based on public clouds and private clouds. Generally, in private clouds there are no new attacks, vulnerabilities or changes in risk that information security personnel need to consider. Although organization's IT architecture may be altered along with the implementation of a private cloud, your current network topology will probably not change significantly. The security considerations you have today also apply to a private cloud infrastructure too. However, if you choose to use public cloud services, changing security requirements will require changes in your network topology, you must address how your existing topology interacts with your cloud provider's network structure. There are four significant risk factors in this use case:

- Ensuring confidentiality and integrity of your organization's data passing to and from your public cloud provider.
- Ensuring proper access control (authentication, authorization, and auditing) to whatever resources you are using at your public cloud provider.
- Ensuring the availability of the Internet resources in a public cloud that is being used or have been assigned to your organization by your public cloud provider.
- Replacing the established model of network zones and tiers with domains.

2) The Host Level

In order to review host security and evaluate risk (risk assessment), you should consider the context of cloud services delivery model (SaaS, PaaS, and IaaS) and deployment models (public, private, and hybrid). Although there are no known threats to hosts that are specific to cloud computing, some virtualization security threats- such as VM escape, system configuration drift, and insider threats caused due to weak access control to the carry into the public cloud computing environment. The dynamic nature or the elasticity of cloud computing can introduce new operational challenges from security management perspective.

i) SaaS and PaaS Host Security

Customers in the cloud do not have control to host security and the responsibility lies with the Cloud Service Provider (CSP) to secure the hosts. The following points need to be considered to get the assurance from the CSP on the security hygiene of its hosts. Ask the vendor to share information under Non-Disclosure Agreement (NDA) or through a control assessment framework such as Sys Trust or ISO 27002. The CSP has to ensure that appropriate preventive and detective controls are in place through third party assessment or ISO 27002 type assessment framework.

ii) IaaS Host Security

In IaaS customers are primarily responsible for securing the host provisioned in the cloud. The host securities primarily considered in IaaS are as follows:

Virtualization software security: The virtualization software sits on top of the hardware; the customer will not have visibility or access to this software. CSP manages the virtualization software. IaaS services use hypervisor technology such as VMware ESX, Xen, Oracle VM, and Microsoft's Hyper-V. The hypervisors support a variety of guest OSs, including Microsoft Windows, and Sun Open Solaris. It is very critical to protect the hypervisors from unauthorized access. The CSP should implement necessary security controls, which includes restricting physical and logical access to the hypervisor and other forms of employed virtualization layers. IaaS customers should have clear visibility and understanding on those security controls, technology and process that are enforced by the CSP to protect the hypervisor. This will help customers understand the compliance and gaps with reference to host security standards, policies, and regulatory compliance.

Virtual Server Security: As customers have full access to the virtualized guest VMs, they are responsible for securing and managing the security of the guest VM. The virtual servers may be accessible to anyone over the internet, so stringent network access mitigation steps should be taken to restrict access to virtual servers. CSP has a web interface API to perform management functions like provisioning, decommissioning, and replication of virtual servers on IaaS platform. Hence securing the cloud management API is also important as it adds another layer of attack in public cloud. The host securities threats that may occur in the public IaaS environment are listed below:

a. Stealing SSH keys.
b. Attacking unpatched, vulnerable services on standard ports like ftp, NetBIOS, SSH.
c. Account hijacking.
d. Attacking systems those are not properly secured by host firewalls.
e. Deploying Trojan embedded in the VM.

The recommendations to secure virtual servers are as follows:

a. Harden your image and use a standard hardened image for the guest OS in a public cloud.
b. Keep track of the inventory of VM images and OS versions.
c. Protect the integrity of the hardened image from unauthorized hosts.
d. Safeguard your private keys required to access hosts in the public cloud.
e. Do not implement authentication credentials in virtualized images except for a key to decrypt the file system key.
f. Do not use password-based authentication for shell access.
g. Mandatory passwords for role-based access.
h. Run host firewall and open only necessary ports.
i. Run only required services and turn off the unused services.
j. Install HIDS/HIPS.
k. Enable system auditing and event logging and capture the logs in a centralized log server.
l. Institute a process and blue print for patching the images.
m. Review logs periodically.

V. CONCLUSION AND FUTURE WORK

In this paper, we have analyzed the major security challenges cloud faces. They are as follows:

A) Security provided to Data

The data has to secure if you are sending it to a third party. The data has to be insured while it's in transit or it is stored on a device. In order to provide security to the data the enterprises should ask the providers to provide access paths to only the physical servers.
The major areas where data security might be at risk and need to be mitigated are as follows:

1. Cloud data–in-transit: The protocol used to transfer data across clouds provides confidentiality and integrity (like https, sftpand so on.) that is the data transfer happens in encrypted channel
2. Cloud data-at-rest: It is strongly recommended to encrypt the data-at-rest in IaaS, PaaS, and SaaS cloud for simple storage only
3. Processing of data: Data must be encrypted when it is processed in the cloud, which means that it allows the data to be processed without decryption.
4. Data lineage: Following the path data (mapping application data flows or data path visualization) is

known as data lineage that is exactly when and where the data was specifically located within the cloud and maintained for auditor's assurance.

5. Data provenance: Data Provenance means that not only data has integrity, but it is computationally accurate also.
6. Data remanence: Data remanence is the residual representation of data that has been in some way nominally erased or removed, the risk posed by this in cloud is that an organization's data can be inadvertently exposed to an unauthorized party.

B) Authenticating Users

To make sure that the right people get the right level of access, is a great task. To make sure that right people are accessing your data you need to regularly check the access logs and audit trails. These access logs and audit trails needs to be secured and preserved as long the firm needs them for legal purposes.

C) Data Breach Contingency Planning

In case of some unexpected event the focus is generally to bring the business back on track. The risk of data being compromised is high. Who is liable if data loss is caused due to natural calamity? There should be a strict security assessment from a neutral third party and negotiation contract should be well established.

D) Cloud: Infrastructure Security

If we talk about the network level of security, we must take care of four possible risk factor. Confidentiality and integrity of data in transit, ensuring proper access control, Ensuring that resources in the public cloud are available all the time and finally replacing the model of network zone with tiers and domains.

In section 4, we see a process to secure data over cloud. The. paper talked about Encrypting the data and sending over cloud and on the receiving end the data was being decrypted. The encryption algorithm used was AES algorithm that is by far the best encryption technique but if 'Honey Encryption' technique would serve more fruitful. Honey Encryption technique provides fake set of data to the attacker when they try to hack into the network.

In the future, incorporating the 'Honey Encryption' will be adding extra security to data as well as the network and cloud.

A revolutionary style of computing, cloud computing is emerging from evolutionary change. Cloud computing sets the stage for a new approach to IT that enables individuals and businesses to choose how they'll acquire or deliver IT services, with less emphasis on the constraints of traditional software and hardware licensing models. The emergence of cloud and other Web platforms enables composite applications and composite business and has the potential to have a profound impact on IT and business. IT is catching up with the rest of the Internet by extending the IT topology beyond the traditional data center walls. Although cloud computing is transforming traditional IT, it is still immature. Like any technology, creating competitive advantage through cloud computing is contingent on comprehension: knowing what the cloud is, the strengths and weaknesses, potential risks, and the usage and pricing models. The best organizations will use cloud computing's unique - elastic and scalable - business model to streamline IT operations, offload lower valued IT processes and focus on driving core business value. Higher-value, business-oriented services will take longer to reach the cloud as they require a high degree of trust between providers and customers; they also require a degree of security and robustness that is just now becoming viable for Internet-based computing.

REFERENCES

[1] M. A. Aldakheel, S. M. M. Rahman, R. Al-Zahrani, and E. El-Qawasmeh, "Investigation of security challenges and a novel security mechanism for cloud computing environment," in Web Applications and Networking (WSWAN), IEEE 2nd World Symposium pp. 1-6, March 2015.

[2] Z. Tari, X. Yi, U. S. Premarathne, P. Bertok, and I. Khalil, "Security and Privacy in Cloud Computing: Vision, Trends, and Challenges," IEEE Cloud Computing, 2(2), pp. 30-38. 2015.

[3] S. Srivastava and P. S. Sudhish, "Security in cloud computing systems: A review of challenges and solutions for security in distributed computing environments," IEEE-In Systems Conference (NSC), 39th National pp. 1-5, December 2015.

[4] W. Kong, Y. Lei, and J. Ma, J. (2016, "Data Security and Privacy Information Challenges in Cloud Computing,", IEEE International Conference on an Intelligent Networking and Collaborative Systems (INCoS) pp. 512-514, October 2016.

V. Jain and V. Sharma, "Surveying and analyzing security challenges and privacy in cloud computing," International Journal of Computer Science and Information Technology & Security, vol. 3(5), pp. 316-321. 2013.

[6] X. D. Zhu, H. Li, F. H. Li, "Privacy-preserving logistic regression outsourcing in cloud computing," International Journal of Grid and Utility Computing, vol. 4(2-3), pp. 144-150, 2013.

[7] P. Xiao and N. Han, "A novel power-conscious scheduling algorithm for data-intensive precedence-constrained applications in cloud Environments," International Journal of High Performance Computing and Networking, vol. 7, pp. 299-306, 2014.

[8] S. Naser, S. Kamil, and N. Thomas, "A case study in inspecting the cost of security in cloud computing," Electronic Notes in Theoretical Computer Science, vol. 318(11), pp. 179-196, 2015.

[9] Cloud Security Alliance, "Top threats to cloud computing," v1.0. http:// cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, 2010.

[10] A. Kumar, M.Namdevand, and S. Shakti, "Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment," CSI-Sixth International Conference on Software Engineering (CONSEG), 2012.

[11] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control," CCSW-Chicago, Illinois, USA. ACM 978-1-60558-784-4, November 13, 2009.

[12] R.Shaikh and M. Sasikumar."Security Issues in Cloud Computing: A survey," International Journal of Computer Applications, 2012.

[13] T. Erl, R. Puttini,and Z. Mahmood, “Cloud Computing: Concepts, Technology & Architecture,” Prentice Hall, 2014.

[14] G. Shroff, “Enterprise Cloud Computing: Technology, Architecture, Applications by,” Cambridge University Press, Online publication, 2010.

[15] V. Rao and K. Selvamani, “Data Security Challenges and Its Solutions in Cloud Computing. Procedia Computer Science,” ELSEVIER Journal, Vol. 48, Pages 204-209, 2015.

[16] A. Gawanmeh and A. Alomari, “Challenges in Formal Methods for Testing and Verification of Cloud Computing Systems,” Scalable Computing: Practice and Experience 16 (3): 321-332 (2015), September 2015.

[17] https://en.wikipedia.org/wiki/Cloud_computing.

[18] https://railskey.wordpress.com/tag/iaas/

[19] http://wptidbits.com/techies/cloud-computing-solutions-iaas-paas-saas

[20] https://www.linkedin.com/pulse/understanding-cloud-spi-model-ankur-minotra

[21] http://blog.bounceweb.com/iaas-paas-and-saas-cloud-computing-with-choice/

[22]https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

[23] W. Stallings, Foundation of Modern Networking SDN, NFV, QoE, IoT, and Cloud, Addison Wesly, 2016.

[24] ITU-T Y.3500, Cloud Computing- Overview and Vocabiulary, August, 2014.