International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Data Breaches in Cloud Computing and its Privacy and Security Aspects

M. R. A. Jamadar[1]*, Akanksha A. Gawande*[2]

[1]*Assistant Professor, Department of Information Technology, AISSMS's Institute of Information Technology, Pune-411001, INDIA*
[2]*TE. BE (Information Technology), AISSMS's Institute of Information Technology, Pune-411001, INDIA*

ABSTRACT

The emerging cloud market introduces a multitude of cloud service providers, making it difficult for consumers to select providers who are likely to be a low risk from a security perspective. Recently, significant emphasis has arisen on the need to specify Service Level Agreements that address security concerns of consumers. It has been found that such SecSLAs are not consistent among providers, even though they offer services with similar functionality. However, measuring security service levels and the associated risk plays an important role when choosing a cloud provider. Data breaches have been identified as a high priority threat influencing the adoption of cloud computing. The proposed work is to prevent data breaching threat by way of providing user authentication through one-time password system and challenge response, risk assessment to identify and prevent possible risks, encryption using enhanced elliptic curve cryptography where a cryptographically secure random number generation is used to make the number unpredictable, data integrity, and key management.

1. Introduction to Data Breach in Cloud Computing and its Privacy and Security aspects

1.1 Introduction

Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in either privately owned, or third-party data centers that may be located far from the user–ranging in distance from across a city to across the world. Despite the advantages and rapid growth of cloud computing, existing cloud environments are still not seen to be sufficiently trustworthy by consumers. This framework enables consumers to specify which security parameters are most significant for them, enabling a subjective view to be formed of different cloud providers. Security remains an important concern for many users, particularly prevention of data breaches at the cloud provider and the ability of a provider to interrogate data stored at their systems. The proposed work is to prevent data breaching threat.

1.2 Motivation

i. Basically Data Breach is hacking of information from Cloud Computing.

ii. Data Breach might be some issue in cloud computing which can be solved using some Privacy and Security aspects.

iii. It's a interesting subject

iv. Privacy and Security aspects ideas can help us to overcome on Data Breaches in Cloud Computing.

v. An Engineering Student should have the basic knowledge about the Data Breaches in Cloud Computing and privacy and security aspects.

1.3 Aim and Objective of the work

i. The aim of this project is to what is Data Breaches in Cloud Computing and identify various Privacy and Security ways .

ii. To increase the trust of user on Cloud Computing by providing information that how they can protect their data by using privacy.

Project objectives:

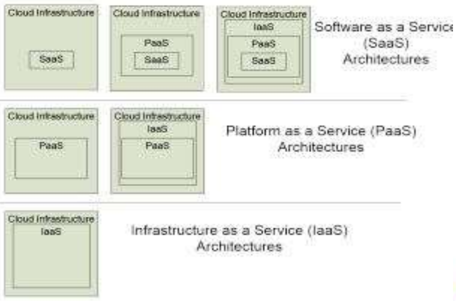
i. Assist in preventing data or information from being hacked .

ii. may undermine user confidence in cloud computing by giving them tools for avoiding data breaches.

iii. Also this knowledge will helpful for engineering students or other users.

2. In Brief

- **CLOUD COMPUTING:** Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in either privately owned, or third-party data centers that may be located far from the user–ranging in distance from across a city to across the world. There are three Deployment models in Cloud Computing 1. **SaaS (Software as a Service) 2. Paas(Platform as a Service) 3.Iaas(Infrastructure as a Service)**


Cloud Infrastructure
SaaS
PaaS
IaaS
Software as a Service (SaaS) Architectures
Platform as a Service (PaaS) Architectures
Infrastructure as a Service (IaaS) Architectures

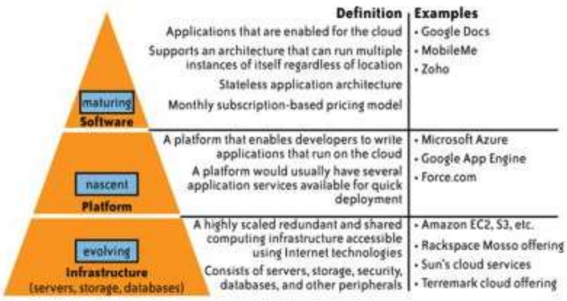

Definition
Examples
Applications that are enabled for the cloud
Supports an architecture that can run multiple instances of itself regardless of location
Stateless application architecture
Monthly subscription-based pricing model
• Google Docs
• MobileMe
• Zoho
maturing
Software
A platform that enables developers to write applications that run on the cloud
A platform would usually have several application services available for quick deployment
• Microsoft Azure
• Google App Engine
• Force.com
nascent
Platform
A highly scaled redundant and shared computing infrastructure accessible using Internet technologies
Consists of servers, storage, security, databases, and other peripherals
• Amazon EC2, S3, etc.
• Rackspace Mosso offering
• Sun's cloud services
• Terremark cloud offering
evolving
Infrastructure
(servers, storage, databases)

Figure 2.1**:** Service Models of Cloud Computing

Figure 2.2: Examples of Service models of Cloud Computing

- **Data Breach:** A data breach is the intentional or unintentional release of secure or private/confidential information to an untrusted environment. A data breach is an incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner. Victims of data breaches are usually large companies or organizations, and the data stolen may typically be sensitive, proprietary or confidential in nature (such as credit card numbers, customer data, trade secrets or matters of national security). Damage created by such incidents often presents itself as loss to the target company's reputation with their customer, due to a perceived betrayal of trust. The damage may also involve the company's finances as well as that of their customers' should financial records be part of the information stolen. There are two types of Data Breach 1.Active Data Breach 2. Passive Data Breach

2.1 Causes of Data Breach:

1. Weak and Stolen Credentials, a. k. a Passwords Hacking attacks may will be the most common cause of data breach but it is often a weak or lost Passwords that is the vulnerability that is being exploited by the opportunist hacker .Stats show that 4 in 5 breaches classified as a "hack" in 201 were in part caused by weak or lost(stolen)passwords!

2. Back Doors, Application Vulnerabilities Hackers targets the software applications which are poorly written or network systems which are poorly designed or implemented, they leave holes that they can crawl straight through to get directly at your data.

3. Malware The use of both direct and in-direct Malware is on the rise. Malware is by definition , malicious software; software loaded without intention that opens up access for a hacker to exploit a system and potentially other connected systems.

4. Social Engineering users may accidentally share work-critical information, details and files with friends either through negligent file-handling practices or idle conversation.

5. Physical Attacks Company devices that may be lost or stolen by employees who bring them home.

- **Effects on User:** Understandably, consumers are concerned about the security of their personal information and have lost confidence in organizations' data security standards. The majority of consumers do not believe that organizations that they interact and transact with are looking out for their best interests. And on top of that, more than twice as many respondents believe that the onus of protecting and securing customer data falls on the company versus the consumer.

- **Effects on Organization:**

  1. Reputation damage

  2. Financial loss

  3. Legal consequences:

a. DPA penalties and the ICO

b. The Data Protection Act 1998 (DPA) is enforced by the Information Commissioner's Office (ICO , which has several options when it finds an organization to be in breach of the act: Monetary penalty notices, Prosecutions, Undertaking, Enforcement notices, Audit.

A. Possible Solutions to avoid Data Breaches

i. Minimize Lack of Trust: It involves Policy Monitoring and Certification

ii. Minimizing Loss of Control: It can be avoid by using Monitoring and Identity Management(IDM).

iii. Minimize Multitenancy: In multi-tenancy server runs a signal instance of the service and serves multiple tenants i. e. clients. These tenants have specific permissions while communicating with the provider. Sometimes the provider does not isolate the user's workspace from each other. So there is chance of data breach. We can't really force the provider to accept less tenants. But we can try to increase isolation between the tenants and increase trust in tenants.

iv. Blockchain: Blockchain can be used as a security purpose in data breach dimension of cloud computing several current studies apply blockchain technology to cloud environment for data protection .Block chain cryptographically links blocks, and the chain continues to grow. A block contains the cryptographic hash, timestamp, and transaction data of previous blocks. Modifications cannot be performed on the bloclchain, and it effectively records transactions between stakeholders. Here we look at a study on blockchain technology in data movement, data management, and the Cloud Storage.

v. Elliptic curve cryptography: For elliptic-curve based protocols, it is assumed that finding the discrete logarithm of a random, elliptic curve element with respect to a publically known base point is infeasible. The size of the elliptic curve determines the difficulty of the problem. The primary benefit promised by ECC is a smaller key size, reducing storage and transmission requirements—i.e. that an elliptic curve group could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key---e.g, a256-bit ECC public key should comparable security to a 3072-bit RSA public key. For current cryptographic purpose, an elliptic curve is a plane curve which consists of the points satisfying the equation y2=x3 + ax + b.

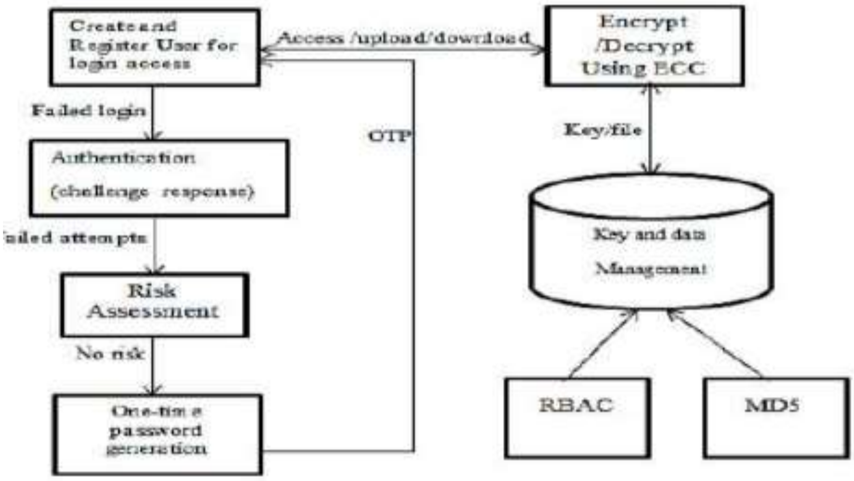
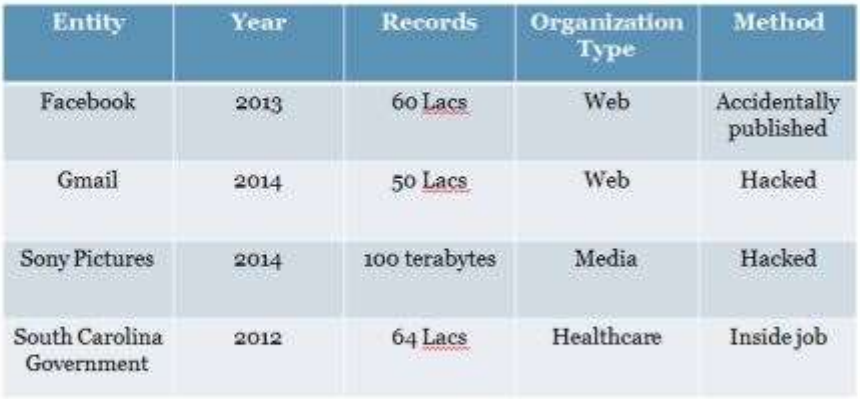

Create and Register User for login access
Access /upload/download
Encrypt /Decrypt Using ECC
Failed login
OTP
Key/file
Authentication (challenge response)
ailed attempts
Key and data Management
Risk Assessment
No risk
One-time password generation
RBAC
MD5

Figure 2.3: Secure System to prevent Data Breach

2.2 Examples

Facebook blamed the data leaks, which began in 2012, on a technical glitch in its massive archive of contact information collected from its 1.1 billion users worldwide. As a result of the glitch, Facebook users who downloaded contact data for their list of friends obtained additional information that they were not supposed to have.



Entity	Year	Records	Organization Type	Method
Facebook	2013	60 Lacs	Web	Accidentally published
Gmail	2014	50 Lacs	Web	Hacked
Sony Pictures	2014	100 terabytes	Media	Hacked
South Carolina Government	2012	64 Lacs	Healthcare	Inside job

Figure 2.4: Examples of Data Breach

2.3 Mechanism

1. - Research- The cybercriminal, having picked his target, looks for weaknesses that he can exploit: the target's employees, its systems, or its networks. This entails long hours of research on the cybercriminal's part, and may involve stalking employees' social networking profiles to finding what sort of infrastructure the company has.

2. – Attack: Having scoped out his target's weaknesses, the cybercriminal makes initial contact through either a network-based attack or through a social attack. In a network attack, the cyber-criminal uses the weaknesses in the target's infrastructure to get into its network. These weaknesses may include (but are not limited to) SQL injection, vulnerability exploitation, and/or session hijacking. In a social attack, the cybercriminal uses social engineering in order to infiltrate the target's network. This may involve a maliciously-crafted email to one of the employees, tailor-made to catch that specific employee's attention. The mail could be a phishing mail, where the reader is fooled into supplying personal information to the sender, or one that comes with attached malware set to execute once accessed. Either attack, if successful, allows the cybercriminal to:

3 . -Exfiltration Once inside the network, the cybercriminal is free to extract the data he needs from the company's infrastructure and transmit it back to himself. This data may be used for either blackmail or black propaganda. It may also result in the cybercriminal having enough data for a more damaging attack on the infrastructure as well. Data breaches may involve 1.financial information 2.Personal Health Information (PHI) 3.Personally Identifiable Information (PII) 4.trade secrets of corporations unstructured data - files, documents, and sensitive information

2.4 Methodology

In methodology we can protect the data breach in several ways Blockchain is one of the better way to avoid the data breach. A blockchain cloud storage solution divides up a user's data into manageable portions. Then it distributes the additional layer of protection over the network. Blockchain technologies like the hashing algorithm, public/private key encryption, and transaction ledgers make this possible. Also by using encryption, decryption and one time password Risk assessment etc we can secure data breaches .

2.5 Enhancement

i. Cloud is massive concentration of resources. Hence, it is a massive concentration of risk - expected loss from a single breach can be significantly larger concentration of "users" represents a concentration of threat.

ii. The cloud acts as a big black box, nothing inside the cloud is visible to the clients Clients have no idea or control over what happens inside a cloud.

iii. We can avoid or control data breaches by using several ways..

iv. Therefore, it should be simple to use and comprehend/ understand.

3. Conclusion

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction .Cloud is massive concentration of resources. Hence, it is a massive concentration of risk. Also concentration of users represents a concentration of threats. The cloud acts as a big black box, nothing inside the cloud is visible to the clients. Clients have no idea or control over what happens inside a cloud. This may lead to explosion of large amount of data to untrusted environment by intentional or unintentional means (i.e. a data breach). Loss from a single breach can be significantly larger and loss depends on sensitivity of data. Data breach can be avoided by developing more secure system by minimizing Loss of Control, Multi-tenancy, etc. Also we can use encryption and description by Elliptic Curve Cryptography. Elliptic curve group could provide the same level of security afforded by an RSA-based system but with a smaller key size, reducing storage and transmission requirements. Accidental data breaches can't be avoided but must be controlled in time to minimize the consequences. These consequences are user level as well as organizational level.

It has been seen that ECC has considerably smaller key size as compared to RSA. Thus, there is a computational advantage to using ECC with a shorter key length than a comparably secure RSA. The results show that ECC is efficient in terms of the size of Data files and Encrypted files. The above information is useful for wireless communication due to low data rate transmission and for constrained devices because of low power requirements. The ECC API is used in the security layer to automatically encrypt/decrypt all data that flows to or from the application layer. The security layer in turn will depend on the API to carry out its task. And Cloud Computing can also be replace by Blockchain technology in future.

References

[1] Yogachandran R., Muttukrishnan, Omer F. Rana, Malik S. Awan, Pete Burnap, and Sajal K. Das, "Assessing Data Breach Risk in Cloud Systems," 2015 IEEE 7th International Conference on Cloud Computing Technology and Science

[2] Nina Pearl Doe, Suganya V, ”Secure Service to prevent Data Breaches in Cloud,” 2014 International Conference on Computer Communication and Informatics (ICCCI -2014)

[3] Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy, ”Cloud Computing: Security Issues and Research Challenges,” IRACST - International Journal of Computer Science and Information Technology Security (IJCSITS) Vol. 1, No. 2, December 2011J

[4] Osama Harfoushi, Bader Alfawwaz, Nazeeh A. Ghatasheh, Ruba Obiedat, Muaad M. Abu-Faraj, Hossam Faris, ”Data Security Issues and Challenges in Cloud Computing: A Conceptual Analysis and Review,” Communications and Network, 2014, 6, 15-21 Published Online February 2014.

[5] B. Zhao, P. Fan and M. Ni, “Mchain: A blockchain-based vm measurements secure storage approach in iaas cloud with enhanced integrity and controllability. IEEE Access, vol. 6, pp. 43758–43769, 2018.

[6] Security and Privacy Aspects of Cloud Computing: A Smart Campus Case Study Sajid Habib Gill1 , Mirza Abdur Razzaq1 , Muneer Ahmad2 , Fahad M. Almansour3 , Ikram Ul Haq4 , NZ Jhanjhi5,*, Malik Zaib Alam6 and Mehedi Masu IASC, 2022