ANALYSIS OF CLOUD DATA BREACHES AND ITS MANAGEMENT

Ranjan Kumar
Amity Institute of
Information Technology
Amity University
Noida, India
ranjan.kumar@s.amity.edu

Neetu Mittal
Amity Institute of
Information Technology
Amity University
Noida, India
nmittal1@amity.edu

Abstract— **Cloud data breaches are becoming increasingly common and can have major consequences for individuals, businesses, and governments. Financial losses, reputational harm, and legal obligations can all result from cloud data breaches. As a result, effective management of cloud data breaches is critical for organizations to mitigate these risks and protect their data. The research paper aims to examine the major factors that contribute to cloud data breaches and discuss strategies for their management. In the first section the technical factors contributing to cloud data breaches. The second section examines how cloud data breaches have been discussed. The third section w focuses on the management of cloud data breaches. Further, the conclusion summarized the key findings and provides recommendations for organizations looking to secure their cloud data. The research paper comprehensively analyzed the major factors that contribute to cloud data breaches and discusses strategies for their management. This research will help organizations to better understand the risks associated with cloud data and how to protect their critical information.**

Keywords – Cloud Computing, Security, Data Breaches

I. INTRODUCTION

A cloud data breach occurs when an unauthorized party has access to private or sensitive data kept on cloud computing systems. Cloud computing stores manage and process data online via remote servers. It has grown in popularity due to its practicality and affordability. Data is no longer kept on local servers, but this also necessitates the implementation of security measures to guard against data breaches. Weak passwords, improperly configured access controls, unpatched vulnerabilities, phishing attacks, and insider threats are just a few of the causes of cloud data breaches. After gaining access to the cloud system, an attacker could be able to steal or erase confidential information, put ransomware or malware in place, or utilize the cloud system as a jumping-off point for other assaults. A cloud data breach may have serious repercussions, including monetary losses, reputational harm, legal obligations, and regulatory fines. Moreover, it may seriously undermine both consumer confidence and corporate operations. As a result, it is critical for enterprises to have strong security measures and to regularly audit their cloud systems for risks and vulnerabilities. Ultimately, a cloud data breach may have large and pervasive consequences. Strong security measures must be implemented by enterprises to guard against data breaches, and they must have a strategy in place for an effective response in the case of a breach. Many nations have passed legislation requiring businesses to follow security standards to protect sensitive data. If there are data breaches within corporations, non-compliance with these standards may result in hefty penalties as well as civil and criminal actions. Companies must also cover the expenses of data breach investigations and notify consumers who may have been harmed. Several firms use expert legal services to ensure they are ready to manage violations. In cases when customer data is stolen and used maliciously, corporations can also employ credit monitoring services to help. Data breaches may also have unintended consequences, such as harming the company's brand and making it difficult to continue operating the firm. If clients leave the business, it could be necessary to hire new users, which might be expensive. Data that is sent to the cloud is carefully safeguarded thanks to the efforts of cloud service providers. Putting in place a robust security procedure is a good method to prevent data breaches.[1]

II. LITERATURE SURVEY

Cloud data breaches have become a major concern for organizations throughout the world, and knowing the primary variables that contribute to them is essential to effective management. A cloud data breach happens when an unauthorized person has access to confidential information that is kept there, perhaps leading to data loss, identity theft, financial loss, and reputational harm to the company. This study of literature attempts to investigate the key causes of cloud data breaches and the most effective management techniques. Insider risks, misconfigurations, external assaults, and insufficient security procedures all contribute to cloud data breaches. Insiders have access to sensitive data and can trigger security issues either purposefully or accidentally. Incorrect configuration of cloud services leads to misconfigurations, whereas hostile actors that attack cloud infrastructure or applications carry out external attacks. Poor security controls can lead to breaches; data encryption and access control are crucial preventative measures. Frequent audits and monitoring and an incident response strategy may also assist firms in managing security problems.[2]

III. CLOUD DATA BREACHES

Data breaches can happen in many ways. Such as in 2018, one of the biggest Aadhaar data breaches happened when the personal information of over one billion Aadhaar users was posted online. Personal information like name, address, and Aadhaar number, as well as biometric information like fingerprint and iris scans, were among the data that was exposed. Until the Indian government took action to get it deleted, this data was available for download on the internet for a short period of time.[3] The All-India Institute of Medical Sciences (AIIMS) in Delhi was targeted by a ransomware assault in November 2022, causing appointments, registration, billing, and laboratory report generation to be halted. The hack impacted both the hospital's primary and backup systems, corrupting all stored material.

Ransomware, a form of virus that encrypts system data, was responsible for the attack. This event emphasizes the requirement for robust security measures to safeguard sensitive data, particularly in government-run systems that store substantial volumes of individual data. Moreover, it highlights the significance of openness and responsibility. Separate your text and graphic files until the text has been prepared and styled. Hard tabs should be avoided, and hard returns should be used just once at the conclusion of a paragraph. There should be no pagination anywhere in the paper. Don't bother numbering text heads; the template will do it for you.

TABLE I.

Some Cloud Data Breaches in India		
Date	**Company/Organization**	**Estimate No. of data points lost**
Jan 2018	Zomato	17 million
Feb 2018	Punjab National Bank	10000
Mar 2019	Air India	4.5 million
Apr 2021	Mobikwik	100 million
Apr 2021	Facebook	500 million
Nov 2022	AIIMS	40 million

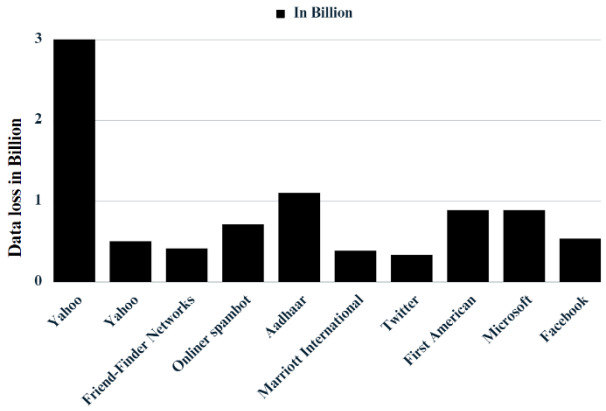

Fig 1. History of data breaches

1) Types Of Cloud Data Breaches.

There are different types of data breaches which are as follows:

A. Misconfiguration

Cloud data breaches are frequently caused by misconfiguration. When cloud services and systems are not correctly configured, they become exposed to cyberattacks and data breaches. Misconfiguration can contribute to cloud data breaches in a variety of ways.[4] For example, if a cloud storage service is not correctly set up, sensitive data may be vulnerable to unauthorized access. Furthermore, if a cloud system is not adequately protected, it may be subject to assaults such as denial of service attacks or malware infestations.

B. Weak Authentication

A significant source of cloud data leaks is weak authentication. The process of validating a user's identity before giving access to a system or data is referred to as authentication. When the authentication procedure is not robust enough to prevent unwanted access to the cloud system or data, this is referred to as weak authentication.[4] for example, with a company's cloud system, weak passwords or password reuse across several accounts might make it simpler for attackers to get access. Hackers can simply circumvent the authentication procedure and obtain access to the cloud if multi-factor authentication is not used.

C. Insider Threats

Insiders. with access to cloud resources, such as employees or contractors, can significantly threaten cloud security. Insider threats are a significant concern in cloud data breaches. An insider threat occurs when an employee or other authorized person with access to sensitive data intentionally or inadvertently exposes the data to unauthorized persons, possibly resulting in a data breach. [4] There are several ways that insider threats can contribute to cloud data breaches. For example, an employee may intentionally steal sensitive data from the cloud and sell it to a third party. Alternatively, an employee may accidentally expose sensitive data by misconfiguring a cloud service, such as accidentally making data publicly available.

D. Improper Storage

Improper storage in cloud data breaches refers to situations where sensitive information is stored in the cloud without adequate security measures in place to protect it. This can lead to cybercriminals' unauthorized access to confidential information, leading to data breaches. There are several ways that improper storage can contribute to cloud data breaches.[5] For example, if an organization fails to properly configure its cloud storage services, it could allow unauthorized access to data stored in the cloud. This could happen if the cloud service provider is not properly secured, or the organization's cloud storage is not properly secured. Another common cause of improper storage in cloud data breaches is when employees use weak passwords or reuse passwords across multiple accounts. Cybercriminals can take advantage of these weaknesses to gain access to cloud storage and steal sensitive information.

E. Malware

Malware is software intended to harm or disrupt computer systems, steal sensitive data, or gain unauthorized access to computer networks. Malware may infect cloud systems and steal data from the cloud, making it a substantial contributor to cloud data breaches. Malware may attack cloud systems in a variety of ways.[5] Cybercriminals, for example, can use phishing emails to fool employees into installing harmful software on their devices, which can then move to the cloud. Moreover, fraudsters might use flaws in cloud software to obtain access to cloud systems and infect them with malware.

F. Third-Party Service Provider

Organizations frequently engage third-party service providers to provide specialized services and expertise. Cloud service providers manage security service providers, and other firms that assist corporations manage their IT infrastructure are examples of third-party service providers. Regrettably, third-party service providers can also pose a risk to businesses.[6] In the case of cloud data breaches, for example, if a third-party service provider fails to adequately

safeguard their services or fails to apply sufficient security measures, thieves may be able to obtain access to sensitive data more easily.[7] Furthermore, if a third-party service provider suffers a data breach, sensitive data belonging to various firms that employ their services may be exposed.

2) Cost Analysis of Data Breach.

According to IBM and Verizon research, misconfigured cloud servers were a major cause of data breaches in 2020, responsible for around 20% of incidents.[8] Another significant component was weak or stolen passwords, which accounted for 61% of all breaches. According to IBM and the Ponemon Institute, insider risks accounted for around 25% of data breaches.[9] Inadequate data storage and unintentional data disclosure were also significant causes, accounting for almost 20% of all instances. Third-party services were also responsible for around 17% of cloud data breaches, according to IBM.

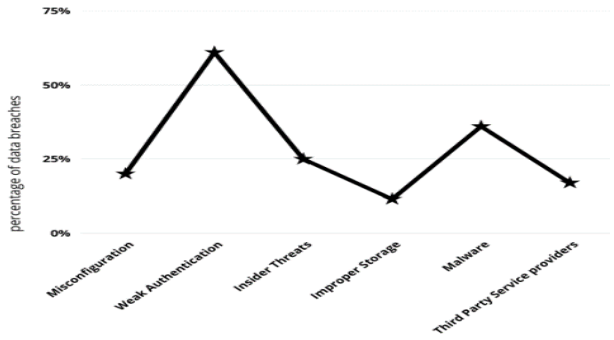

Fig 2. Amount of cloud data breached.

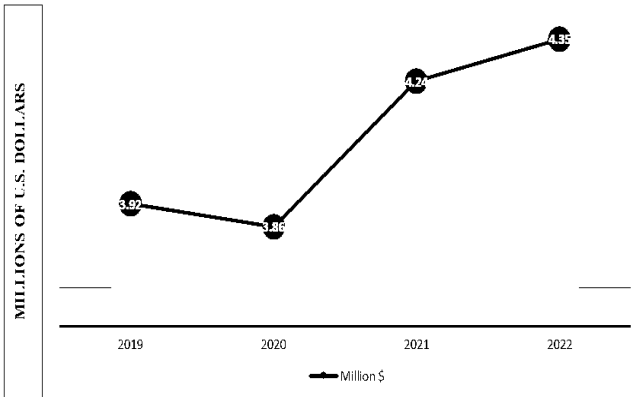

Fig 3. Average Cost of a Data Breach 2019 to 2022[10].

The highest average data breach cost in IBM Security's "The Cost of a Data Breach Report" ever was $4.35 million in 2022, up 2.6% from $4.24 million in 2021. The global average data breach cost increased by 1.5% in 2020 over the previous year, reaching $3.86 million, according to the 2021 report. According to the study, it takes an average of 287 days to discover and contain a data breach, with breaches that last more than 200 days costing an average of $4.24 million. According to the report, the average cost of a data breach in 2019 was $3.92 million, a 1.5% increase from the previous year. Malicious assaults were also revealed to be the top source of data breaches, with a malicious attack costing more than a non-malicious breach.10]

According to a Verizon data breach investigation report in 2022, ransomware is on the rise, increasing by 13% in the last five years and accounting for 25% of cases in 2021. The most prevalent problems identified were cloud misconfiguration errors, which contributed to 13% of the attacks. Regardless of event type, 82% of occurrences had a human component.[11]

IV. Prevention of Cloud Data Breach

Cloud data breaches can be avoided by combining technical measures and best practices. Here are some methods for avoiding cloud data breaches:

A. Misconfiguration :

Cloud misconfiguration refers to any flaws, gaps, or faults in your cloud adoption that could put your environment at risk.[12] Misconfiguration is a cloud computing issue since multi-cloud settings can be complex, making it difficult to notice and manually correct errors. Some common cloud misconfigurations.

a) Unrestricted Inbound & Outbound ports: Unrestricted inbound ports can be a serious security risk to your system since they permit anybody to connect to it via any port, possibly enabling hostile actors to take advantage of weaknesses in it.[12]

Unrestricted outbound ports can put your system at risk for security breaches because they let any application or process interact with outside services or systems. Malicious software can connect these uncontrolled outbound ports to command-and-control servers or secretly exfiltrate sensitive data.

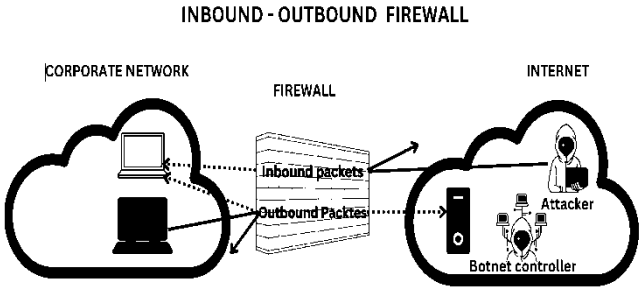

Fig 4. Protect Inbound & Outbound traffic.

b) Install a firewall: An essential element of any network security plan is a firewall. Set up your firewall to only permit traffic on required ports and protocols and block all incoming and outgoing traffic by default.

c) Use network segmentation: Divide the network into zones, each with its own set of security and access controls. This can lessen the effects of a security breach and stop threats from moving laterally.

d) Use endpoint protection: To safeguard your endpoints and thwart unwanted activity, use endpoint protection software such as antivirus, firewalls, and intrusion detection and prevention systems (IDPS).

e) Follow up on your network: With network monitoring tools and intrusion detection systems, keep an eye on your network for unusual activities and potential threats (IDS).

This can assist you in identifying risks and acting before they can harm you.[13]

B. Weak Authentication:

A data breach caused by poor authentication in the cloud might have huge consequences for an enterprise. Sensitive data, including private information, financial information, and intellectual property, may be taken, misplaced, or exposed as a result of a data breach. In addition to financial losses and legal and regulatory repercussions, this can harm an organization's reputation.

The following actions can be taken to mitigate this risk:

a) Put in place secure password procedures: Adopt strict password regulations that oblige users to use challenging, one-of-a-kind passwords. Think about utilizing a password manager to create and securely store strong passwords.

b) Install multi-factor authentication (MFA): To require users to submit a second element of authentication in addition to their password, such as a code texted to their mobile device.[14][15] This can greatly improve the authentication process's security. Employ secure authentication protocols OAuth, OpenID Connect, and SAML may all be used to securely authenticate users and prevent illegal access. MFA enables various authentication procedures to confirm a certain user's identity in many dimensions and numerous times. To protect the security and confidentiality of end-user credentials, a combination of single sign-on (SSO) and multifactor authentication (MFA) is used to get authentication, authorization, accountability, and availability (AAAA) [16]

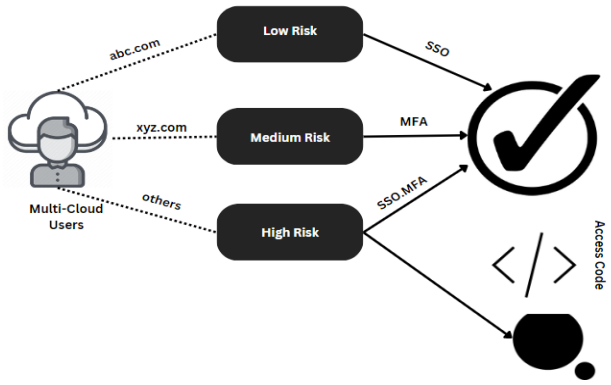

Fig 5. Proposed mitigation techniques.

Step 1: To place an order hosted by xyz.com, users from various domains sign in to abc.com. By web login, orders are confirmed and authorized. A single sign-on can be used to access low-risk data. The absence of necessary metadata prevents the implementation of additional security. Users receive an authority certificate from IDP when they log in. Step 2: Due to their reliance on the hosted services environment, users from the domain xyz.com are regarded as medium risk. For service access, multifactor authentication (MFA) is used to improve security and accountability.

Step 3: Additional users outside the federated trust environment will be rejected if SSO and MFA criteria are not met.[17] They are classified as "high-risk" since they are not associated with any federated or hosted domain. As a result, they have limited access to and completion of their order.

Methodology: Users from abc.com offer authentication by online login while attempting to place an order on the hosted site. When the order information arrives at xyz.com, the SSO procedure will be initiated. SSO provides authentication and authorization since the first and third parties are linked as a federated trust at the domain level.

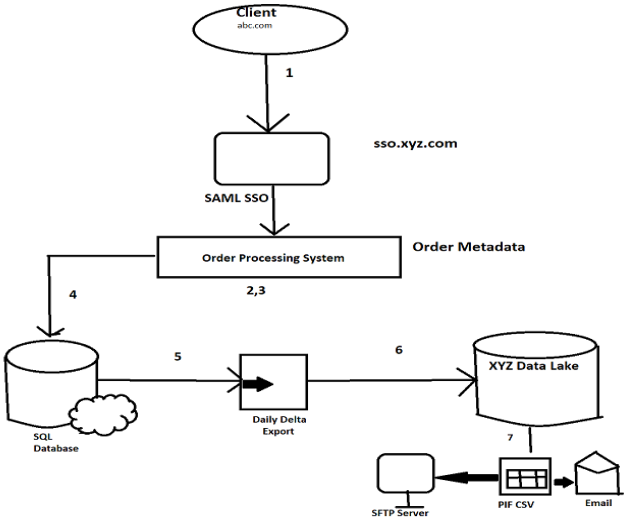

Fig 6. SSO workflow

c) Monitor the authentication logs: Keep an eye out for any strange or suspicious behaviour, such as unsuccessful login attempts or repeated login attempts coming from the same IP address. This can aid in your ability to recognize and address any hazards.

d) Review and update your authentication policies often to keep up to date with the most recent security best practices and to address any new risks or vulnerabilities as they appear.

C. Insider Threats & Improper Storage:

An insider threat is defined by the Cyber and Infrastructure Security Agency (CISA) as someone who, intentionally or accidentally, utilizes their allowed access to harm the organization's mission, resources, staff, facilities, information, equipment, networks, or systems. Insider threat actors are those who have genuine access to your data or security network. [18]

Insider threats can take many forms, including:

Insiders who steal or expose sensitive information on purpose; insiders who are careless; and insiders whose credentials have been compromised. Malicious insiders steal

or expose sensitive information on purpose; negligent insiders accidentally delete data; and insiders accidentally fall for phishing scams. Insider threats in a cloud data breach might be difficult to identify and avoid because the threats come from someone who has authorized access to the organization's system and data.

An organization's data is improperly stored in the cloud when it is exposed to theft or unauthorized access because it is not safe or secure. A few factors, including improperly

configured cloud storage settings, a lack of encryption, or insufficient access restrictions, might lead to improper storage.

Organizations can take the following actions to mitigate insider threats & Improper storage in a cloud data breach.

a) Implement access controls: Access controls should be put in place by organizations to restrict employee access to certain systems and data. The least privilege principle should guide access restrictions, which implies only allowing workers access to the information and systems they need to do their jobs.

b) Monitor user activity: Organizations should monitor user activity, including logins, file access, and other actions. This can assist in identifying illegal access to data or unusual activity that can point to an insider threat.

c) Implement data loss prevention (DLP) solutions:

By tracking data transfer and enforcing data usage guidelines, DLP solutions may help prevent sensitive data from being stolen or disclosed. [19]

d) Conduct regular security audits: Organizations may find security flaws and possible insider threats earlier by conducting regular security audits.

D. Malware:

Ransomware is a type of malware that encrypts essential data, rendering it unavailable to legitimate users, and demands a ransom in exchange for the decryption key.[20][21] If an attacker successfully installs ransomware on a cloud system, they may encrypt any data stored on that system, including sensitive information such as personally identifiable information (PII), financial records, or private corporate data. After encrypting the data, the attacker might demand money in return for the decryption key. If the ransom is not paid, the attacker may threaten to publicize or permanently wipe the encrypted data, inflicting serious harm to the cloud user or the business that operates the cloud service. Mitigating ransomware in cloud data breaches entails adopting preventative steps and building a complete incident response strategy in the event of an attack. These are some methods that may be used to assist reduce ransomware in cloud data breaches:

a) Enforcing access control policies: multi-factor authentication, zero-trust architecture, network segmentation, and other similar measures help keep ransomware and crypto worms from gaining access to sensitive data and propagating to additional network devices.

b) Keeping cybersecurity technologies up to date Anti-malware and antivirus software, firewalls, and secure web gateways, as well as enterprise cybersecurity solutions such as endpoint detection and response (EDR) and extended detection and response (XDR) technologies, assist security teams in detecting and responding to ransomware in real-time.

*c) Regularly backup data***:** Back up vital data stored in cloud services on a regular basis and preserve the backups offshore. This can assist to mitigate the effect of a ransomware attack by allowing encrypted data to be restored from a backup.

d) Applying patches regularly to aid in the prevention of ransomware attacks that take the use of software and operating system flaws.

e) Train users on security best practices: Regularly teach cloud users how to detect and avoid ransomware attacks, including how to spot phishing emails, notice unusual activity, and report security problems.

E. Third-party Service Provider:

A third-party service provider in a cloud data breach is a firm or organization that offers services to a cloud user or cloud service provider, such as data processing, storage, or management.[22][23] These are some actions you may take to reduce the risk of third-party service providers in a cloud data breach:

a) Conduct due diligence: examine the provider's security posture, compliance with applicable rules, and track record before interacting with a third-party service provider.[24]

b) Contractual protections: Verify that adequate contractual safeguards, including liability provisions, indemnity clauses, data protection standards, and incident response duties, are in place.

c) Keep a list of your active merchants.: Determine who all your third-party vendors are and how much information is shared with each of them before you can properly analyze the risk that your third-party providers present. Without a list of your third-party agreements, it is difficult to determine the level of risk such suppliers present. Despite this, just 46% of companies evaluate the cybersecurity risks associated with their vendors that deal with sensitive data.

d) Continuously check vendors for security risks: Over the course of your contract, a vendor's security posture may change. It is crucial that you continually review their security settings as a result. The issue is that the majority of companies don't regularly audit their suppliers. Instead, they rely on snapshot assessments, such as audits or security questionnaires, which frequently offer little insight into an organization's security position.

ANALYSIS AND DISCUSSION

In this research work the analysis has been done on some of the main cloud security issues including improper configuration, weak authentication, insider attacks, and unsuitable storage. Unrestricted inbound and outgoing ports might pose a security risk; to secure the network, it is advisable to create a firewall, implement network segmentation, and use endpoint protection. Secure password methods and multi-factor authentication (MFA) should be adopted, along with evaluating and upgrading authentication rules, as inadequate authentication can result in a data breach. The danger posed by insider threats can be reduced by regularly updating rules and checking authentication logs. To prevent insider threats and restrict unauthorized access, storage rules, and access restrictions should also be put in place. To reduce the risk of ransomware in cloud data

breaches, preventative steps such as access control policies, cybersecurity tool updates, regular data backups, and patch applications should be implemented. Additionally, training cloud users on security best practices can help them detect and avoid ransomware attacks. To minimize the risk of a data breach when working with third-party service providers in the cloud, it is important to take several steps. These include conducting due diligence, ensuring adequate contractual safeguards, maintaining a list of active merchants, and continuously monitoring vendors for security risks.

V. CONCLUSIONS

In this work, the different breaches have been presented, and prevention methods have been analyzed. cloud data breaches are a significant threat to organizations that store sensitive data in the cloud. misconfigurations, weak authentication, insider threats, inappropriate storage, malware, and third-party service providers are the key contributors to cloud data breaches. Organizations can use measures such as access control, frequent audits and monitoring, incident response planning, and data encryption to successfully manage these risks. To avoid data breaches and secure sensitive information, firms must be alert and proactive in their security practices. Organizations may limit the chance of data breaches and safeguard their reputation and financial well-being by employing appropriate security policies.

REFERENCES

[1] Govind Rao Mettu, Dr. Anitha Patil, "Data Breaches As Top Security Concern In Cloud Computing", Volume 119 No. 14 2018, pp.19-28

[2] Nandhakumar.C, Ranjithprabhu.K, Raja.M, "Counter Measures For Data Breach In Cloud Computing", Vol.2 Issue.11, Pg.: 124-129 November 2014

[3] Embracing Innovation in Government Global Trends," Aadhaar- India- Case Study- Oecd, Identity 1, pp.27-33, 2018.

[4] Insider Threat Mitigation | Cybersecurity and Infrastructure Security Agency CISA

[5] Moulika Bollinadi, Vijay Kumar Damera, “Cloud Computing: Security Issues and Research Challenges”, Volume 7, Issue 11, pp.64-73, 2017.

[6] Priyanka S P, Ranjith, Shridevi Prabhu B S, Nalini " A Review Paper on Security in Cloud Computing", Volume 7, Issue 08, pp.1-5,2019

[7] Anatomy of a Data Breach Why Breaches Happen and What to Do About It

[8] Ponemon Institute and IBM Security "Cost of a Data Breach Report" 2021.

[9] Ponemon Institute and IBM Security "Cost of a Data Breach Report" 2022.

[10] KLR | New Data Breach Study Highlights Risks of Remote Work (kahnlitwin.com)

[11] Cybercrime thrives during a pandemic: Verizon 2021 Data Breach Investigations Report | About Verizon

[12] National Security Agency | Cybersecurity Information, "Mitigating Cloud Vulnerabilities", U/OO/106445-20 ,PP-29-0025, 22 jan 2020.

[13] John Patrick Barrowclough, Rameez Asif, "Securing Cloud Hypervisors: A Survey of the Threats, Vulnerabilities, and Countermeasures", Volume 2018, pp.1-20, 2018

[14] Aleksandr Ometov, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, Tommi Mikkonen and Yevgeni Koucheryavy, "Multi-Factor Authentication: A Survey", 2018

[15] B. Madhuravani, Dr. P. Bhaskara Reddy, P. LalithSamanth Reddy "A Comprehensive Study on Different Authentication Factors", Vol. 2 Issue 10, pp.1358-1361, 2013

[16] Muhammad Iftikhar Hussain, Jingsha He, Nafei Zhu, Fahad Sabah, Zulfiqar Ali Zardari, Saqib Hussain, and Fahad Razque, "AAAA: SSO and MFA Implementation in Multi-Cloud to Mitigate Rising Threats and Concerns Related to User Metadata", Vol 11 Issue 7, pp.1-16,2021

[17] Kari, N.M.; Kebande, V.R.; Ikuesan, R.A.; Sookhak, M.; Venter, H.S. “Hardening SAML by Integrating SSO and Multi-Factor Authentication” Proceedings of the 3rd International Conference on Networking, Information Systems & Security, Marrakech, Morocco, 15 December pp. 1–6.

[18] Cybersecurity and Infrastructure Security Agency "Insider Threat Mitigation Guide" Nov 2020

[19] Abdullah Tariq Al-Essa, "Best Practices For A Successful Dlp Implementation", Vol.9, Issue 3, pp.18-20, Jul-Sep 2021.

[20] Aashi Singh Bhadouria, "Study of: Impact of Malicious Attacks and Data Breach on the Growth and Performance of the Company and Few of the World’s Biggest Data Breaches", Volume 10, Issue 10, pp.1-11, June 2022.

[21] Chenquan Gan, Qingdong Feng, Xulong Zhang, Zufan Zhang, And Qingyi Zhu, "Dynamical Propagation Model of Malware for Cloud Computing Security", Volume 8, pp.20325-20333, 2020.

[22] Third-Party Security Assurance and Shared Responsibilities Special Interest Groups PCI Security Standards Council, "Information Supplement: Third-Party Security Assurance", pp.1-48, 2016

[23] Long Cheng, Fang Liu and Danfeng (Daphne) Yao, "Enterprise data breach: causes, challenges, prevention, and future directions", pp.1-14, 2017.

[24] Jennifer Quartana Guethoff, Marie-Josée Bérubé, Hylton Macdonald, Jens Ole Legart, Randall Corley," The Good Practice Guidelines on Conducting Third Party Due Diligence",pp.1-48,2013.