INSE 6320

Risk Analysis for Information and Systems Engineering

Summer 2024

Topic:- Cybersecurity Risks in Cloud Computing Environments: An Integrated Risk Analysis and Risk Assessment

Submitted to:

Prof. Manar Amayri

Submitted by:

Sayyed Hussain	**40262414**
Shaik Mohammad Haneef	**40264904**
Athira Dinesh Mangaparambil	**40258046**
Arjun Payyattil Bindeswar	**40263448**

Cybersecurity Risks in Cloud Computing Environments: An Integrated Risk Analysis and Risk Assessment

1st Sayyed Hussain *2nd Shaik Mohammad Haneef* *3rd Athira Dinesh Mangaparambil*

40262414 *4026904* *40258046*

4th Arjun Payyattil Bindeswar

40263448

1. ABSTRACT:

Cloud computing has transformed the digital environment by delivering scalable and adaptable hosted services via the internet, resulting from distributed software design. This technology has created new user communities and markets, supported by data centers worldwide. Despite these advantages, security remains a major concern for the widespread use of cloud computing services. This project identifies and assesses important cloud computing risks, which are divided into three categories: confidentiality, integrity, and availability. The project uses Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Bayesian analysis, F-N curves, sensitivity analysis, and utility functions to provide a thorough understanding of potential risks and evaluate the effectiveness of alternative mitigation techniques. The report emphasizes the significance of strong security policies, procedures, and technology for protecting sensitive data and ensuring the integrity and availability of cloud services.

2. INTRODUCTION:

Cloud computing has revolutionized the digital landscape by providing scalable and flexible hosted services over the internet,emerging from distributed software architecture. This technology has fostered new user communities and markets, supported by data centers worldwide. Examples of widely used cloud services include Microsoft SharePoint and Google applications[1].

Security is paramount for the broader adoption of cloud computing services. Various studies have explored security solutions, including technological measures and security policies. Recent research has examined new types of attacks on cloud environments from a criminological perspective,proposing solutions based on criminal theories. Security issues affecting cloud computing attributes have been identified, with recommendations provided to address these problems[1].

Significant security challenges and vulnerabilities accompany the widespread use of cloud computing in information technology. Intruders often exploit weaknesses in cloud models to access users' private data and attack computer processing power. Despite the advantages of cloud computing, some service providers are hesitant to embrace it due to immature security technologies. Research indicates a need for investment in security measures associated with cloud computing

devices. Studies have proposed various methods to evaluate cloud security, including an “attack tree map” (ATM) to analyze vulnerabilities and threats[1]. Trusted computing platforms combined with cloud computing can offer enhanced security services like confidentiality, authentication, and integrity.

3. LITERATURE REVIEW:

Current literature emphasizes the importance of robust security measures and effective risk management in cloud computing. Fault Tree Analysis (FTA) and Event Tree Analysis (ETA) are essential for identifying and analyzing cybersecurity threats by breaking down complex events and mapping potential failure points (Marten et al.[4],2012; Tchernykh et al.[3], 2016). Bayesian Analysis updates the likelihood of security breaches using new data, providing a

dynamic risk assessment (Alouffi et al.[1],2021; Thalesgroup[7],2023). F-N curves and sensitivity analysis help visualize and prioritize risks (Ali et al.[5], 2024).

Mitigation strategies include implementing encryption, multi-factor authentication, stringent security policies, regular employee training, and disaster recovery plans (Alassafi et al.[2],2017; Thales Group[7], 2023). Some analysis rely on assumptions due to limited data, such as estimating system failure probabilities to evaluate risk reduction measures (Verizon[8], 2024).Integrating these methods and assumptions helps organizations manage cloud computing risks, ensuring data protection and service reliability (PricewaterhouseCoopers[11], 2024).

4. PROBLEM DESCRIPTION:

Overview:
Cloud computing has transformed the digital world by providing scalable and adaptable hosted services via the internet. This technology, which emerged from distributed software architecture, has enabled new user communities and marketplaces through data centers worldwide. Microsoft SharePoint and Google apps are two popular cloud services. Despite these benefits, the security of cloud computing remains critical to its widespread adoption. Several studies have investigated security solutions, including technological methods and security regulations, to address security concerns about cloud computing properties.

Individual Components and Risks:

The project focuses on identifying and assessing important risks in cloud computing, which are divided into confidentiality, integrity, and availability issues.

Assumptions and Data:

Due to a lack of specific data, we make assumptions about system failure probabilities and their influence on confidentiality, integrity, and availability.

- Utility functions for assessing risk reduction measures.
- Assumptions are justified using industry data and average statistics from relevant studies.

Fault and Event Tree Analysis:

Fault Tree Analysis (FTA) analyzes the underlying causes of a cybersecurity risk event in cloud computing, categorizing it into intermediate or base events such as data breaches, external attacks, and insider threats. Event Tree Analysis (ETA) depicts the sequence of events that occur following a data breach, demonstrating how quick detection and good mitigation can result in limited effects, but delays and ineffective responses might have far-reaching implications.

- Using these risk analysis tools, the project aims to provide a thorough understanding of potential risks and the efficacy of various mitigation tactics in cloud computing settings.

5. RISK IDENTIFICATION & ASSESSMENT:

Cloud security is critical for modern corporate operations but comes with inherent hazards. Below are the major risks in cloud computing.

5.1 Cloud Computing Risks:

Security principles	Risks	Cloud service models (SaaS, PaaS and IaaS)		
Confidentiality	Insider user	SaaS	PaaS	IaaS
	External attacker	SaaS	PaaS	
	Data Leakage	SaaS	PaaS	
Integrity	Data segregation	SaaS	PaaS	
	User access	SaaS	PaaS	IaaS
	Data quality	SaaS	PaaS	
Availability	Change management	SaaS	PaaS	IaaS
	Denial of Service	SaaS	PaaS	IaaS
	Physical disruption			IaaS
	Exploiting weak recovery procedures	SaaS	PaaS	IaaS

Table: Classification of Risks [2]

5.1.1 Confidentiality Risks:

1. ***Data Leakage or Breach:*** Unauthorized access to sensitive cloud-stored data can expose confidential information due to security flaws, poor access controls, or insufficient encryption.
2. ***External Attacker:*** External attackers can exploit weaknesses in the cloud infrastructure to obtain access to sensitive data through hacking, phishing, and malware attacks.
3. ***Insider Threat:*** Employees or contractors with access to sensitive data may misuse their authority, either purposefully or accidentally.Insiders already have legitimate access, making their potential misuse very risky[2].

5.1.2 Integrity Risks:

1. Data Segregation: In multi-tenant cloud environments, improper data segregation can result in unauthorized access or alteration. Data isolation between multiple users is critical for maintaining data integrity.

2. User Access: Inadequate management of user access permissions can result in illegal alterations to the data. Proper access controls are required to ensure that only authorized users can modify data.

3. Data Quality: Maintaining the quality and completeness of data is essential. Errors during data processing, transport, or storage can jeopardize the data's integrity[2].

5.1.3 Availability Risks:

1. Change Management: Uncontrolled or poorly managed modifications to the cloud environment might cause system downtime or poor performance. Proper change management techniques are required to ensure service availability.

2. Denial of Service (DoS) Attack: DoS attacks attempt to disable cloud services by overwhelming them with traffic, preventing legitimate users from accessing the services and disrupting business operations.

3. Physical Disruption: Physical Disruption: Natural disasters, power outages, and data center damage can reduce cloud service availability.Proper physical security and catastrophe recovery plans are crucial.

4. Exploiting Weak Recovery Procedures: Inadequate disaster recovery and backup processes can cause protracted outages and data loss. Effective recovery processes are required to rapidly restore services and data following an incident[2].

5.1.4 Other Risks:

1. Time Risk: Delays in detecting cloud adoption, complying with data protection rules, and adopting new solutions can impact cloud computing performance and benefits.

2. Performance Risk: Concerns regarding the cloud system's performance and transparency in meeting service levels may influence confidence and satisfaction. Ensuring that the cloud service meets performance requirements while remaining reasonably priced is critical.

3. Social or Reputational Risk: Data breaches and service unavailability can harm an organization's reputation, potentially affecting customer trust and the organization's public image.

4. Financial Risk: Data breaches can cause financial losses, reputational damage, and costs associated with security failures. It is crucial to consider the cost-benefit of cloud services in terms of security[2].

5.2 Qualitative Risk Analysis:

By understanding these risks, organizations can implement appropriate measures to safeguard their data and ensure their cloud services remain secure, confidential, and available.

Confidentiality Risks:

1. Data Breach: Security issues and weak access restrictions can lead to sensitive cloud data being leaked or breached, posing a significant risk to confidentiality. Attackers can exploit these vulnerabilities to gain access to and steal data from the company, causing substantial financial and reputational damage.

2. External Attacker: These attacks are highly likely and have a significant impact, using sophisticated tactics such as phishing, malware, or hacking to breach security and access confidential data. Organizations must deploy effective security measures to protect against these increasingly complex threats.

3. Insider Threat: Insiders with legitimate access have a medium likelihood and serious impact of misusing their authorization, either mistakenly or maliciously. This could include unauthorized data sharing or harmful behavior by dissatisfied staff, underscoring the importance of rigorous access restrictions and monitoring[3].

Integrity Risks:

1. Data Segregation: This risk has a medium likelihood but a high impact due to inadequate data segregation in shared environments, resulting in unauthorized access or alterations. Ensuring effective data segregation through techniques such as encryption and access controls is critical for maintaining data integrity.

2. User Access: Improper management of user permissions is a medium likelihood and high impact risk, potentially leading to illegal data alterations. Implementing strict user access controls and conducting regular audits can assist in reducing this risk by ensuring that only authorized individuals can edit data.

3. Data Quality: Errors in data processing, transit, and storage have a medium likelihood and moderate

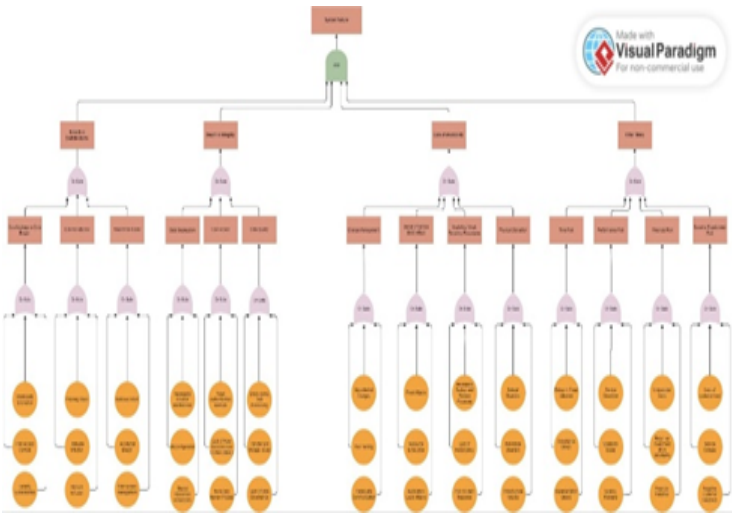
impact on data correctness. Organizations should establish data validation and error-checking systems to maintain high data quality and avoid inaccuracies[3][5].

Availability Risks:

1. ***Change Management:*** Uncontrolled or poorly managed modifications to the cloud environment might cause system downtime or poor performance. Proper change management techniques are required to ensure service availability.
2. ***Denial of Service (DoS) Attack:*** DoS attacks attempt to disable cloud services by overwhelming them with traffic, preventing legitimate users from accessing the services and disrupting business operations.
3. ***Physical Disruption:*** Physical catastrophes such as natural disasters, power outages, and data center damage can impact cloud service availability. Effective physical security measures and disaster recovery strategies are critical.
4. ***Exploiting Weak Recovery Procedures*:** Inadequate disaster recovery and backup processes can cause protracted outages and data loss. Effective recovery processes are required to rapidly restore services and data following an incident[3][5].

6. RISK ANALYSIS:

6.1 Fault tree:



Fault Tree Analysis[17]

A rigorous technique called fault tree analysis (FTA) is used to locate and examine the possible sources of a major event. This top event is broken down into multiple categories in the diagram, each of which adds to the overall risk through different intermediate and base events. Breach in Confidentiality, Breach of Integrity, Lack of Availability, and Other Risks are the four primary categories into which the top event is divided. Events such as data leaks or breaches brought on by insufficient encryption, subpar access controls, or security flaws are considered ***breaches of confidentiality.*** By taking advantage of flaws in endpoint security, network security, and training, external attackers increase this risk through phishing, malware, and network intrusions. Insiders increase this risk because of inadequate access control and inadequate training, whether through deliberate or unintentional breaches.

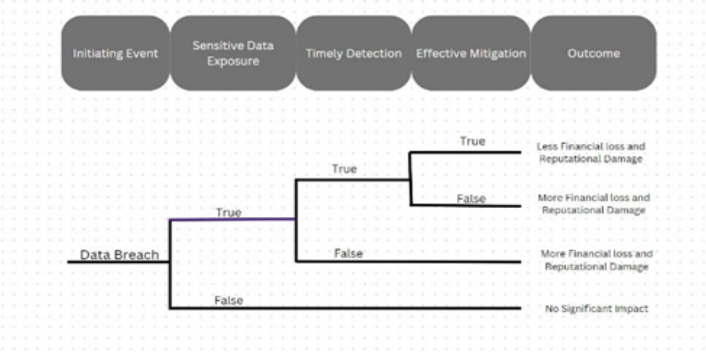
Problems with data quality, inadequate user access controls, and incorrect data segregation are all examples of ***breaches of integrity*.** Unauthorized data access and alterations can be caused by inadequate isolation techniques, misconfigurations, and shared resources. Data quality is further lowered by processing, transport, and storage problems combined with inadequate data governance. Weak authentication, a lack of role-based access control, and irregular access reviews also jeopardize data integrity. A lack of availability mitigates the danger of ineffective recovery methods, DoS attacks, change management failures, and physical disruptions. Poor communication, insufficient testing, and uncontrolled modifications can all cause service disruptions. DoS attacks overload cloud systems via a number of tactics, making them inaccessible. Weak backups, weak recovery procedures, and subpar incident responses increase the impact of incidents, whereas infrastructure failures and natural and man-made calamities physically interrupt service availability.

Time, performance, money, and social or reputational hazards are some additional issues. The timely provision of services might be impeded by delays in cloud acceptance, compliance, and implementation. Service outages, scalability challenges, and latency concerns are performance hazards that affect dependability and user pleasure. While social or reputational risks stem from data breaches, service interruptions, and unfavorable reviews that harm the company's brand and undermine customer confidence, financial risks include unforeseen expenses, questionable returns on investment, and fines. Many techniques can be used to reduce cybersecurity threats in cloud computing. Confidentiality breaches can be decreased by improving encryption methods, enforcing strict password regulations, using multi-factor authentication, and implementing role-based access

controls. Employees who receive regular security awareness training are better able to avoid phishing and social engineering scams. Strict data governance regulations, frequent access checks, network segmentation, and efficient data isolation are necessary to preserve data integrity. Anti-DoS technology can be used in conjunction with disaster recovery, business continuity plan implementation, and testing to guarantee availability and reduce downtime. Simplifying project and compliance management, utilizing performance monitoring technologies, and putting cost control measures into place are all necessary to address additional risks. Creating a strong incident response plan and public relations communication strategy aids in breach management and upholding client confidence. When combined, these methods lower the cybersecurity risks associated with cloud computing settings[3] [4].

6.2 Event tree:

An effective technique for comprehending the chain of events that follows an initial incident—in this case, a data breach and how different factors influence the final outcomes is event tree analysis. It



Event Tree Analysis[17]

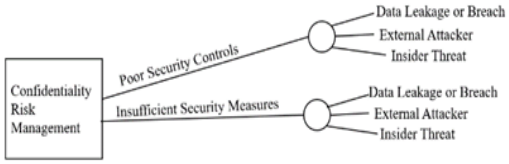
contributes to the identification of important points where interventions can be most effective by offering a visual depiction of multiple possible paths from the initiating event to the end outcomes. The study focuses on the logical sequence of events rather than the probability of each path due to the absence of specific data. A data breach is the catalyst that starts the process.Whether sensitive data is exposed is the first decision to be made after this incident. In the event that private information is truly compromised, prompt detection of the breach is the next crucial element. Early detection is essential because it enables quick action to lessen the harm.

The next stage, if the breach is discovered quickly, is to assess how well the mitigating measures worked. Repercussions can be greatly reduced with effective mitigation, resulting in less financial loss and reputational harm. However, there could be serious repercussions, including large financial losses and serious harm to the organization's reputation, if the mitigation is ineffective or if the breach is not discovered in a timely manner. On the other hand, if no confidential information is made public, the breach will have little effect and won't have a big effect on the company. In the event of a data breach, this scenario is the best-case scenario. The significance of implementing strong detection and mitigation tactics to efficiently handle cybersecurity concerns is highlighted by this event tree analysis. Organizations may significantly lessen the negative effects that breaches have on their finances and reputation by promptly identifying and addressing them[5][10].

6.3 Decision Tree:

6.3.1 Confidentiality Risk Management:

The decision tree diagram depicts the important elements contributing to confidentiality concerns in cloud computing, focusing on the impact of insufficient security controls and weak safeguards.These flaws can lead to data leaks or breaches, external attacks, and insider risks. The diagram emphasizes the importance of strong security policies, procedures, and technology in protecting sensitive data from unauthorized access and exploitation. Understanding the core reasons allows firms to focus on upgrading their security frameworks to protect data from breaches and unauthorized access[4][6].



Decision Tree for Confidentiality Risk Management[17]

Confidentiality Mitigation Strategies:

1. Implement Strong Access Controls: Use multi-factor authentication, role-based access restrictions, and scheduled audits.

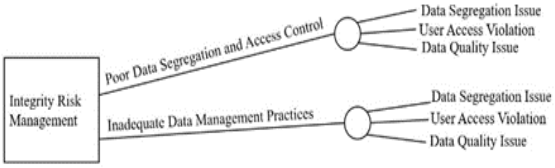
2. Enhance Security Measures: Install encryption, intrusion detection systems, and perform regular security updates.

3. Employee Training: Consistently educate personnel on security best practices and data protection.

4. Conduct Regular Security Assessments: Perform frequent security assessments and penetration testing[18].

6.3.2 Integrity Risk Management:

The decision tree diagram identifies the primary elements contributing to integrity threats in cloud computing, emphasizing the consequences of poor data segregation and access control, as well as inappropriate data management procedures. These difficulties can lead to data segregation challenges, user access violations, and data quality issues. The diagram shows that without effective data segregation, strict access controls, and robust data management practices, data integrity is at risk. Understanding these core issues allows firms to focus on improving their data management frameworks, ensuring data accuracy and reliability[4][6].



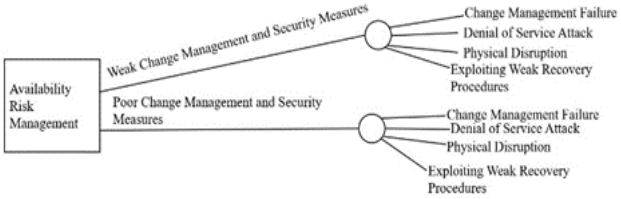
Decision Tree for Integrity Risk Management[17]

Integrity Mitigation Strategies:

1. ***Implement Effective Data Segregation:*** Use logical and physical separation strategies to maintain data integrity.
2. ***Enhance Access Control:*** Enforce Rigorous access controls and regularly review user permissions.
3. ***Adopt Robust Data Management Practices:*** Use data validation, error checking, and regular audits to preserve data quality[18].

6.3.3 Availability Risk Management:

The decision tree diagram depicts major elements contributing to availability concerns in cloud computing, focusing on the repercussions of ineffective change management and security measures. These flaws can lead to change management failures, denial of service (DoS) attacks, physical interruptions, and the exploitation of weak recovery methods. The diagram demonstrates that without adequate change management and security policies, cloud service availability is significantly jeopardized. Understanding these core reasons allows firms to focus on improving their change management and security frameworks to maintain service continuity[4].



Decision Tree for Availability Risk Management[17]

Availability Mitigation Strategies:

1. ***Implement Robust Change Management Processes:*** Ensure all modifications are thoroughly tested and confirmed before implementation.
2. ***Strengthen Security Measures:*** Deploy firewalls, intrusion detection systems, and traffic monitoring to protect against DoS assaults.
3. ***Create and Update Disaster Recovery Plans Regularly:*** Develop plans to efficiently handle physical disturbances.
4. ***Enhance Recovery Procedures*:** Regularly test and update backup and recovery mechanisms to ensure quick restoration of services following an incident[18].

6.4 Bayesian Analysis:

Bayesian analysis is a theory that uses probability to express a degree of belief in an event, which may be based on prior knowledge or personal beliefs [7].

Based on recent data from 2023 [8], we can define prior probabilities for different security risks affecting the CIA triad in cloud environments:

P(C)= .30 Probability of a confidentiality breach.

P(I)= .25 Probability of an integrity breach.

P(A)= .35 Probability of an availability breach.

E1: Data breaches affecting confidentiality.

E2: Integrity issues detected in software supply chains and cloud environments.

E3:Service outages affecting availability.

The likelihood of happening if events are P(E1|C): The likelihood of data breaches if there is a confidentiality breach is around 0.8. This is supported by data showing that 45% of cloud-based breaches are due to compromised data storage and IAM misconfiguration.

P(E2|I): The likelihood of integrity issues if there is an integrity breach is approximately 0.7. The increasing number of software supply chain attacks and misconfigurations highlights this.

P(E3|A): The likelihood of service outages if there is an availability breach is around 0.9, considering the frequency and impact of service disruptions in cloud

environments. Using Bayes' theorem to update the probabilities based on the new evidence:

6.4.1 For Confidentiality Breach:

$P(C|E1)=(P(E1|C)*P(C))/P(E1)$

Where: $P(E1)=P(E1|C)*P(C)+P(E1|C')*P(C')$

Assuming $P(E1|C')=0.2$:

$P(E1)=(0.8*0.30)+(0.2*0.70)=0.24+0.14=0.38$

Now calculating $P(C|E1)$:

$P(C|E1)= 0.8*0.30/0.38=0.24/0.38=0.632$

The updated probability of a confidentiality breach given data breaches is approximately 63.2%.

6.4.2 For Integrity Breach:

$P(I|E2)= (P(E2|I)*P(I))/ P(E2)$

Where: $P(E2)=P(E2|I)*P(I)+P(E2|I')*P(I')$

Assuming $P(E2|I')=0.3$:

$P(E2)=(0.7*0.25)+(0.3*0.75)=0.175+0.225=0.40$

Now calculating $P(I|E2)$:

$P(I|E2)=0.7*0.25/0.40 =0.175/ 0.40=0.438$

The updated probability of an integrity breach given integrity issues is approximately 43.8%.

6.4.3 For Availability Breach:

$P(A|E3)= (P(E3|A)*P(A))/ P(E3)$

Where: $P(E3)=P(E3|A)*P(A)+P(E3|A')*P(A')$

Assuming $P(E3|A')=0.1$:

$P(E3)=(0.9*0.35)+(0.1*0.65)=0.315+0.065=0.38$

Now calculating $P(A|E3)$:

$P(A|E3)= 0.9*0.35/0.38=0.315/0.38=0.829.$

The updated probability of an availability breach given service outages is approximately 82.9%.

The Bayesian analysis was conducted to update the probabilities of security breaches in cloud environments, helping to quantify and prioritize risks based on recent evidence[8][9].

Mitigation strategies:

1. Confidentiality Breach: Implement data encryption.

2. Integrity Breach: Strengthen software supply chain security.

3. Availability Breach: Deploy redundancy and failover mechanisms.

6.5 Sensitivity Analysis For Data Breach Risk:

Let us consider "Data Breach" risk under the Confidentiality Risks category, as it is a significant concern for organizations. Let us assume 3 scenarios: Low, Medium, and High Risk of Data Breach. The potential financial impact of a data breach will be estimated based on industry averages and the organization's size. According to the IBM Cost of a Data Breach Report the average total cost of a data breach is $4.35 million. The report also states that the average cost of a data breach for organizations with more than 25,000 employees is $5.71 million.

Let us also consider an organization that has more than 25,000 employees and uses $5.71 million[10].

6.5.1 Low Risk of Data Breach Scenario:

Probability of occurrence (p) = 0.2 (20%)

Potential financial impact (I) = $1.14 million (20% of $5.71 million)

Expected Value (EV) = p × I + (1 - p) × 0

= 0.2 × $1.14 million + 0.8 × 0

= $228,000.

6.5.2 Medium Risk of Data Breach Scenario:

Probability of occurrence (p) = 0.5 (50%)

Potential financial impact (I) = $2.86 million (50% of $5.71 million)

Expected Value (EV) = p × I + (1 - p) × 0

=0.5 × $2.86 million + 0.5 × 0 = $1.43 million

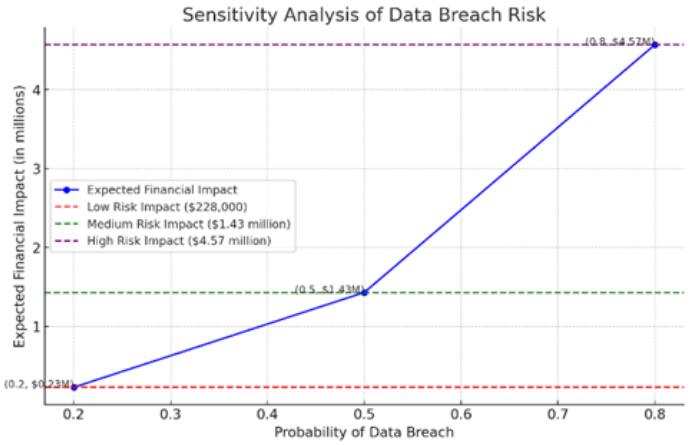
6.5.3 High Risk of Data Breach Scenario:

Probability of occurrence (p) = 0.8 (80%)

Potential financial impact (I) = $5.71million (100% of the average cost)

Expected Value (EV) = p × I + (1 - p) × 0

= 0.8 × $5.71 million + 0.2 × 0 = $4.57 million.



If the probability of a data breach is below 0.25 (25%), the Low Risk scenario has the lowest expected financial impact.

If the probability is between 0.25 and 0.75 (25% to 75%), the Medium Risk scenario has the lowest expected financial impact. If the probability exceeds 0.75 (75%), the High Risk scenario has the lowest expected financial impact.

Based on this sensitivity analysis, the organization can prioritize its risk mitigation efforts and allocate resources accordingly. For example, if the estimated probability of a data breach is around 0.6 (60%), focusing on mitigating the Medium Risk scenario would be most effective in minimizing the expected financial impact[10].

6.6 F-N Curve Analysis for Cyber Attacks on Cloud Environments:

The F-N curve provides a visual representation of societal risk from different cloud cyber attack scenarios, illustrating both their projected frequency and potential consequence severity in terms of the number of records exposed[13].

Cyber Attack Scenarios and Assumptions[13]:

1. Less Frequent Cyber Attack with Lower Number of Records Exposed:

i. Jamming Attacks:

Assume: F = 10^-4 incidents/year, N = 10^3 records exposed. Assume potential loss: $0.1 million

2. Moderately Frequent Cyber Attacks with Moderate Number of Records Exposed:

i. Insecure Interfaces and APIs:

Assume: F = 10^-2 incidents/year, N = 10^5 records exposed. Assume potential loss: $1 million

ii. Misconfigurations:

Assume: F = 5 * 10^-2 incidents/year, N = 5 * 10^5 records exposed. Assume potential loss: $5 million

3. Less Frequent but High Number of Records Exposed:

i. Data Breaches:

Assume: F = 10^-3 incidents/year, N = 10^7 records exposed. Assume potential loss: $10 million.

ii. Account/Identity Hijacking:

Assume: F = 5 * 10^-4 incidents/year, N = 5 * 10^6 records exposed. Assume potential loss: $8 million

4. Very Rare but Potentially Exposing a Huge Number of Records[13]:

i. Malicious Insider Threats:

Assume: F = 5 * 10^-6 incidents/year, N = 5 * 10^8 records exposed. Assume potential loss: $ 20 million.

Data Points Summary:

- (F, N)
- (10^-4, 10^3)
- (10^-2, 10^5)
- (5 * 10^-2, 5 * 10^5)
- (10^-3, 10^7)
- (5 * 10^-4, 5 * 10^6)
- (5 * 10^-6, 5 * 10^8)

Calculating Cumulative Frequency:

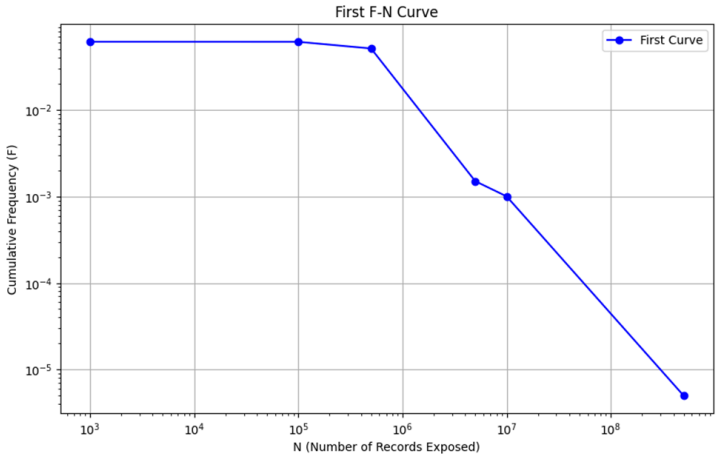
Sorted Points in Descending Order by NNN:

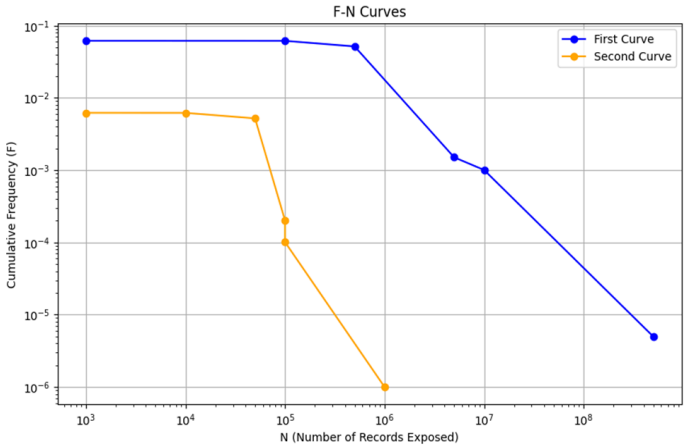
1. (5 * 10^-6, 5 * 10^8)
2. (10^-3, 10^7)
3. (5 * 10^-4, 5 * 10^6)
4. (5 * 10^-2, 5 * 10^5)
5. (10^-2, 10^5)
6. (10^-4, 10^3)

Cumulative Frequency Points:

1. (5 * 10^-6, 5 * 10^8)
2. (1.005 * 10^-3, 10^7)
3. (1.505 * 10^-3, 5 * 10^6)
4. (5.1505 * 10^-2, 5 * 10^5)
5. (6.1505 * 10^-2, 10^5)
6. (6.1605 * 10^-2, 10^3)

Plotting the F-N Curve: Plot points (N, cumulative F) on a log-log scale to visualize societal risk.





The F-N curves[14] illustrate the impact of mitigation measures on cyber attacks. The blue curve (pre-mitigation) shows higher frequencies and greater severities, while the orange curve (post-mitigation) shows significant reductions in both, reflecting improved security and reduced impact from cyber attacks.

Mitigation Measures and New Data Points[14]:
Assumed reduced risk profile post-implementation of security controls:
1. Jamming Attacks: New Point: (10^-5,10^3) // Monitoring and signal strength enhancement.
2. Insecure Interfaces and APIs: New Point: (10^-3, 10^4) //Patch management and strong access controls.
3. Misconfigurations: New Point: (5 * 10^-3, 5 * 10^4) // Automated configuration management and audits.
4. Data Breaches: New Point: (10^-4, 10^5) // Vulnerability management and encryption.
5. Account/Identity Hijacking: New Point: (10^-4, 10^5) // Multi-factor authentication and behavior monitoring.
6. Malicious Insider Threats: New Point: (10^-6, 10^6) // Activity monitoring and background checks.

Here are the sorted points in descending order by \(N \) and their corresponding cumulative frequencies.

Sorted Points in Descending Order by (N):
1. (10^-6, 10^6)
2. (10^-4, 10^5)
3. (10^-4, 10^5)
4. (5 * 10^-3, 5 * 10^4)
5. (10^-3, 10^4)
6. (10^-5, 10^3)

Cumulative Frequency Points:
1. (10^-6, 10^6)
2. (1.01 * 10^-4, 10^5)
3. (2.01 * 10^-4, 10^5)
4. (5.201 * 10^-3, 5 * 10^4)
5. (6.201 * 10^-3, 10^4)
6. (6.211 * 10^-3, 10^3)

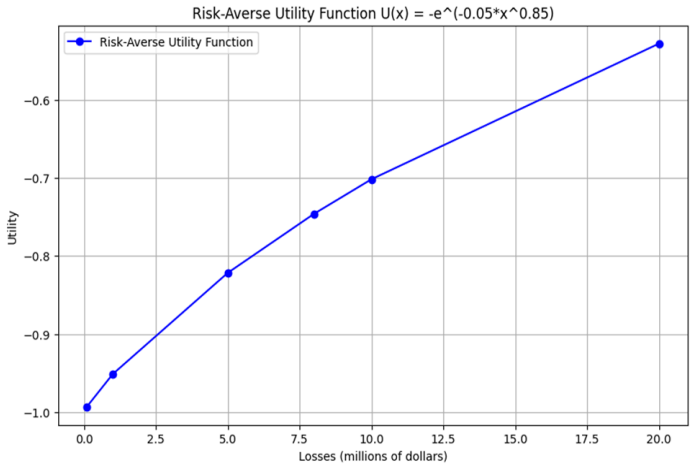
6.7 UTILITY FUNCTION GRAPH:

A utility graph in this scenario helps quantify the company's risk preferences and visualize the impact of potential cyber attack losses. It aids in decision-making by illustrating how different levels of losses affect the company's overall utility. This helps prioritize cybersecurity investments and strategies, balancing risk and reward effectively[16].
We don't have highly quantifiable data to know both 'a' and 'b' in the utility function, hence we are assuming them such that they will produce a risk averse graph. Because most of the company's investments show they are risk averse in nature, as they prioritize minimizing potential financial losses and maintaining customer trust over taking on higher risks. For example, JPMorgan Chase, one of the largest banks in the United States, invests heavily in cybersecurity measures to protect against data breaches and other cyber attacks.

Parameters for Utility Function:
(a = 0.05), (b = 0.85).
Potential Losses in Millions of Dollars for each type of cyber attack annually (x).
$0.1 million, $1 million, $5 million, $8 million, $10 million, $20 million.
The utility function is defined as: U(x) = -e^{-ax^b}
Calculations
1. For x = 0.1: U (0.1) = -e^ (-0.05 * (0.1) ^ 0.85) ≈ -0.995.
2. For x = 1: U (1) = -e ^ (-0.05 * (1) ^ 0.85) ≈ -0.951
3. For x = 5: U (5) = -e ^ (-0.05 * (5) ^ 0.85) ≈ -0.788

4. For x = 8: U (8) = -e ^ (-0.05 * (8) ^ 0.85) ≈ -0.696
5. For x = 10: U (10) = -e ^ (-0.05 * (10) ^ 0.85) ≈ -0.650
6. For x = 20: - U (20) = -e ^ (-0.05 * (20) ^ 0.85) ≈ -0.419

Points to be Plotted: (0.1, -0.995), (1, -0.951), (5, -0.788), (8, -0.696), (10, -0.650), (20, -0.419)



Here is the utility function graph that represents the risk preferences of a company dealing with financial losses due to cyber attacks[16].

While most companies are risk-averse when it comes to cybersecurity, particularly due to the potentially severe consequences of cyber attacks, there are contexts and scenarios where a more risk-seeking approach might be observed. These tend to be driven by factors such as growth ambitions, competitive pressures, and the nature of the industry. In any case, even risk-seeking companies usually aim to strike a balance, ensuring that the potential benefits of taking on additional risk outweigh the possible downsides. This often involves sophisticated risk management strategies and contingency planning[17].

7. DISCUSSION:

The risk analysis technique identifies the most serious vulnerabilities in cloud computing, focusing on confidentiality, integrity, and availability risks. Key findings show that insufficient security controls and weak safeguards result in data leaks, breaches, external attacks, and insider risks, while poor data segmentation, user access management, and data quality issues compromise integrity. Inadequate change management, DoS assaults, physical disturbances, and inefficient recovery methods all contribute to availability issues. Although comprehensive, the analysis has flaws such as data inconsistencies, assumptions, and scope constraints. Future improvements should include enhanced data collection, regular updates, a greater scope, and addressing human problems through training and awareness campaigns to maintain strong cloud security frameworks. Sources cited include BMC Software and NextLabs for in-depth information on these hazards and mitigation techniques.

8. CONCLUSION:

In conclusion, our integrated risk analysis and evaluation provide a thorough understanding of cybersecurity concerns in cloud computing systems. The analysis begins by identifying important cybersecurity threats in cloud environments, which is then followed by a qualitative analysis that provides insights into the nature and effect of these identified risks, as well as the causes for them. Fault Tree and Event Tree Analysis are used to map probable failure sites and event sequences that lead to security breaches. Decision Tree Analysis provides organized frameworks to help make decisions and manage risks effectively. Bayesian analysis uses probabilistic approaches to estimate the possibility of breaches in confidentiality, integrity, and availability. Sensitivity Analysis evaluates how modifications in user access controls affect overall security.The F-N Curve depicts the frequency and severity of incidents in order to better understand and manage risk, whereas the Utility Function demonstrates the company's risk aversion by displaying how utility changes with varying levels of financial loss. This complete study improves the organization's security posture, informs strategic decision-making, and assures long-term resilience to evolving cyber threats. By integrating these techniques, businesses may better secure their cloud environments from possible threats and create effective risk mitigation measures.

9. REFERENCES:

[1] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, "A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies," *IEEE Access*, vol. 9, no. 1, pp. 1–1, 2021, doi: https://doi.org/10.1109/access.2021.3073203.

[2] M. O. Alassafi, Raid Hussein, G. Wills, and Robert John Walters, "Security in organisations: governance, risks and vulnerabilities in moving to the cloud," *ResearchGate*, Jan. 18,2017. **https://www.researchgate.net/publication/316098648_Security_in_organisations_governance_risks_and_vulnerabi**

lities_in_moving_to_the_cloud

[3] Tchernykh, Andrei & Schwiegelshohn, Uwe & Talbi, El-Ghazali & Babenko, Mikhail. (2016). Towards Understanding Uncertainty in Cloud Computing with risks of Confidentiality, Integrity, and Availability. Journal of Computational Science. 36. 10.1016/j.jocs.2016.11.011.

[4] Martens, Benedikt & Teuteberg, Frank. (2012). Teuteberg, F.: Decision-making in cloud computing environments: A cost and risk based approach. Information System Frontiers 14, 871-893. Information Systems Frontiers - ISF. 14. 10.1007/s10796-011-9317-x.

[5]IBM, "What Is a Data Breach?," *IBM*, 2023. https://www.ibm.com/topics/data-breach

[6] T. Ali, M. Al-Khalidi, and Rabab Al-Zaidi, "Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review," ˜*The* œ*Journal of computer information systems*, pp. 1–28, Mar. 2024, doi: https://doi.org/10.1080/08874417.2024.2329985.

[7] "What is Bayesian analysis? | Stata," *www.stata.com*. https://www.stata.com/features/overview/bayesian-intro/

[8] "2023 Cloud Security Report Shows Many Data Breaches - Press Release," *cpl.thalesgroup.com*, Jul. 05, 2023. https://cpl.thalesgroup.com/about-us/newsroom/2023-cloud-security-cyberattacks-data-breaches-press-release

[9] Verizon, "DBIR Report 2024 - Summary of Findings | Verizon," *Verizon Business*, 2024. https://www.verizon.com/business/resources/reports/dbir/2024/summary-of-findings/

[10]IBM, "Cost of a Data Breach 2023," *IBM*, 2023. https://www.ibm.com/reports/data-breach

[11] Shondel, C., & Bartholomew, P. (2021). (ISC)² CISSP Certified Information Systems Security Professional Official Study Guide. John Wiley & Sons, Incorporated. (Chapter 13: Cloud Security)

[12] PricewaterhouseCoopers, "Cloud attacks are top cyber risk concern: PwC 2024 Global Digital Trust Insights," *PwC*. https://www.pwc.com/bm/en/press-releases/pwc-2024-global-digital-trust-insights.html

[13] C. Jones, "50 Cloud Security Stats You Should Know In 2022," *Expert Insights*, Jun. 14, 2021. https://expertinsights.com/insights/50-cloud-security-stats-you-should-know/

[14]"75+ Surprising Cloud Security Statistics You Should Know in 2024," Apr. 10, 2024. https://www.stationx.net/cloud-security-statistics/

[15] "The dark side of the cloud: How cloud is becoming prey to sophisticated forms of cyber attack," *Business Today*, Aug. 08, 2023. https://www.businesstoday.in/magazine/deep-dive/story/the-dark-side-of-the-cloud-how-cloud-is-becoming-prey-to-sophisticated-forms-of-cyber-attack-393051-2023-08-08

[16] S. Madnick, "Why Data Breaches Spiked in 2023," *Harvard Business Review*, Feb. 19, 2024. https://hbr.org/2024/02/why-data-breaches-spiked-in-2023

[17] Dr.M.Amayri (Summer 1 2024). Risk Analysis INSE 6320 [PowerPoint slides]. Moodle. https://moodle.concordia.ca/moodle/course/view.php?id=165727

[18] Arogundade, Oluwasanmi. (2024). Strategic Security Risk Management in Cloud Computing: A Comprehensive Examination and Application of the Risk Management Framework. 11. 45-55. 10.17148/IARJSET.2024.11105.