**Cloud Computing Security Issues of Sensitive Data**

Harshal Thaware
*Dept of M. C. A.*
*Finolex Academy of Management and Technology*Ratnagiri, India
harshalthaware9049@gmail.com

Siddhivinayak Thorat
*Dept of M. C. A.*
*Finolex Academy of Management and Technology*Ratnagiri, India
siddhivinayakthorat29@gmail.com

**ABSTRACT**

Cloud computing is very advantageous for storing and processing sensitive data owing to evolvements, such as scalability, flexibility, and overall cost reduction. But, indeed, there are considerable doubts about data security in cloud systems. This research presents an inclusive review of the concerns related to storing and processing sensitive data in cloud environments. Specifically, this paper discusses the main risks, which are data breaches, unauthorized access, data loss, and compliance concerns. In turn, regarding countermeasures, the paper overall explains the most effective means for tackling security issues, which are encryption, access restrictions tools, data masking, and monitoring. Finally, the paper articulates recent trends and solutions, including homomorphic encryption and confidential computing.

The current abstract addresses sensitive cloud computing security issues. The need for the current paper is boosted by the increasing occurrence of cloud computing that significantly influences the process of data storage and access. However, such changes also enhance the possibility of sensitive data breaches due to a lack of appropriate security measures. The abstract focus is described in the following way.

The following paper is dedicated to the most critical issues of protecting sensitive data in cloud execution. By presenting a range of measures that are used nowadays to address these problems, such as encryption, access management, data localization, and compliance checking, and analysing the information provided by other researchers, the proposed paper can add to the knowledge available for those who conduct investigations and work on improving the performance and safety of sensitive data in cloud condition.

**Keywords -** Cloud computing, security Issue

1. **INTRODUCTION**

In short, cloud can be described as various kinds of services that we can access using an Internet connection. Microsoft, Amazon, Google and many more provide cloud services in which users are enabled to pay for a service-based subscriptions or consumption. Some of these services include Messaging, Social, Storage, CRM, Identity, and Content request Focus; Cloud computing makes it easier to use by subverting early computer behaviour’s and the techniques it offers overcomes the agility performance of traditional computers by several seconds.

Cloud computing is also known as "the cloud". Since its success hinges on resource sharing to enable convergence and scale economies, Cloud computing allows application software to be operated using internet-enabled devices, it offers storage, and file backup of all applications. It also supports multiple users working on a document for different sort of jobs, so collaboration is improved.Cloud computing that although its advantages, it also it at risk of being exposed to cloud security threats. For instance, botnets can be used to spread spam and malware A 2011 survey by the security systems supplier Symantec Corp. stated that nearly 73% of more than 2,000 small and medium businesses had been previously targeted with a cyber-attack. According to a post for The Wall Street Journal, a study conducted by the U.S. Secret Service in 2010 found that 63% of the 761 data breaches it had investigated that year took place at small- to medium-sized businesses with 100 or fewer employees.

In the evolution of distributed systems, it is a novel trend that cloud computing displays. It gives you abstraction, you should not have to know or be an expert to drive the cloud infrastructure. Common business applications delivered through the cloud service include online storage, email, and customer relationship management (CRM) to network security management solutions. This has changed the way businesses work because it has enabled to be resources to come at a cheaper price and has made them available for organizations of all sizes.

1. **CLOUD COMPUTING MODELS**

Cloud hosting deployment models are classified by proprietorship, size, and access, which determine the nature of the cloud. Most organizations are willing to implement cloud computing because it reduces expenditure and controls operational costs.

1. **SECURITY ISSUES**

The advent of cloud computing has transformed the way organizations operate as now an enormous amount of data can be stored, processed and managed through it in ways that were never possible before. This has made it an enticing proposition to businesses operating in different sectors, due to its scalability, accessibility, and cost-effective nature. These benefits, however, are accompanied by serious security concerns and threats that organizations need to deal with — after all, the digital content stored in the data should be kept secure and away from unauthorized eyes as much as possible.In this piece, we will focus on the various security problems within cloud computing. Not only this, but these vulnerabilities can be the very reason for the breach to happen or they could be targeted-breach on the cloud systems.

**3.1 Threats in Cloud Computing**Cloud computing is vulnerable to various threats, including:**3.1.1 Compromised Credentials and Broken Authentication**One of the most significant security risks in cloud computing is compromised credentials and broken authentication. This occurs when organizations fail to manage user identities and access permissions effectively. For instance, when an employee leaves the organization, their access permissions may not be revoked, leaving the door open for unauthorized access. Moreover, developers often embed credentials and cryptographic keys in source code, making it vulnerable to hacking. The Anthem breach, which exposed over 80 million customer records, is a prime example of the consequences of compromised credentials.**3.1.2 Data Breaches**Cloud environments are attractive targets for hackers due to the large amount of data stored on cloud servers. Data breaches can have severe consequences, including legal action, breach investigations, and customer notifications, which can result in significant costs. Moreover, data breaches can lead to brand damage and loss of business, impacting an organization's future for years.**3.1.3 Hacked Interfaces and APIs**Cloud services and applications offer APIs, which are used by IT teams to manage and interact with cloud services. However, these APIs can be vulnerable to hacking, exposing organizations to security risks such as confidentiality, accountability, and availability issues. Third-party reliance on APIs can further increase the risk of security breaches.**3.1.4 Exploited System Vulnerabilities**Multitenancy in cloud computing creates new attack surfaces, making it easier for hackers to exploit system vulnerabilities.

**3.1.5 Account Hijacking**Cloud services add a new dimension to account hijacking, making it easier for attackers to eavesdrop on activities, manipulate transactions, and modify data. Phishing, fraud, and software exploits are highly prevalent, and organizations must prohibit sharing of account credentials between users and services. Multifactor authentication schemes can help prevent account hijacking.

**3.1.6 DoS Attacks**DoS attacks have been around for a long time and have gained prominence again thanks to cloud computing. These attacks can affect availability, causing systems to run slow or time out.

1. **LITERATURE REVIEW**

Cloud computing has revolutionized the IT landscape by offering on-demand access to a shared pool of configurable computing resources. This paradigm shift has been extensively studied in the academic and industrial domains. Armbrust et al. (2009) described cloud computing as a model that enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources, which can be rapidly provisioned and released with minimal management effort.

Studies have highlighted both the benefits and the challenges associated with cloud computing. According to Mell and Grance (2011), the primary advantages include cost savings, flexibility, scalability, and improved disaster recovery. Kandukuri et al. (2009) identified key security issues such as data breaches, loss of control over data, and challenges in data privacy. Another crucial aspect is compliance with legal and regulatory requirements, which can be complex in cloud environments due to the distributed nature of data storage (Subashini & Kavitha, 2011).

Jamil and Zaki (2011) discussed several security countermeasures, including the use of advanced encryption techniques, robust identity and access management (IAM) systems, and continuous monitoring for anomalies. These measures are critical for maintaining the integrity and confidentiality of data in cloud environments. Additionally, recent advancements in cloud security, such as homomorphic encryption and blockchain technology, offer promising solutions for enhancing data security and privacy.

1. **PROBLEM DEFINITION**

Despite the numerous benefits of cloud computing, its adoption brings significant security challenges that threaten the integrity, confidentiality, and availability of data. The multi-tenant nature of cloud environments means that multiple users share the same physical infrastructure, increasing the risk of data breaches and unauthorized access. Additionally, the dynamic and scalable nature of cloud resources complicates the implementation of consistent security measures.

Organizations face risks such as data breaches, where sensitive information can be accessed by unauthorized entities, and data loss, which can occur due to system failures or malicious attacks. The potential for service disruptions also poses a significant threat, impacting business continuity and operations. Furthermore, compliance with regulatory requirements becomes more complex in cloud environments, where data may be stored across multiple geographic locations with varying legal frameworks.

1. **OBJECTIVE/SCOPE**

The primary objective of this research is to identify and analyse the key security challenges associated with cloud computing and propose effective countermeasures. The scope of this study includes an examination of various cloud deployment models (public, private, hybrid, and community clouds) and their respective security concerns. This research aims to evaluate existing security frameworks and propose improvements to enhance data protection, access control, and overall system integrity. Additionally, the study will explore advanced security technologies and practices that can be implemented to mitigate the identified risks.

1. **RESEARCH METHODOLOGY**

This research employs a qualitative approach, combining literature review and case study analysis to explore cloud computing security issues. The literature review encompasses a wide range of sources, including academic journals, industry reports, and standards from organizations such as NIST and ISO. This review aims to gather insights into the current state of cloud security and identify gaps in existing knowledge.

The case study analysis focuses on real-world incidents involving cloud security breaches, examining the causes, impacts, and mitigation strategies. Examples include the Sony PlayStation Network breach in 2011, where attackers exploited vulnerabilities in the network to gain access to personal information of millions of users, and the Capital One data breach in 2019, where a misconfigured firewall allowed unauthorized access to sensitive data stored in Amazon Web Services (AWS).

By integrating findings from both literature and case studies, this research aims to develop a robust understanding of cloud security challenges and propose actionable recommendations. The research methodology also includes interviews with cloud security experts to gain practical insights and validate the proposed solutions.

1. **ANALYSIS & FINDINGS**

The analysis reveals several critical security issues in cloud computing. Data breaches and unauthorized access are the most prominent threats, often resulting from weak authentication mechanisms and insufficient encryption practices. For instance, the Capital One breach highlighted the importance of proper configuration and monitoring of cloud resources to prevent unauthorized access.

Network-related vulnerabilities, including Distributed Denial of Service (DDoS) attacks and SQL injection attacks, pose significant risks to cloud environments. These attacks exploit weaknesses in network protocols and application security, leading to data loss and service disruptions. The analysis of the Sony hack demonstrates the severe consequences of inadequate network security measures, where attackers exploited vulnerabilities in the system to steal sensitive user information.

The findings underscore the necessity for comprehensive security frameworks that encompass robust encryption, strong access controls, and continuous monitoring of cloud environments. Encryption techniques, such as homomorphic encryption, can protect data even when it is being processed, while blockchain technology can enhance data integrity and transparency.

1. **LIMITATIONS & FUTURE SCOPE**

The study acknowledges certain limitations, including the rapidly evolving nature of cloud technologies, which may render some findings obsolete. Additionally, the research focuses primarily on security issues, potentially overlooking other critical aspects of cloud computing such as performance and cost efficiency. Future research should aim to address these limitations by incorporating a broader range of factors and exploring the intersection of security with other cloud computing concerns.

Furthermore, the development of advanced security solutions, such as machine learning-based threat detection and blockchain for enhanced data integrity, represents a promising area for future exploration. Machine learning algorithms can analyse large volumes of data to identify patterns and anomalies, enabling proactive threat detection and response. Blockchain technology can provide a decentralized and tamper-proof ledger for recording transactions and verifying the integrity of data.

1. **CONCLUSION**

Cloud computing offers significant benefits, including cost savings, scalability, and flexibility. However, it also introduces substantial security challenges that must be addressed to ensure safe and reliable operation. This research highlights key security issues such as data breaches, unauthorized access, and network vulnerabilities, and proposes effective countermeasures. The adoption of robust encryption, strong authentication, and continuous monitoring are critical for mitigating these risks.

By understanding and addressing the security challenges in cloud computing, organizations can leverage its benefits while safeguarding their data and resources. Future research should continue to explore advanced security technologies and practices to stay ahead of emerging threats and ensure the continued trust and reliability of cloud computing services.

1. **REAL TIME REFERENCES**
2. "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance" by Tim Mather, Subra Kumaraswamy, and Shahed Latif
3. "Cloud Computing Security: Foundations and Challenges" by John R. Vacca
4. "Cloud Computing: Concepts, Technology & Architecture" by Thomas Erl, Ricardo Puttini, and Zaigham Mahmood
5. "Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS)" by Michael J. Kavis
6. "Security, Privacy and Trust in Cloud Systems" edited by Surya Nepal and Mukaddim Pathan
7. **"Securing the Cloud: Cloud Computer Security Techniques and Tactics"** by Vic (J.R.) Winkler
8. **"Cloud Security: A Comprehensive Guide to Secure Cloud Computing"** by Ronald L. Krutz and Russell Dean Vines
9. **"Data Security in Cloud Computing"** by Vimal Kumar, Arvind Negi, and Hemant Kumar Singh
10. **"Cloud Computing Security: Foundations and Challenges"** edited by John R. Vacca
11. **"Practical Cloud Security: A Guide for Secure Design and Deployment"** by Chris Dotson
12. **"Applied Cloud Security: A Practical Guide to Securing Public Cloud Services"** by Michael J. Chapple
13. **"Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance"** by Tim Mather, Subra Kumaraswamy, and Shahed Latif
14. **"Building the Infrastructure for Cloud Security: A Solutions View"** by Ravi Das and Thomas A. Peters
15. **"AWS Security Best Practices"** by Albert Anthony
16. **"Cloud Computing Security: From Strategy to Practice"** edited by Bruno Crispo and Fabio Massacci
17. **"Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance"** by Tim Mather, Subra Kumaraswamy, and Shahed Latif
18. **"CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security"** by Raj Samani, Brian Honan, and Jim Reavis
19. **"Cloud Security Auditing"** by Suryadipta Majumdar, Sudip Misra, and Subhankar Dhar
20. **"Cloud Security For Dummies"** by Ted Coombs
21. **"Hands-On Cloud Solutions with Azure: Architecting, developing, and deploying the Azure way"** by Greg Leonardo
22. **"Network Security in Virtualized Data Centers For Dummies"** by Lawrence Miller and James Pinto
23. **"Cybersecurity for Executives: A Practical Guide"** by Gregory J. Touhill and C. Joseph Touhill
24. **"Zero Trust Networks: Building Secure Systems in Untrusted Networks"** by Evan Gilman and Doug Barth
25. **"Cloud Security: Strategies, Concepts, and Solutions"** by Ramgovind S., Eloff M.M., and Smith E.
26. **"Applied Network Security Monitoring: Collection, Detection, and Analysis"** by Chris Sanders and Jason Smith
27. **"Cloud Computing: Implementation, Management, and Security"** by John W. Rittinghouse and James F. Ransome
28. "Cloud Security Alliance: Top Threats to Cloud Computing" <https://www.cloudsecurityalliance.org/top-threats/>
29. "NIST Cloud Computing Security Reference Architecture" <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-299.pdf>
30. "ENISA Cloud Computing Security Risks" <https://www.enisa.europa.eu/publications/cloud-computing-security-risks>
31. "OWASP Cloud Security Project" <https://owasp.org/www-project-cloud-security/>