International Journal of Research Publication and Reviews

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

Understanding Cloud Outages and Security Breaches.

Soham Shah

Department of Information Technology & Computer Science
SK Somaiya College, Somaiya Vidyavihar University
Mumbai - 400077, India
Email: soham27@somaiya.edu

ABSTRACT :

Cloud computing refers to the on-demand provision of computing services, wherein applications and infrastructure are delivered to users as metered services over networks. This model is financially advantageous because it eliminates the need for users to invest in physical hardware. As a modern technology, cloud computing provides services such as online business applications and data storage accessible via the Internet. Embracing cloud technology supports a distributed work environment, lowers organizational expenses, and improves data security. However, as more organizations migrate to the cloud, cybercriminals are increasingly targeting these systems to gain unauthorized access to valuable information. The shift from traditional computing to cloud-based systems has introduced numerous security challenges for both customers and service providers. Even reputable cloud providers offer a variety of services through different technologies, which consequently exposes them to a range of security threats. This paper examines cloud security concerns, including various threats and attacks, and aims to offer valuable insights for security professionals involved in developing and managing cloud infrastructure.

Keywords- Security, Cloud Computing Security, Authentication, Organizations, Virtualization, Encryption, Data privacy protection.

Introduction :

Cloud computing has attracted widespread attention for its key advantages, including flexibility, scalability, reliability, sustainability, and cost-efficiency (Varghese & Buyya, 2017; Vasiljeva, Shaikhulina, & Kreslins, 2017). Its pay-per-use model has become appealing to both individuals and businesses, offering an innovative way to increase profitability (Becker et al., 2017; Bohn et al., 2011; Weinman, 2018)[1]. A 2020 survey of 750 cloud professionals revealed that, due to the impact of COVID-19, organizations planned to boost their cloud spending by 47% in 2021. Moreover, critical sectors like IT, machine learning/AI, data warehousing, and serverless computing are projected to see an average growth rate of 47.2% (Bahrami & Singhal, 2015).

Despite intense competition among leading tech companies such as Google, Microsoft, and IBM to deliver cloud computing solutions, there is still a pressing need for further research into effective security strategies (Kaur et al., 2018; Kumar & Goyal, 2019; Zissis & Lekkas, 2012). Cloud computing provides customers with virtualized resources through various technologies, including web services and virtualization, all accessed over the Internet (Flexera, 2020). Web applications are crucial for managing and accessing these cloud resources, making them integral to the cloud computing ecosystem (Bahrami & Singhal, 2015)[2]. However, while virtualization offers numerous advantages by enabling multiple users to share the same physical hardware in a multi-tenant environment, it also introduces notable security risks.

The key advantages of cloud computing are its elasticity, allowing Software as a Service (SaaS) providers to dynamically scale resources according to demand, ensuring that costs are only incurred for actual usage. Although cloud computing offers numerous solutions with a focus on security, it still encounters significant challenges. As the adoption of cloud technology increases, security concerns continue to pose a threat. Organizations must carefully choose secure infrastructures when transferring data to remote locations. According to NIST, the primary hurdles to cloud adoption are related to security, portability, and interoperability.

In 2009, numerous companies voiced increasing concerns about cloud security challenges[3]. The International Data Corporation (IDC), a market research and analysis firm, offered recommendations to Chief Information Officers (CIOs) regarding the most significant security vulnerabilities. Survey findings indicated that 87.5% of respondents prioritized security as their main concern. Due to the risks involved in storing sensitive data within cloud environments, many organizations were reluctant to transfer critical information to remote cloud storage systems (Armbrust et al., 2009).

For achieving the high-level security and privacy of related data and services, cloud service provider settles a Service Level Agreement (SLA) to the cloud consumers. But unfortunately, there is no standard procedure to design an SLA. The paper (Kandukuri et al., 2009) describe an SLA report related to the provided services, which is helpful for consumers and provider both. But, these SLA reports do not completely fulfill the consumer losses.

Many cloud providers, including Google, Amazon (2015), and Salesforce, do not provide complete SLAs that fully ensure the security of user data and often omit several key service-related parameters. A notable example is Amazon Elastic Cloud Computing (EC2) (Amazon, 2015), which offers virtual hardware abstraction to its users, addressing various types of failures such as hardware, software, and operator node failures. In the future, researchers have introduced an SLA model for Google App Engine (Google, 2015) that covers all failure scenarios, providing a more comprehensive approach to service reliability.

Determining the appropriate number of resources for a cloud service during execution is challenging, as it depends on the service's current workload. Since users access cloud services provided by SaaS vendors unpredictably, these services often experience workload fluctuations. Such fluctuations can result in two undesirable scenarios: over-provisioning and under-provisioning. Over-provisioning occurs when more resources than necessary are allocated for a cloud application, which, while meeting the terms of the SLA, leads to unnecessary costs for both the user and the provider. In contrast, under-provisioning arises when fewer resources than required are allocated, causing SLA violations that result in lost revenue and dissatisfied users.[4] Therefore, an effective elasticity mechanism must accurately estimate resource needs based on the current workload to maintain SLA compliance and efficiency. Complex encryption algorithms are not friendly resources-limited users, so it is a practical problem to ensure that they can operate on their own devices. In addition, it should be high probability for user's devices to be under the side channel attack is very high.

In summary, the data security and privacy-preserving in cloud storage system mainly faced with the following challenges:

- Fine-grained data access control.
- Malicious cloud service providers may return incorrect integrity audit results.
- Side channel attack.
- Malicious cloud service providers do not comply with customers' requests to completely delete data in the cloud.
- Privacy-preserving.

Although cloud storage has developed for many years, it is still very important in the Internet of Things, smart city and digital economy. Data security[5] and privacy protection in cloud storage are still of great importance, which inspires us to present this review. we make a comprehensive review of the literature on data security and privacy issues, data encryption technology, and applicable countermeasures in cloud storage system. The main contributions of this paper are as follows

- We first make an overview of cloud storage, classification, architecture and applications.
- Data encryption technologies and protection methods are summarized. These correspond to the security requirements.
- We discuss several open research topics of data security for cloud storage.
- Also, we will discuss the Recent Crowd strike on cloud service Microsoft

Cloud Security Analysis :

Data in cloud storage is organized in the form of blocks, files, and objects. Ensuring the security of this data can be approached through several key principles: data confidentiality, data integrity, data availability, secure data sharing within groups, and privacy protection [6]

- **Data Confidentiality:** This principle involves safeguarding customer information and computations from both cloud vendors and other users. Ensuring confidentiality is a significant concern in cloud computing, as most cloud servers are managed by third-party providers who may not be trustworthy, raising various security concerns about customer data.
- **Data Integrity:** This refers to the accuracy and consistency of data. Data integrity ensures that customer information stored on the cloud server remains intact and is not subject to loss or unauthorized alterations.
- **Computational Integrity:** This implies that any programs executed in the cloud remain uncompromised by malicious users.
- **Data Availability:** Data availability ensures that cloud services are accessible to customers at all times. Attackers may use Denial of Service (DoS) attacks to disrupt service availability for users.
- **Data Accountability:** This principle involves tracking whether the resources allocated to cloud users comply with specified Service Level Agreements (SLAs).
- **Data Privacy:** Data privacy concerns the protection of customer data stored by cloud providers. Issues arise from the potential for insider threats and untrustworthy servers, which create security concerns related to privacy in cloud computing.

TABLE 1. VARIOUS POSSIBLE ATTACKS IN CLOUD COMPUTING

Compromising Service	Possible Attacks	Issues and Cryptographic solutions
Data Confidentiality	1)Eaves Dropping 2)Information Gathering 3)Traffic Analysis 4)Ping sweeps and port scanning 5)Packet sniffing 6)Emanations capturing	**Issue:** Unauthorized individuals can gain access to the data owner's information. **Solution:** Implement robust encryption and key generation algorithms to protect the data during transmission.
Data Integrity	1) Masquerade	**Issue:** Unauthorized users may

	2) Replay 3)Message suppression / Fabrication / Alteration 4) Sequence Prediction 5) Man-in-the-Middle 6) Attacks IP	perform insertion or deletion operations on the data owner's information. **Solution**: Employ effective data auditability algorithms and error detection and recovery mechanisms.
Access Control	1)Denial of Service 2)Distributed Denial of Service 3)Spoofing 4)Social Engineering	**Issue**: Authorized users may be denied or restricted access to the system. **Solution**: Utilize various access control mechanisms such as Mandatory Access Control (MAC) and Role Based Access Control (RBAC).
User Privacy	1)Cloaking Attacks 2) Inference Attack 3) Link reconstruction attacks 4) Intersection Attack 5)Phishing attack 6) Social worms 7) Spam attacks	**Issue**: Unauthorized users can gain access to sensitive or personal information belonging to users. **Solution:** Implement robust cryptographic keys and identity management algorithms to safeguard the system.
Authentication	1)Password Attacks 2) Dictionary attacks 3) Brute force Attack 4) Hybrid crackers 5) Message Tampering	**Issue:** Unauthorized users may log into the system, gaining access to resources, enforcing policies, and compromising sensitive information. **Solution**: Utilize efficient authentication algorithms, such as digital certificates and RSA-based digital signatures, to enable secure user login to the system.

Objectives

- Analyse common causes of cloud outages, Security Breaches.
- How outages affect cloud-based security controls and possible vulnerabilities
- Identifying best practices and strategies that enterprises can employ to maintain security posture and continuity during cloud service interruptions.

Critical Analysis and Fresh Interpretations

CrowdStrike attacks –

Google Cloud Platform (GCP) BSOD Incident (2018)

In 2018, Google Cloud Platform (GCP) experienced a notable Blue Screen of Death (BSOD) event affecting several virtual machines (VMs) running Windows. This issue was caused by a specific Windows upgrade that led to compatibility problems with GCP's virtualization architecture. As a result, numerous clients faced VM failures and service interruptions. Google promptly addressed the problem by collaborating with Microsoft[7] to resolve the compatibility issues and provided affected clients with guidance on how to remedy the situation, such as rolling back the problematic update or applying specific fixes. This incident highlighted the importance of collaboration between cloud service providers and software developers, as well as the need for thorough testing to prevent such disruptions. In response, Google improved their update distribution processes to minimize the likelihood of similar issues in the future.

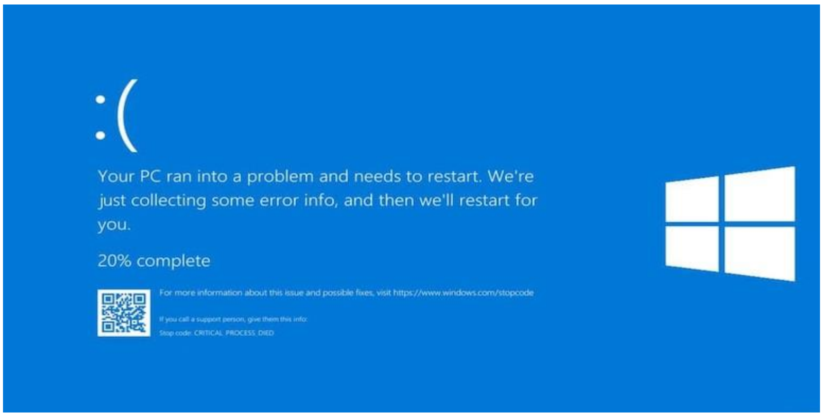
Potential for Recurring Issues:

CrowdStrike Falcon BSOD Incident (2024)

On July 19, 2024, CrowdStrike, a prominent cybersecurity firm, faced a significant setback when it released a flawed update for its Falcon sensor tailored for Windows operating systems. This misstep resulted in widespread system failures, leading to the notorious "blue screen of death" (BSOD) affecting thousands of machines globally. The incident disrupted critical sectors, including banking, airlines, and broadcasting. The root cause of the BSOD was a software bug within the Falcon sensor update that conflicted with Windows kernel components, triggering extensive system crashes. Compounding the problem were inadequate compatibility tests and insufficient quality assurance measures that overlooked various system configurations. The bug created a race condition during specific input/output operations, resulting in erratic system behaviour and crashes.

The immediate repercussions were severe, with organizations experiencing significant downtime, which tarnished CrowdStrike's reputation and incurred hefty costs for recovery efforts and potential customer compensation. In a swift response, CrowdStrike rolled back the faulty update, deployed emergency patches, and worked diligently to restore systems to stable operation. They enhanced customer support by establishing dedicated helplines and providing detailed recovery guides. Additionally, the company undertook a comprehensive review of its development and quality assurance protocols, instituting more rigorous testing procedures, including automated tools and simulation environments, to prevent recurrence of similar issues. Transparent communication with customers—including regular updates—helped to alleviate reputational damage. This incident emphasized the critical need for thorough testing, a deep understanding of customer impact, and continuous enhancements in quality assurance processes

Fig 1. Blue Screen of Death-BSOD



:(

Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

20% complete

For more information about this issue and possible fixes, visit https://www.windows.com/stopcode

If you call a support person, give them this info:
Stop code: CRITICAL PROCESS DIED

Blue Screen of Death (BSOD)

The Blue Screen of Death (BSOD) is a critical error screen that appears on Windows systems (refer to Fig 1.) when a severe system issue arises. This error is serious enough to render the operating system unable to function safely. The BSOD details the specific fault that led to the crash, allowing both users and IT professionals to pinpoint and address the underlying problem. Understanding the significance of the BSOD is crucial, especially in light of recent Microsoft service interruptions that have had a global impact on users and organizations alike.

Impact of BSOD

When a Blue Screen of Death (BSOD) error occurs, the approach to troubleshooting may differ depending on the system and the specific cause of the problem. One strategy is to systematically document and assess the components connected to the industrial computer, helping to pinpoint any defective parts or interfaces. Another technique involves establishing a VNC connection to a virtual machine, which can aid in resolving issues when login difficulties arise. Additionally, using a troubleshooting system that collects fault data, transmits it to a server, and provides a structured resolution plan can enhance the efficiency of addressing the problem. In wireless communication scenarios, troubleshooting may necessitate accessing various base stations based on bandwidth allocations, along with gathering related information for future analysis and problem-solving. By utilizing these diverse troubleshooting methods derived from research, users can effectively tackle BSOD errors through a methodical analysis and targeted interventions.

Capital One breach (2019)

In 2019, Capital One experienced a significant data breach when a hacker took advantage of a vulnerability stemming from a misconfigured firewall in the company's Amazon Web Services (AWS) cloud infrastructure. This misconfiguration granted unauthorized access to a cloud storage system containing sensitive customer data. As a result, the breach exposed 106 million credit card applications and records, including personal details such as names, addresses, credit scores, and Social Security numbers.

This incident underscores the dangers associated with cloud misconfigurations, where even minor setup errors in firewalls or access controls can lead to substantial data exposure. Implementing proper security protocols, conducting regular audits, and monitoring systems could have potentially prevented the breach by identifying the vulnerability earlier.

The hacker exploited this configuration flaw to access sensitive data without needing legitimate credentials. The 2019 Capital One breach stands out as one of the most significant cybersecurity incidents, compromising the personal information of over 100 million individuals. Cyberattack reports often attribute such breaches to isolated errors, such as an employee clicking on a phishing link or failing to update software, suggesting that a single person is to blame. However, this view oversimplifies the issue. Ignoring broader managerial and organizational shortcomings leaves the system exposed to future threats.

Through our Cybersafe analysis methodology, we identified failures at various levels, including technical controls, top management, the Board of Directors, and even government regulators. Our analysis reconstructs Capital One's hierarchical cybersecurity framework, identifies the failures, and provides recommendations for improvement. This work demonstrates how to uncover the root causes of security breaches in complex systems and proposes systematic cybersecurity enhancements that other organizations can adopt. Additionally, it offers a framework for individuals to evaluate and strengthen their organization's security measures.

Cloud Computing Vulnerabilities [8] Table 2.

ID	**Vulnerabilities**	Description
V01	Insecure interfaces and APIs	Cloud service providers deliver services accessible through APIs (SOAP, REST, or HTTP with XML/JSON)[42]. The overall security of the cloud is contingent upon the security of these interfaces. Notable concerns include: a) Poor input validation b) Inadequate authorization checks
V02	Unlimited Resource Allocation	Data from unknown owners can be allocated without restrictions, leading to potential security and ownership issues.
V03	Data vulnerabilities	a) Incomplete data b) Security and data integrity may be compromised due to backups handled by untrusted third parties.
V04	Related Virtual Machines	a) Uncontrolled Migration b) Plain text data

Table 3 demonstrates how threats can exploit vulnerabilities to compromise a system, emphasizing the relationship between these factors. The analysis seeks to pinpoint existing defenses that can mitigate such threats. Misuse patterns provide insight into how attackers take advantage of vulnerabilities. For instance, an attacker may access or modify VM state files during live migration due to the insecure nature of data transfers over networks like the Internet. To combat this issue, several techniques have been suggested: TCCP guarantees secure and confidential execution and migration of VMs, while PALM provides a secure migration system operating within a VMM-protected environment. Another threat arises when attackers create malicious VM images containing viruses or malware, which is feasible since any user can create and upload VM images to a provider's repository for others to download. To address this risk, the Mirage image management system has been developed, featuring an access control framework, image filters, provenance tracking, and repository maintenance to enhance security management.

Threats in cloud computing, Table 3

Threat	**Vulnerabilitie*s***	**Incidents**	**measures**
T01	V01	Utilization of the victim's account to gain access to the target's resources.	IAM Guidance
T02	V03	Data from hard drives shared among multiple customers cannot be effectively removed.	Establish data destruction strategies within Service Level Agreements (SLAs).
T03	V04	Confidential data from other virtual machines on the same server could be accessed.	Implement encryption and digital signatures to protect sensitive information and maintain its security.
T04	V01, V02	An attacker may request additional computational resources.	Cloud providers can enforce policies to prevent such requests.
T05	V01	Command	Implement web

		injection and cross-site scripting.	application scanning tools.

Maintaining Security Posture

Step 1: Classification

The first step in risk assessment is to categorize the information system and its data, focusing on how it processes, stores, and transmits information. This classification is performed through a system impact analysis that assesses the system's importance and its potential impact on the organization. Additionally, this phase involves identifying operational, performance, security, and privacy requirements to create a foundation for security controls. The importance of this classification process is highlighted by Akinrolabu et al. (2019) and Amini & Jamil (2018) [9]

Step 2: Selection

After completing the categorization phase, the subsequent step is to select the initial set of security controls, known as baseline security controls. These controls are identified based on recognized best practices and standards but should be adapted to the unique risks and circumstances of the cloud environment. This adaptation takes into consideration the organization’s risk assessment and operational context. Furthermore, a strategy for ongoing monitoring of the effectiveness of these controls is established. The selected controls are documented in a detailed security plan, which is then reviewed and approved, as noted by Akinrolabu et al. (2019) and Amini & Jamil (2018).

Step 3: Implementation of Security Controls

This phase involves putting the selected security controls into action within the cloud environment. It includes both technical and procedural strategies aimed at effectively mitigating the identified vulnerabilities and weaknesses.

Step 4: Assessment of Security Controls

After implementation, it is crucial to evaluate the effectiveness of the security controls based on the procedures specified in the assessment plan. This assessment is vital for confirming that the controls have been correctly applied and are fulfilling their intended objectives. Additionally, it aids in identifying and rectifying any gaps or deficiencies in the implementation of the controls.

Step 5: Authorization of Operations

The last phase focuses on approving the operation of the information system. This essential stage involves a comprehensive assessment of the risks associated with the system's functioning. The decision-making process evaluates the potential impact on organizational operations, assets, individuals, and other stakeholders to determine if the identified risks are manageable or if additional mitigation measures are necessary.

Risk Identification, Types of Risks in cloud computing

Table 4

RI1	Data breaches
RI2	Unauthorized access
RI3	Service outages
RI4	Vendor lock-in
RI5	Compliance violations

Data Breaches

Data breaches happen when unauthorized individuals access sensitive information stored in cloud systems. Such breaches may arise from vulnerabilities in the cloud infrastructure, poor encryption practices, or weaknesses in security protocols. To effectively address data breaches, it is essential to implement robust security measures, including advanced encryption and continuous monitoring, to prevent unauthorized access and protect sensitive information.

Unauthorized Access

Unauthorized access occurs when individuals access systems or data without the necessary permissions, typically as a result of weak authentication processes or compromised credentials. To mitigate the risk of unauthorized access, organizations must implement strong authentication mechanisms, enforce stringent access controls, and consistently update and monitor security protocols to ensure that only authorized users can access sensitive information.

Insecure APIs (Application Programming Interfaces)

APIs with vulnerabilities or flaws in their design, implementation, or management that can be exploited by attackers to gain unauthorized access, manipulate data, or disrupt services. APIs are essential for enabling communication between software applications, making them vital for web services, mobile apps, and cloud computing. However, if APIs are not properly secured, they pose significant security risks.

Common Security Issues in Insecure APIs:

1. Weak or No Authentication: APIs that do not verify the identity of users properly can allow unauthorized access. Without strong authentication measures, attackers can impersonate legitimate users and access sensitive data.
2. Inadequate Authorization Controls: Even if authentication is present, APIs must ensure that users only access resources they are permitted to. Weak or missing authorization controls can allow attackers to gain access to restricted data or perform actions they should not be able to.
3. Unencrypted Data Transmission: APIs that transmit data without proper encryption (e.g., over HTTP instead of HTTPS) expose sensitive information like passwords and personal data, making it easy for attackers to intercept and exploit the data.
4. Lack of Input Validation: APIs that fail to validate inputs are vulnerable to attacks such as SQL injection, command injection, or cross-site scripting (XSS), allowing attackers to manipulate database queries or run unauthorized commands.
5. Excessive Data Exposure: APIs that provide more information than necessary can lead to data leaks. For instance, an API might reveal internal system details or sensitive user data that attackers can exploit.
6. No Rate Limiting: APIs that lack rate limiting or throttling are susceptible to brute-force attacks or denial-of-service (DoS) attacks. Without limiting the number of requests, attackers can flood the API with numerous requests in a short period.
7. Broken Authentication and Session Management: Improper handling of session tokens or cookies makes APIs vulnerable to session hijacking or replay attacks, allowing attackers to impersonate users.
8. Insecure Third-Party APIs: Applications often rely on external APIs, which can introduce security risks if they are not adequately secured. A vulnerability in a third-party API can compromise the entire application.
9. Misconfigured API Security Settings: Misconfigurations, such as exposing unnecessary endpoints or allowing risky HTTP methods like PUT or DELETE, can open up security holes in APIs.
10. Lack of Monitoring and Logging: Without proper logging or monitoring, it becomes difficult to detect malicious activities or breaches, leading to delayed responses to security incidents.

Service Outages

Service outages refer to disruptions in cloud services that can occur due to a range of factors, such as hardware failures, network issues, or natural disasters. These interruptions can significantly affect an organization’s operations and the availability of its services. To reduce the risk of service outages, it is crucial to implement redundancy measures, establish thorough disaster recovery plans, and engage in proactive monitoring to maintain the continuity and reliability of cloud-based services.

Vendor Lock-In

Vendor lock-in happens when an organization becomes reliant on a particular cloud service provider, making it difficult to transfer data or services to a different provider. This situation can arise from the use of proprietary technologies or restrictive contractual obligations. To prevent vendor lock-in, organizations should negotiate contract terms diligently, advocate for interoperability standards, and develop flexible data migration strategies to minimize dependence on a single provider.

Compliance Violations

Compliance violations occur when an organization does not comply with regulatory requirements or industry standards related to data security and privacy. Such violations can result in legal repercussions and harm to the organization's reputation. To avoid compliance violations, organizations should remain updated on applicable regulations, put in place appropriate security measures, and conduct regular audits of their practices to ensure adherence to compliance standards.

The Causes and Potential Impact of Each Risk [9]

To manage risks in cloud computing effectively, organizations need to possess a thorough understanding of their origins and potential impacts on operations and security. Data breaches may arise from vulnerabilities in cloud infrastructure, weak encryption practices, or insider threats, necessitating the implementation of robust security measures and continuous monitoring. Incidents of unauthorized access can result from poor authentication protocols, compromised credentials, or inadequate access controls, highlighting the need for strong authentication systems and strict access management policies (Amini & Jamil, 2018). Service outages stemming from hardware failures, network disruptions, or natural disaster underscore the critical importance of incorporating redundancy, disaster recovery planning, and proactive monitoring within cloud environments. Furthermore, to mitigate the risks associated with vendor lock-in, organizations should carefully evaluate contract terms, advocate for interoperability standards, and devise effective data migration.

Risk Management

- **Approaches for Mitigating Risks in Cloud-Based Systems**

To effectively manage risks in cloud-based systems, organizations must adopt a comprehensive strategy that includes a range of security measures. There are several key strategies that organizations can implement to mitigate risks associated with cloud computing.

- **Data Protection Through Encryption**

Encryption is a crucial method for protecting sensitive data in cloud environments. It involves the use of robust encryption techniques to maintain data security and confidentiality, even in the event of unauthorized access. Encryption should be implemented at every stage of data management—whether the data is stored, transmitted, or processed. Utilizing strong cryptographic algorithms along with effective key management practices can greatly reduce the risk of data breaches and unauthorized access. This approach is reinforced by research in cloud security, such as the work of Mozumder et al. (2017) [10], which emphasizes the significance of strong encryption for safeguarding data during both transmission and storage.

- **Robust Access Control Strategies**

To reduce the risk of unauthorized access to cloud resources, organizations need to establish strict access control measures. This involves implementing strong authentication techniques, such as multi-factor authentication, to verify user identities when accessing cloud systems. Furthermore, organizations should apply detailed access controls, ensuring that users are granted permissions that align with their roles and responsibilities. Creating a comprehensive identity and access management (IAM) system can centralize user access, provisioning, and authentication, significantly improving overall security (Tissir, El Kafhali, & Aboutabit, 2021)[11]

- **Deployment of Intrusion Detection Systems**

Implementing intrusion detection systems (IDS) is critical for identifying and responding to possible security breaches in cloud environments. IDSs continuously monitor network traffic, system logs, and other pertinent data to detect unusual activities and indicators of compromise. By utilizing sophisticated threat detection methods, including anomaly detection and signature-based detection, organizations can swiftly recognize and respond to security incidents. IDSs are vital for enhancing situational awareness, enabling early detection of security breaches, and mitigating the effects of potential attacks.

- **Disaster Recovery Planning**

Effective disaster recovery planning is critical in cloud computing to mitigate risks associated with service disruptions and data loss. Organizations should develop and implement comprehensive recovery plans that include resilient backup and recovery mechanisms.

Regular data replication and maintaining backup sites in different geographical locations are essential. Additionally, conducting periodic disaster recovery drills helps simulate various scenarios and tests the effectiveness of recovery processes. Investing in robust disaster recovery capabilities ensures operational continuity and minimizes disruptions from unforeseen incidents.

- **Strategies for Effective Vendor Management**

Effective management of third-party cloud service providers is essential for minimizing related risks. Organizations must thoroughly evaluate prospective cloud vendors by reviewing their security protocols, compliance certifications, and incident response capabilities. Establishing clear and transparent service-level agreements (SLAs) is critical for defining the vendor's responsibilities and aligning security goals. Regular performance assessments, security audits, and open communication with vendors are vital for addressing emerging security issues proactively (Al Nafea & Almaiah, 2021).[12]

NIST Cybersecurity Framework :

Founded in 1901, the National Institute of Standards and Technology (NIST) is a federal agency that collaborates with various industries to improve technology, measurement standards, and best practices, although it does not possess regulatory power. In response to the growing need for effective cybersecurity risk management, NIST developed the Cybersecurity Framework (CSF). This framework is designed to align cybersecurity efforts with organizational goals, enabling businesses to incorporate cybersecurity into their overall risk management strategies and processes.

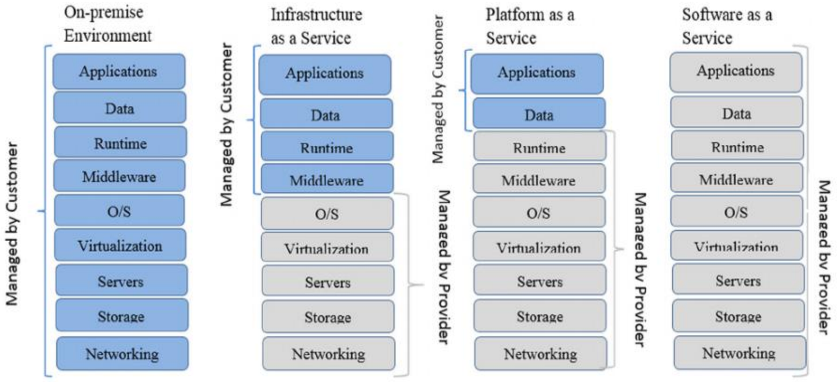


Fig 2. The traditional IT model and Cloud Computing service models

The initial version of the NIST Cybersecurity Framework The Cybersecurity Framework (CSF) was established under Executive Order 13,636 and subsequently updated by the Cybersecurity Enhancement Act of 2014 (CEA). It offers fundamental principles and best practices for managing cybersecurity risks, enhancing the security and resilience of critical infrastructure, regardless of an organization’s size, focus, industry, or location. These practices can be customized to suit the specific objectives and needs of an organization. The framework primarily assists organizations in evaluating their current cybersecurity posture, setting their target state, identifying areas for improvement, measuring progress toward their goals, and effectively communicating cybersecurity risks to both internal and external stakeholders (NIST, 2018).

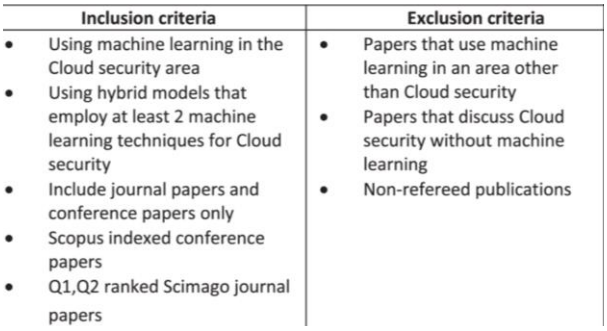
Organizations can utilize the NIST Cybersecurity Framework (CSF) to enhance and communicate their efforts in managing cybersecurity risks or refer to it when developing a cybersecurity program. The framework is comprised of three main components: the Framework Core, Implementation Tiers, and Framework Profile. The Framework Core presents a collection of cybersecurity activities organized into five ongoing and interconnected functions:

Identify, Protect, Detect, Respond, and Recover. Each of these functions has specific categories and subcategories that outline the desired outcomes. These subcategories are backed by Informative References, which include established standards and guidelines such as ISO/IEC 27001, COBIT, NIST SP 800-53, and ISA 62443 (NIST, 2018).

The Implementation Tiers assist in decision-making regarding the management of cybersecurity risks. There are four tiers: Partial, Risk Informed, Repeatable, and Adaptive . These tiers do not denote maturity levels; instead, they reflect progressively more sophisticated approaches to managing cybersecurity risks.[13] Progression through these tiers relies on the formalization of risk management practices, the organization's level of cybersecurity awareness and culture, communication strategies, and cooperation with external partners (NIST, 2018).

Finally, the Framework Profile connects the results of the Framework Core and the chosen tiers with the organization's business objectives, risk tolerance, and available resources. Organizations can utilize this profile to outline their existing cybersecurity status ("Current Profile") and their anticipated future condition ("Target Profile"). By analysing these profiles, organizations can pinpoint gaps and develop a strategy to meet their cybersecurity goals and attain their Target Profile (NIST, 2018).

Fig 3. Inclusion and Exclusion Criteria



Inclusion criteria	Exclusion criteria
• Using machine learning in the Cloud security area • Using hybrid models that employ at least 2 machine learning techniques for Cloud security • Include journal papers and conference papers only • Scopus indexed conference papers • Q1,Q2 ranked Scimago journal papers	• Papers that use machine learning in an area other than Cloud security • Papers that discuss Cloud security without machine learning • Non-refereed publications

Cloud Security Domains

Based on the analysis of the collected research papers, we identified 11 key cloud security topics that are frequently studied. These include anomaly detection, attack detection, data confidentiality, data privacy, denial of service (DoS), distributed denial of service (DDoS), intrusion detection (ID), malware, privacy preservation, and security and vulnerability detection.[14]

Software-Based Attack Vectors:

Many cyberattacks stem from defects, vulnerabilities, and weaknesses in application software, and this issue has worsened with the rise in software-related problems. Key sources of these vulnerabilities include:

a) Input validation failures
b) User access control issues
c) Incomplete or flawed authentication mechanisms
d) Directory traversal vulnerabilities
e) Buffer overflow exploits
f) SQL injection attacks
g) Cross-site scripting (XSS) vulnerabilities
h) Use of components with known vulnerabilities
i) Weaknesses in web services and APIs
j) Insufficient security testing during software development.

Despite significant progress in software development, security testing is often inadequate during both the development and testing stages. This gap is largely due to developers' limited expertise in secure coding practices. Additionally, the deployment of applications across multiple platforms and devices exposes new vulnerabilities, heightening the risk of software-based attacks[15]. For instance, a buffer overflow can allow unauthorized access or lead to data loss, while SQL injection attacks can compromise databases, stealing sensitive information like usernames, passwords, and credit card details. While software updates are a common solution, they don't always fully resolve vulnerabilities and may sometimes introduce new issues.

Current SLA Terms :

The Service Level Agreement (SLA) forms part of the Master Service Agreement and pertains to all services delivered directly to the cloud provider's customers. It does not cover unrelated third parties or individuals without a contractual agreement with the provide. Uptime guarantees, along with any related SLA credits[16], are typically measured on a monthly basis unless stated otherwise. The primary details of the SLA are as follows:

- **SLA Credit Request**: To claim an SLA credit, customers are required to submit a support ticket via email within seven days of the reported outage. The request should provide the service type, IP address, contact details, and a thorough description of the service disruption, including logs if available. SLA credits are provided as service credits applicable to future billing cycles.

- **SLA Claim Violations:** Customers who submit false or repetitive SLA claims will incur a one-time fee of $50 per occurrence. These actions violate the Terms of Service and could lead to service suspension. Furthermore, customers engaged in malicious or aggressive online behavior, which results in attacks or counterattacks, are not eligible for SLA claims and are in breach of the Acceptable Use Policy.

- **Public Network:** The cloud service provider ensures 99.9% uptime for all public network services offered to customers in partner data centers. These services include high-quality, redundant internet connections, advanced intrusion detection systems, DoS mitigation, traffic analysis, and tools for monitoring bandwidth usage.

- **Private Network**: The provider also ensures 99.9% uptime for service network services to customers in partner data centers. These private network services include secure VPN access, unlimited server bandwidth, unrestricted uploads and downloads, access to contracted services, traffic analysis, and comprehensive bandwidth monitoring.

Conclusion:

In conclusion, although cloud computing offers substantial transformative benefits, its security concerns demand ongoing research, innovation, and the implementation of proactive security measures to safeguard data, ensure uninterrupted service, and preserve user confidence in cloud services. The migration to cloud environments introduces a range of security challenges, thoroughly explored in this research, which has examined the main areas of cloud security, focusing on the threats, vulnerabilities, and strategies necessary to maintain robust security frameworks. Noteworthy incidents, such as the CrowdStrike Falcon BSOD issue, underscore the pressing need for comprehensive testing and quality assurance in cloud service management. These events reveal potential vulnerabilities arising from software updates, highlighting the critical importance of collaboration between cloud providers and software developers to prevent security lapses.

To effectively address the risks associated with cloud deployments, organizations must prioritize strong security practices. This involves adopting and adhering to industry standards, regularly updating security protocols, and fostering collaboration between all stakeholders, including cloud service providers, cybersecurity experts, and regulatory bodies. Such a unified approach will ensure the development of resilient cloud security frameworks capable of adapting to evolving threats and challenges.

REFERENCES & CITATIONS:

[1] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," *J. Netw. Comput. Appl.*, vol. 79, pp. 88–115, Feb. 2017, doi: 10.1016/j.jnca.2016.11.027.

[2] M. Bahrami and M. Singhal, "A dynamic cloud computing platform for eHealth systems," in *2015 17th International Conference on E-health Networking, Application & Services (HealthCom)*, Oct. 2015, pp. 435–438. doi: 10.1109/HealthCom.2015.7454539.

[3] "Cloud security issues and challenges: A survey - ScienceDirect." Accessed: Sep. 14, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1084804516302983?via%3Dihub

[4] M. Ghobaei-Arani, S. Jabbehdari, and M. A. Pourmina, "An autonomic resource provisioning approach for service-based cloud applications: A hybrid approach," *Future Gener. Comput. Syst.*, vol. 78, pp. 191–210, Jan. 2018, doi: 10.1016/j.future.2017.02.022.

[5] "Data Security and Privacy Protection for Cloud Storage: A Survey | IEEE Journals & Magazine | IEEE Xplore." Accessed: Sep. 14, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/9142202

[6] "A Detailed Study on Security Services in Cloud Environment | IEEE Conference Publication | IEEE Xplore." Accessed: Sep. 14, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/8057501/authors#authors

[7] S. de Zoysa, "Microsoft global outages caused by CrowdStrike software glitch," Jul. 2024.

[8] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," *J. Internet Serv. Appl.*, vol. 4, no. 1, p. 5, Feb. 2013, doi: 10.1186/1869-0238-4-5.

[9] O. Arogundade, "Strategic Security Risk Management in Cloud Computing: A Comprehensive Examination and Application of the Risk Management Framework," vol. 11, pp. 45–55, Jan. 2024, doi: 10.17148/IARJSET.2024.11105.

[10] D. P. Mozumder, Md. J. Nayeen Mahi, and M. Whaiduzzaman, "Cloud Computing Security Breaches and Threats Analysis," *Int. J. Sci. Eng. Res.*, vol. 8, pp. 1287–1297, Jul. 2017.

[11] N. Tissir, S. El Kafhali, and N. Aboutabit, "Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal," *J. Reliab. Intell. Environ.*, Jun. 2021, doi: 10.1007/s40860-020-00115-0.

[12] R. A. Nafea and M. Amin Almaiah, "Cyber Security Threats in Cloud: Literature Review," in *2021 International Conference on Information Technology (ICIT)*, Jul. 2021, pp. 779–786. doi: 10.1109/ICIT52682.2021.9491638

[13] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 04162018, Apr. 2018. doi: 10.6028/NIST.CSWP.04162018.

[15] F. N. U. Jimmy, "Cyber security Vulnerabilities and Remediation Through Cloud Security Tools," *J. Artif. Intell. Gen. Sci. JAIGS ISSN3006-4023*, vol. 2, no. 1, Art. no. 1, Apr. 2024, doi: 10.60087/jaigs.v2i1.102.
10.6028/NIST.CSWP.04162018.

[16] "Cloud Security Issues | IEEE Conference Publication | IEEE Xplore." Accessed: Sep. 28, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5283911

REFERENCES :

1] Abhishek Bhuva, Dipen Bhuva, A. Hema, D. Anandhasilambarasan, G. Gowri, Mukesh Soni, "Business Clouds Security: Crafting a Contemporary Adoption Framework", *2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*, pp.1-5, 2024.

2] Amira Mahamat Abdallah, Aysha Saif Rashed Obaid Alkaabi, Ghaya Bark Nasser Douman Alameri, Saida Hafsa Rafique, Nura Shifa Musa, Thangavel Murugan, "Cloud Network Anomaly Detection Using Machine and Deep Learning Techniques— Recent Research Advancements", *IEEE Access*, vol.12, pp.56749-56773, 2024.

3] Vineet Joon, Anubhav De, Nilamadhab Mishra, "Study and Investigation of Cloud Based Security Policies Using Machine Learning Techniques", *2024 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC)*, pp.1-6, 2024.

4] Abhay Ajith, Adharsh S Mathew, Remya S, "A Brief Study on Cloud Security", *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, pp.1-7, 2023.

5] A survey paper on cloud computing https://ieeexplore.ieee.org/document/6168399