INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 3 | Issue 3 [2025] | Page 495 – 508

CLOUD SECURITY

- **Abhishek Roy**[1]

ABSTRACT

In the rapidly evolving digital landscape, cyber security has emerged as a critical domain, influencing national security, business integrity, and individual privacy. This paper explores the fundamental principles, evolving threats, and advanced defense mechanisms within cyber security. Cloud computing provides the flexible architecture where data and resources are dispersed at various locations and are accessible from various industrial environments. Cloud computing has changed the using, storing, and sharing of resources such as data, services, and applications for industrial applications. During the last decade, industries have rapidly switched to cloud computing for having more comprehensive access, reduced cost, and increased performance. In addition, significant improvement has been observed in the internet of things (IoT) with the integration of cloud computing. However, this rapid transition into the cloud raised various security issues and concerns.

Cloud computing provides the flexible architecture where data and resources are dispersed at various locations and are accessible from various industrial environments. Cloud computing has changed the using, storing, and sharing of resources such as data, services, and applications for industrial applications. During the last decade, industries have rapidly switched to cloud computing for having more comprehensive access, reduced cost, and increased performance. In addition, significant improvement has been observed in the internet of things (IoT) with the integration of cloud computing. However, this rapid transition into the cloud raised various security issues and concerns.

Key Word's: cyber security, national security, internet of things.

INTRODUCTION OF CLOUD SECURITY

Cloud security refers to the set of policies, technologies, controls, and best practices designed to protect data, applications, and infrastructure that are hosted in cloud environments. As organizations increasingly move their operations and data to the cloud for greater flexibility, scalability, and cost savings, ensuring the security of these resources has become a critical priority.

[1] 4th year law student, Galgotias University, Greater Noida, Uttar Pradesh.

Cloud security[2] aims to safeguard cloud-based assets from a wide range of threats, including unauthorized access, data breaches, cyberattacks, and accidental data loss. This involves implementing measures such as data encryption, identity and access management (IAM), threat detection, disaster recovery planning, and compliance with legal and regulatory requirements.

A unique aspect of cloud security is the shared responsibility model, where both the cloud service provider and the customer have distinct roles in maintaining security. The provider secures the underlying infrastructure, while the customer is responsible for securing their data, applications, and user access within the cloud environment1.

LEGAL AND REGULATORY FRAMEWORK

Cloud security is governed by a complex set of legal and regulatory frameworks designed to protect data, ensure privacy, and maintain trust in cloud environments. These frameworks include international standards, national regulations, and industry-specific guidelines that organizations and cloud service providers [3](CSPs) must follow to ensure compliance and security.

KEY INTERNATIONAL STANDARDS AND FRAMEWORKS

- ISO/IEC: International Standard Organization /International Electrotechnical Commisoon
  An international standard for information security management systems (ISMS), including cloud environments. It provides a systematic approach to managing sensitive information, ensuring confidentiality, integrity, and availability. Certification demonstrates a commitment to robust security practices.
- NIST Frameworks:
  The U.S. National Institute of Standards and Technology (NIST) provides comprehensive guidelines, such as security controls for federal information systems, cloud standards, and security and privacy in public cloud environments. These frameworks are widely used by government agencies and adopted by private organizations to enhance cloud security.
- Cloud Security Alliance (CSA) Controls Matrix:
  CSA offers the Cloud Controls Matrix[4] (CCM) and STAR certification to help

[2] 2009 IEEE International Conference on Cloud Computing
Published: 2009

[3] 2024 International Conference on IoT, Communication and Automation Technology (ICICAT)
Published: 2024

[4] 2013 9th International Conference on Information, Communications & Signal Processing

organizations assess and improve their cloud security posture, and to simplify audits and compliance checks.

MAJOR REGULATORY REQUIREMENTS

- General Data Protection Regulation [5](GDPR): Applies to organizations handling personal data of EU residents, with strict requirements for data protection, privacy, and cross-border data transfers in cloud environments.
- Health Insurance Portability and Accountability Act (HIPAA): U.S. regulation for protecting healthcare data, relevant for cloud services handling sensitive health information.
- Payment Card Industry Data Security Standard (PCI DSS): Mandates security controls for organizations processing payment card data, including those using cloud services.
- Federal Risk and Authorization Management Program [6](FedRAMP): U.S. government program that standardizes security assessment and authorization for cloud services used by federal agencies. certification is mandatory for CSPs working with the government, ensuring high security standards and ongoing monitoring.
- Other Notable Regulations:
    - Sector-specific frameworks like SEBI's guidelines for regulated entities in India

CORE COMPONENTS OF CLOUD LEGAL AND REGULATORY FRAMEWORKS

- Governance:

  Policies for managing cloud assets and configurations to prevent vulnerabilities.

[5] 2014 International Conference on Interactive Collaborative Learning (ICL)
Published: 2014

[6] 2012 7th International Conference on Telecommunication Systems, Services, and Applications (TSSA)

- Change Control: Procedures to ensure security during system changes, often supported by automation.
- Continuous Monitoring: Ongoing logging and monitoring of cloud activity to maintain audit readiness.
- Reporting and Auditing: Documenting compliance and providing evidence for regulatory inquiries.
- Shared Responsibility Model: Security responsibilities are divided between the cloud provider and the customer, emphasizing the need for clear contracts and accountability

CONTRACTS, LIABILITIES AND RESPONSIBILITIES

1. SHARED RESPONSIBILITY MODEL

Cloud security operates under a shared responsibility model, meaning both the cloud service provider (CSP) and the customer have distinct but interconnected duties:

- **Cloud Provider Responsibilities:** The[7] CSP is responsible for securing the underlying infrastructure, including hardware, networks, and physical data centers. For example, AWS, Microsoft Azure, and Google Cloud manage the security of the cloud itself—covering physical security, core networking, and foundational services.
- **Customer Responsibilities:** Customers are responsible for securing their own data, managing user identities, configuring access controls, and ensuring compliance for the applications and workloads they deploy in the cloud. This includes data backup, identity and access management (IAM), audit logging, and training staff to recognize security risks.
- **Division Varies by Service Type:** The split of responsibilities depends on whether the service is[8] Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS).

[7] College of Information Technology, United Arab Emirates University, PO Box 15551, Al Ain, United Arab Emirates

[8] Department of Electrical and Computer Engineering, Newark College of Engineering, New Jersey Institute of Technology, University Heights, Newark, NJ 07102, USA

For IaaS, customers have more control and thus more responsibility; for SaaS, the provider handles more aspects, but customers still manage data and access.

2. CONTRACTS

- **Service Agreements:** Cloud contracts clearly define the roles, responsibilities, and expectations of both parties. They specify the security measures, compliance requirements, and service levels (SLAs) the provider must meet, as well as the customer's obligations to configure and use the services securely.
- **Liability Clauses:** Most cloud contracts limit the provider's liability, often capping it at the fees paid or restricting it to direct damages only. Indirect losses (like regulatory fines or reputational harm) are typically excluded, placing additional risk on the customer.
- **Insurance Requirements:** Contracts may require one or both parties to maintain cyber insurance to cover potential losses from breaches or outages. Customers are encouraged to have their own insurance, as provider coverage is often limited.

3. LIABILITIES

- **Cloud Computing Liability:** Both providers and customers face legal responsibilities and risks, including data breaches, loss of data, service interruptions, and regulatory non-compliance. If a breach occurs due to a provider's failure, the provider may be liable within the contract's limits. If the customer misconfigures security settings or fails to protect credentials, they bear the liability.
- **Risk Management:** Given the limitations in provider liability, customers must proactively manage risks—negotiating contract terms, implementing robust security controls, and maintaining adequate insurance coverage.

PRIVACY AND SURVEILLANCE

Cloud computing introduces significant privacy and surveillance concerns because sensitive personal and business data is stored, processed, and transmitted through third-party infrastructure, often across multiple jurisdictions.

KEY PRIVACY ISSUES

- **Data Location and Control:** Users often do not know where their data is physically stored, which can complicate compliance with privacy laws and make it difficult to control or monitor access.
- **Data Access and Ownership:** Cloud providers and their employees may have technical access to user data, raising concerns about unauthorized use or exposure. Users need assurance that their private information will not be misused by the provider or shared without consent.
- **Data Breaches and Leakage:** Cloud environments are attractive targets for hackers. Data breaches can expose sensitive personal or corporate information, leading to identity theft, financial loss, or reputational harm.
- **Account Hijacking and Insecure APIs:** Weaknesses in authentication or poorly secured [9]APIs can allow attackers to gain unauthorized access, leading to privacy violations and potential surveillance of user activities.
- **Data Sharing and Multi-Tenancy Risks:** Data from multiple organizations may be stored on the same physical hardware, making strong data isolation and encryption essential to prevent accidental or malicious access by other tenants.

SURVEILLANCE RISKS

- **Government and Third-Party Access:** Data stored in the cloud may be subject to lawful access requests by

[9] "Study Analysis of Cloud Security Chanllenges and Issues in Cloud Computing Technologies", Journal of Science, Computing and Engineering Research, 6(8), 06-10, August 2023.

governments or law enforcement in the country where the data resides. This can lead to surveillance concerns, especially if users are unaware of such access or if the laws in the data's location are less protective of privacy.

- **Vendor and Insider Threats:** Cloud providers themselves, or their employees, could potentially monitor user data or activities, intentionally or unintentionally, unless strong privacy policies and technical safeguards are in place.

MANAGING PRIVACY AND SURVEILLANCE RISKS

- **Clear Privacy Policies:** Cloud providers should have transparent privacy rules, disclose how data is handled, and notify customers of any changes. Customers should have the ability to opt out of policy changes where possible.
- **Data Encryption:** Encrypting data both in transit and at rest is critical to protect privacy and reduce the risk of unauthorized surveillance or access.
- **Access Controls and Auditing:** Strong identity and access management, regular audits, and monitoring of data access help detect and deter unauthorized surveillance or data misuse.
- **Regulatory Compliance:** Organizations must ensure that their use of cloud services complies with relevant privacy laws and regulations, including requirements for data localization, user consent, and breach notification

CYBERCRIME AND ENFORCEMENT

Cloud computing has transformed how organizations store and manage data, but it also presents new opportunities for cybercriminals. The concentration of valuable data in the cloud, combined with its accessibility and connectivity, makes cloud environments prime targets for cyberattacks.

COMMON CYBERCRIMES IN THE CLOUD

- **Data Breaches:** Attackers exploit vulnerabilities to access and steal sensitive information, such as personal data, financial records, or intellectual property.

- **Account Hijacking:** Weak passwords, lack of multifactor authentication, and phishing attacks allow criminals to take over cloud accounts and misuse resources.
- **Malware and Ransomware:** Malicious software can be introduced through reckless downloading, unpatched systems, or compromised endpoints, leading to data loss or extortion.
- **Insider Threats:** Employees or contractors with access to cloud systems may intentionally or accidentally compromise security, leading to data leaks or sabotage.
- **Misconfiguration:** Incorrect cloud settings or poor access controls can leave data exposed, making it easy for attackers to exploit vulnerabilities.
- **Third-Party Risks:** Reliance on external vendors can introduce new vulnerabilities if those vendors have weaker security measures.

CHALLENGES IN ENFORCEMENT

- **Decentralized Data:** Cloud data is often stored across multiple locations and jurisdictions, complicating investigations and legal actions.
- **Attribution and Evidence Collection:** Tracing cybercrimes back to specific perpetrators is difficult due to the anonymity and complexity of cloud environments.
- **Jurisdictional Issues:** Different countries have varying laws and enforcement capabilities, making cross-border cooperation essential but challenging.
- **Rapidly Evolving Threats:** Cybercriminals constantly develop new tactics, requiring organizations and law enforcement to stay vigilant and adapt quickly.

BEST PRACTICES FOR PREVENTION AND ENFORCEMENT

- **Strong Access Controls:** Use robust passwords, enable multifactor authentication, and implement role-based access to limit exposure.
- **Regular Updates and Patch Management:** Keep all systems and software up to date to close known security gaps.

- **Data Encryption:** Encrypt data both at rest and in transit to protect it from unauthorized access.
- **Continuous Monitoring:** Employ intrusion detection systems and regular audits to quickly identify and respond to suspicious activity.
- **Employee Training:** Educate staff about phishing, shadow IT, and safe cloud practices to reduce human error and insider threats.
- **Vendor Assessment:** Carefully vet third-party providers to ensure they meet strong security standards.
- **Incident Response Planning:** Develop and test response plans for cloud-specific incidents to minimize damage and support investigations.

CORPORATE AND COMPLIANCE CONCERNS

Cloud computing offers significant benefits but introduces complex compliance and corporate governance challenges. Organizations must navigate a landscape shaped by evolving regulations, diverse standards, and heightened security risks.

KEY CORPORATE AND COMPLIANCE CONCERNS

1. REGULATORY COMPLEXITY AND LEGAL RISKS

- Organizations must comply with a patchwork of international, national, and industry-specific regulations.
- Non-compliance can result in regulatory fines, lawsuits, investigations, and reputational damage.
- Data residency and sovereignty laws require careful attention to where data is stored and processed, especially for multinational operations.

2. SHARED RESPONSIBILITY MODEL

- In the cloud, security and compliance duties are shared between the cloud service provider[10] (CSP) and the custom.

[10] 2021 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA)
Published: 2021

- CSPs are responsible for the security of the infrastructure, while customers must secure their data, applications, and user access.
- Misunderstanding this division can lead to compliance gaps and increased risk exposure.

3. MULTI-CLOUD AND OPERATIONAL COMPLEXITY

- Many organizations use multiple cloud providers, increasing the complexity of maintaining consistent compliance and security across platforms.
- Each provider may have different protocols, certifications, and compliance tools, requiring strong coordination and oversight.

4. SHADOW IT AND DATA MANAGEMENT

- Unauthorized use of cloud services (shadow IT) and untracked data (shadow data) can lead to data loss, increased attack surfaces, and non-compliance.
- Fast-paced adoption of cloud apps makes it difficult to monitor and control all data flows.

5. CONTINUOUS COMPLIANCE MONITORING

- Compliance is not a one-time task; it requires ongoing monitoring, regular audits, and adaptation to new regulations and threats.
- Organizations must implement tools for real-time monitoring, comprehensive logging, and automated compliance checks to stay ahead of risks.

6. VENDOR MANAGEMENT AND LOCK-IN

- Ensuring that CSPs maintain their compliance standards is critical, requiring regular reviews and audits.
- Vendor lock-in and interoperability issues can complicate migrations and disrupt compliance efforts if not managed proactively.

7. OVER-RELIANCE ON PROVIDER SECURITY

- Relying solely on a provider’s certifications or security measures can give a false sense of security.

- High-profile vulnerabilities have shown that even major CSPs can have security gaps, emphasizing the need for organizations to maintain their own compliance and security controls

CASE STUDY

[11]K.S. PUTTASWAMY V. UNION OF INDIA (2017)

Court: Supreme Court of India
Issue: Right to Privacy as a fundamental right
Relevance: Set the foundation for data protection laws, influencing cloud data security norms.

Key Takeaway: Cloud services in India must respect constitutional privacy mandates.

[12]JUSTICE K.S. PUTTASWAMY V. UNION OF INDIA (AADHAAR CASE, 2018)

Court: Supreme Court of India
Citation: (2019) 1 SCC 1
Issue: Constitutionality of Aadhaar and data collection/storage practices.
Relevance to Cloud Security:

- The court upheld Aadhaar but struck down provisions enabling indiscriminate data sharing.
- Stressed data minimization, storage limitations, and security safeguards.

Impact: Set limits on centralized cloud storage of biometric and identity data.

[13]INTERNET AND MOBILE ASSOCIATION OF INDIA V. RESERVE BANK OF INDIA (2020)

Court: Supreme Court of India
Citation: (2020) 10 SCC 274
Issue: Validity of RBI's circular banning cryptocurrency transactions.
Relevance to Cloud Security:

[11] (2017) 1 SCC 1081
[12] (2019) 1 SCC 1
[13] 2020) 10 SCC 274

- While not directly about cloud, it discussed data processing and cybersecurity concerns in emerging technologies.
- The judgment emphasized proportionality and evidence-based restrictions, which apply to cloud data regulation too.

Impact: Cloud-hosted financial services must balance innovation with cybersecurity compliance.

RECOMMENDATIONS

Organizations can address corporate and compliance challenges in cloud computing by adopting a combination of technical, organizational, and legal strategies. Here are key solutions and recommendations:

1. IMPLEMENT STRONG DATA PROTECTION MEASURES

- Encryption: Encrypt sensitive data both at rest and in transit to prevent unauthorized access, even if a breach occurs.
- Access Controls: Use robust identity and access management (IAM) systems, enforce multi-factor authentication, and apply the principle of least privilege to reduce insider and external threats.
- Data Loss Prevention (DLP): Deploy DLP tools to monitor, classify, and control the movement of sensitive data within and outside the cloud environment.

2. ADOPT PRIVACY-BY-DESIGN PRINCIPLES

- Integrate privacy and security considerations into the design and architecture of cloud systems from the outset, rather than as an afterthought[1].
- Regularly audit and monitor cloud environments to identify and mitigate risks proactively.

3. CONTINUOUS COMPLIANCE MONITORING AND AUDITING

- Use automated tools and platforms (such as Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR)) to monitor compliance in real time and streamline incident response[5].
- Schedule regular compliance audits to ensure adherence to relevant laws and standards, such as GDPR, HIPAA, and PCI DSS.

4. CLARIFY ROLES AND RESPONSIBILITIES

- Clearly define and document the division of security and compliance responsibilities between the cloud service provider and your organization, following the shared responsibility model.
- Regularly review and update contracts and service-level agreements (SLAs) to reflect evolving compliance requirements and risk environments.

5. LEVERAGE ADVANCED SECURITY SOLUTIONS

- Deploy solutions like Cloud Access Security Brokers (CASB), Cloud Security Posture Management (CSPM), and extended Detection and Response (XDR) to enhance visibility, automate threat detection, and enforce security policies across multi-cloud environments.
- Use network security tools such as firewalls, intrusion detection/prevention systems, and web application firewalls (WAF) to protect against external threats.

6. EMPLOYEE TRAINING AND AWARENESS

- Conduct regular training for employees on cloud security best practices, data privacy, and compliance obligations to reduce human error and insider threats.

7. VENDOR AND THIRD-PARTY RISK MANAGEMENT

- Assess and monitor the security and compliance posture of all third-party vendors and partners who have access to your cloud data or systems.
- Require vendors to adhere to your organization's security standards and participate in regular security reviews.

8. INCIDENT RESPONSE AND BUSINESS CONTINUITY PLANNING

- Develop and routinely test incident response plans tailored to cloud environments to ensure quick and effective action in case of a breach or compliance incident.
- Establish data backup and disaster recovery protocols to maintain business continuity.

REFERENCES

- https://doi.org/10.1016/j.jnca.2016.11.027
- https://ieeexplore.ieee.org/abstract/document/6248654
- https://ieeexplore.ieee.org/abstract/document/6248654
- https://blog.ipleaders.in/cloud-computing-and-cyber-security-the-interpretation-of-security/
- https://blog.ipleaders.in/how-is-cloud-security-and-privacy-space-evolving-around-the-world/
- https://www.balbix.com/insights/cloud-security/
- https://www.investopedia.com/terms/c/cloud-security.asp
- https://www.scconline.com/
- https://www.esecurityplanet.com/cloud/what-is-cloud-security/