IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

# Google Cloud Platform Threat Detection and Incident Response

**Parool Priya[1] and Bipanshi Sharma[2]**
Department of Computer Science & Applications[1,2]
Sharda School of Computing Science & Engineering, Sharda University, Greater Noida, India

**Abstract**: *Cloud computing is revolutionizing the way organizations store, process, and deal with data through greater scalability, cost-efficiency, and responsiveness than ever before. With this surge of momentum to the cloud, though, also comes the most virulent security threats that have to be addressed seriously in order to safeguard critical data as well as ensure regulatory compliance. This study discusses the shared responsibility model of cloud computing and describes how CSPs and customers share security responsibilities. Important issues like data privacy, integrity, and availability are discussed, as well as typical vulnerabilities such as misconfigurations and unauthorized access. The importance of data protection regulations such as GDPR, HIPAA, and PCI-DSS compliance is also emphasized. The research indicates that organizations need to assess their security roles explicitly in the cloud and have strong controls and policies to minimize risk and guarantee compliance.*

**Keywords**: Cloud Computing, Cloud Security, IAM, Shared Responsibility Model, Zero Trust Architecture, Blockchain, Data Privacy, Access Control, Compliance

## I. INTRODUCTION

Cloud computing has been a transformational technology that provides organizations across industries with the flexibility, flexibility and efficiency they never had before [1], but the widespread use of cloud services, whose many benefits also present security challenges that need to be addressed to protect sensitive information and ensure compliance occurs [2]. It also focuses on compliance, and the importance of data privacy, information, integrity and availability [3].


Figure 1: Key Pillars of Cloud Security Framework

### Shared Responsibility Model

Cloud security has a key part called the shared responsibility model [4]. This part explains how both the cloud service company and the customer need to work together to keep the cloud safe [5]. It's really important for groups that use cloud services to get this [6]. We look closely at how responsibilities are split up, especially in services like software as a service (SaaS) [7]. This helps make clear how these shared responsibility models work and shows what jobs the cloud service companies and customers have when setting up cloud services [8]. Figure 2 shows how security responsibilities are divided between the cloud provider and the customer across different cloud service models—On-Prem, IaaS, PaaS, and SaaS. Dark blue areas represent tasks handled by the customer, light blue by the provider, and half-colored boxes indicate shared duties. As cloud services move from On-Prem to SaaS, more responsibilities shift from the customer to the provider, especially in areas like infrastructure, network, and physical security.


DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67


Figure 2: Shared Responsibility Model in Cloud Computing

**Security Challenges in Cloud Computing**

Cloud computing is great for many reasons, but it also has some security problems [9]. We need to fix these issues to stop hackers, people getting into places they shouldn't, and other online dangers [10]. This part discusses what these security problems are, like when things are not in place properly [11], when the ways computers interact with each other are not secure [12], and when the people inside the company commit malicious acts [13]. Understanding these problems, companies can lock down their cloud technology and defend valuable information [14]. The most common security threats that affect organizations which utilize cloud services can be seen in Figure 3. They include technical threats in the way of DDoS attacks, malware, and data breaches and human error-related problems such as poorly implemented access control or misconfigured cloud storage. It also features threats including insider threats, hijacking, and the utilization of unauthorized applications (colloquially known as Shadow IT). By being aware of these concerns, organizations are able to further take steps to secure their data and systems in the cloud.


Figure 3 : Key cloud security risks to be aware of

*ComplianceRequirements*

Companies that use the cloud must ensure they have numerous rules to safeguard customers' data and privacy [15]. There are the big ones like GDPR, HIPAA, and PCI-
DSS, which have stringent regulations about how data should be treated when stored or transmitted on the cloud [16]. This article discusses why it's actually very important for these kind of companies to follow rules so that
there won't be any problems with the law or with money [17].

**Data Confidentiality, Integrity, and Availability**

When we are using cloud computing, it is actually very important that we are keeping our data safe, correct, and confidential [18]. Information is stored, processed and transmitted in a single joint venture [19]. This chapter highlights the importance of the CIA triangle in cloud-based systems and applications [20] and emphasizes the need for security measures to protect data from unauthorized access, alteration or loss [21]. Through monitoring of personal information, integrity and availability, organizations can increase trust and confidence [22]. It reduces the risk of data breaches and service interruptions in systems [23]. Security issues in cloud computing provide insight into accountability standards, key security issues, compliance and best practices to ensure data confidentiality, integrity and availability in the cloud [24]. Once you resolve these issues effectively, the organization can get the job done [25]. They are very valuable and

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

useful as well as the power of cloud computing [26]. The emergence of cloud computing has revolutionized businesses with unprecedented flexibility, and cost efficiency [27]. Some organizations in different industries are moving to storage, processing and cloud services to manage data and capitalize on demand [28]. They do not want to buy more computer products or make infrastructure investment [29]. However, this rapid migration to the cloud also introduces many legitimate security issues [30]. With the cloud computing landscape rapidly evolving, ensuring compliance with regulatory requirements is a top priority for organizations across industries. From data protection regulations to industry-specific standards, compliance mandates play a key role in maintaining trust among customers and stakeholders to protect sensitive information in in this section, we examine the different compliance requirements that organizations face in cloud computing. Data Protection Regulations :One of the main compliance challenges in cloud computing relates to data protection laws, such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States , and imposes stringent processing requirements , requiring stringent data governance and security measures Under the GDPR, organizations are explicitly required to obtain consent Before individuals process their personal data, they will use it accordingly Security measures to protect against data breaches, and regulatory compliance Principles of data reduction and objective constraints. If they don't with GDPR, there can be severe penalties, including penalties of up to 4% Annual global turnover or €20 million (whichever is greater). Similarly, the CCPA gives California consumers the right to information They collect information about themselves, the right to it the personal information companies have, and the right to opt out the sale of their personal information. Organizations subject to CCPA must implement mechanisms for complying with these requirements, including data mapping, consumer rights request management, and privacy policy updates.Industry-Specific Standards: organizations add to general data protection rulesThose working in specific industries must meet specific compliance requirements and certifications. For example, healthcare organizations must comply with the Health Insurance Portability and Accountability Act (HIPAA), which establishes stringent requirements for protecting the privacy and security of protected health information (PHI). HIPAA applies to operational, physical, and technical safeguards to ensure confidentiality, integrity, and availability of PHI. payroll companies and their contractors. Conduct regular risk assessments, implement access controls, and secure PHI where appropriate, and maintain audit procedures for access to PHI and disclosure of Things. The same goes for organizations involved in processing payment cards... Payment cards comply with the Industry Data Security Standard (PCI DSS),which sets out requirements to protect and prevent cardholder data Card cheating mouth. PCI DSS compliance includes network services security measures, secure card terminals, and cardholder encryption data, and perform vulnerability analysis and routine access research.

## II. RELATED WORK

Cloud computing has become a fundamental part of modern IT infrastructure, and with this shift, the importance of cloud security has grown significantly. One of the most cited and foundational contributions to understanding cloud systems came from Mell and Grance [31], who provided the widely accepted definition of cloud computing through NIST. Their framework helped formalize the different service and deployment models that are now standard in the industry. Security in the cloud continues to be a critical concern. Ali et al. [32] examined both the advantages and vulnerabilities introduced by cloud environments. Their study pointed out that while organizations gain flexibility and scalability, they also become more exposed to issues like data breaches and loss of control, especially when sensitive data is involved. Zissis and Lekkas [33] contributed to the discussion by highlighting the central role of the confidentiality, integrity, and availability (CIA) triad in cloud computing. They emphasized that the shared and distributed nature of the cloud environment makes protecting these three principles more challenging and more important than ever. A key concept in cloud security is the Shared Responsibility Model**,** which was clearly outlined by Amazon Web Services [34]. This model explains that security is a joint effort: while cloud providers are in charge of securing the infrastructure, customers are responsible for securing their data, configurations, and user access. Subhashini and Kavitha [35] expanded on this by breaking down how responsibilities shift depending on whether the service model is SaaS, PaaS, or IaaS. Their work offers clarity on which party is accountable for what aspect of cloud security. Chow et al. [36] addressed a common concern in cloud adoption—how to maintain control over data that is stored and processed by a third party. Their research proposed cryptographic methods that allow users to retain control

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 9, June 2025 Impact Factor: 7.67

over their information even when using public cloud services. Microsoft's official documentation [37] also provides a practical guide for cloud users, emphasizing the need for strong identity management and secure configurations. Their clear division of roles and responsibilities helps prevent the security gaps that often result from confusion between providers and clients. The European Union's cybersecurity agency, ENISA, released an influential report [38] that categorized cloud-specific risks such as data loss, service unavailability, and lack of transparency regarding data location. They also offered practical recommendations for both cloud providers and users, which are still relevant for regulatory compliance efforts today. Further cloud-specific threat classification was provided by Has Hizume et al. [39], who created a detailed taxonomy of usual threats, including insecure interfaces, typical technology issues, and malicious insiders. Their classification has been utilized as a reference point in scholarly work as well as enterprise-level security audit. Modi et al. [40] introduced an in-depth survey of cloud-environment-specific intrusion detection systems. They compared various methodologies and elaborated on the impact of cloud-native features such as virtualization and multi-tenancy on the efficiency of conventional security tools. They advocated cloud-appropriate solutions that can identify threats without affecting system performance. Together, these articles serve to offer insightful comments on the changing nature of cloud security. They emphasize the need for collaborative action, compliance with regulations, and flexible security frameworks towards establishing cloud systems as strong, reliable, and secure**.**

## III. METHODOLOGY

In a responsive cloud model where companies more and more rely on cloud service providers (CSPs) to provision and manage applications and data, it is beneficial to understand what shared responsibility lies between CSPs and cloud consumers under. have numerous responsibilities encompassing all security aspects Within this section, we outline the key responsibilities of cloud consumers and how best to fulfil those duties in the cloud environment.

Data Protection and Encryption That involves making sure that your data's being encrypted when it's traveling somewhere and just sitting there. And you've got to have policies in place about who gets to see this stuff. You even have to have policies about how long you retain your information and comply with privacy and record-retention laws. By performing these tasks, like using encryption and restricting access, you lower the chance that an unauthorized user will gain access to your information, which makes everything more secure

*.Identity and Access Management(IAM)*

The other essential duty that cloud customers have is identity and access management within their cloud infrastructure. While CSPs can provide services that involve identity and access control, such as authentication and role-based access control (RBAC), cloud customers are ultimately responsible for defining and enforcing access policies for their users and applications cloud customers should implement a strong IAM policy to manage the useraccess to cloud resources, including defining user roles and permissions,Implement Multifactor Authentication (MFA), and review it regularly and updating access policies to reflect organizational changes Requirements. Managing users and accessibility, the cloud Consumers can reduce the risk of unauthorized access and resulting threats,thereby increasing the security of their cloud environment.

*Security Monitoring and Incident Response*

*In* addition to data security and IAM, cloud customers are responsible for managing their cloud environments to ensure security threats and.and respond quickly to reduce the risks of incidents. While CSPs can provide security management tools and services, including intrusion detection systems (IDS) and security information and event management (SIEM) platforms, cloud customers must proactively monitor their environments surrounding monitors for suspicious activities and indicators of compromise Cloud customers must have a robust incident response plan,Includes presenting, analyzing, and responding to predefined workflows

for safety incidents, and how to conduct post-incident investigations Identify lessons learned and improve future response efforts. By implementing proactive security monitoring and incident response capabilities, cloud customers can detect and respond to security threats in a timely manner, minimizing the impact of potential breaches and

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

enhancing the overall resilience of their cloud environments.While CSPs play a key role in securing the underlying cloud infrastructure, cloud customers have primary responsibilities for data protection, identification and access management, security management and incident response to Dabhang unauthorized entry and mitigate risk As organizations embrace cloud the computing, logic and navigation of shared responsibility models to ensure security and efficiency if in cloud- based applications and data becomes important.

Strategies for Achieving Compliance: To navigate the complex environment of compliance requirements in cloud computing, organizations can take several approaches to ensure compliance with regulatory and industry standards First, organization must types scrutinize their cloud environments for potential compliance gaps and weaknesses. This includes evaluating the security measures provided by cloud service providers (CSPs) and implementing additional measures as necessary to meet compliance requirements Second, organizations need to implement cloud security and compliance Tools for strategic compliance monitoring, risk identification and incidents Information delivery systems. These tools can help organizations achieve this Maintain compliance that allows them to see their safety in real time Money, identifying violations and facilitating discipline The efforts they make. In addition, organizations should provide employee training and awareness programs to educate employees on compliance requirements, safety best practices, and the importance of safety Important Information. Empowering employees to see and. They respond better to compliance risks; organizations can strengthen them their overall security level and risk of non-compliance is reduced. In conclusion, compliance requirements in cloud computing vary and as organizations evolve, they need to be proactive and receptive A comprehensive approach to ensuring compliance with legal mandates and industry standards. By implementing strong data protection decisions, the benefits of cloud security tools, and management priorities training, organizations can take compliance challenges cloud and reduces the risk of compliance penalties Defamation of reputation.

SIEM technology

Security is key in the rapidly evolving cloud computing landscape Organizations looking to use cloud services, and mitigating associated risks As businesses shift their operations to cloud environments have to evolve their security strategies to meet the unique challenges posed by distributed architecture, shared responsibility models and dynamic threat scenarios ) Technology is emerging as a key driver of threat escalation Detection and incident response capabilities in cloud environments. In this section, we examine the role of SIEM technologies in cloud security and discuss ways to implement SIEM solutions to strengthen the cloud security posture. Understanding SIEM technology

SIEM technology integrates security information management (SIM). To provide security event management (SEM) services Comprehensive visibility into the organization's IT infrastructure, including. Web pages, applications, and endpoints. SIEM solutions accumulate and. Link security events from different sources such as firewalls, attacks detection systems (IDS), and endpoint security platforms, for detection and facilitate timely response to potential security issues and actions. in To centralize security incident data and implement advanced analytics, SIEM The solution enables organizations to detect and respond to security threats More effectively, it thereby enhances the overall level of cybersecurity.

Challenges in cloud security

Cloud computing presents unique security challenges Distributed creativity, shared responsibility models, and dynamic provisioningof the use of resources. Cloud environments include a myriad of applications and configurations, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), each requiring specific security considerations , responsibilities a shared instances in cloud environments require collaboration between cloud providers and customers to ensure complete security protection, which will enhance security management. Role of SIEM in Cloud SecuritySIEM technologies play a key role in addressing the security challenges associated with cloud computing by enabling visibility, insight, and response capabilities in cloud environments Some of the key roles that SIEM solutions play in cloud security and:Central Log Management:SIEM solutions collect and analyze log data from various cloud services and infrastructure components, including virtual machines, containers, and serverless applications. By collecting log data from multiple sources, SIEM solutions provide centralized visibility into

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 9, June 2025 Impact Factor: 7.67

cloud activity, enabling security teams to monitor suspicious behavior and potential security issues Risk Identification and Analysis:SIEM solutions use a combination of advanced analytics, machine learning, and threat intelligence to identify abnormal activities and potential security threats in cloud environmentsAction Response Singers: The SIEM solution simplifies incident response orchestration by automating business planning, execution of response actions, and collaboration between security teams and cloud service providers. By simplifying things Incident response systems, SIEM solutions help organizations mitigate impact of security incidents and how to restore normal operation In an effective manner.Compliance monitoring and reporting**:** The SIEM solution also supports compliance monitoring and reporting Provide audit trails, develop and issue compliance reports Compliance assessment in cloud environments. in Security events and activities are recorded, SIEM solutions help Organizations demonstrate compliance with industry regulations and. Standards such as GDPR, HIPAA and PCI DSS. .Best practices for implementing SIEM in cloud environmentsTo maximize the effectiveness of SIEM technology in cloud security, . Organizations should adopt best practices and. Managing SIEM solutions in cloud environments:Advanced data integration:**I**n cloud services, platforms, . and infrastructure components to capture relevant security event data and facilitates thorough risk identification and analysis.Scalability Changes f:Choose a SIEM solution that provides scalability and flexibility for change The dynamic nature of the cloud environment, including the rate atwhich it scales Infrastructure, integration with cloud-native services, and support for hybrid and multicloud..Automation and Orchestration:Leverage the automation and orchestration capabilities of the SIEM solution To streamline incident response planning, develop automatic response actions, and accelerate threat mitigation efforts in cloud environments. Interview with Cloud Providers:Work closely with cloud service providers and integrate SIEM Solution with native cloud security controls, leveraging cloud provider API For data access and integration, compatible security policies and. Processes with cloud provider recommendations and best practices.Continuous review and modification:Ensure that continuous monitoring and quality practices are implemented SIEM solutions that remain efficient and effective in the cloud environmental areas, where routine searches are conducted and search rules are modified Correlation algorithms, and early detection ofemerging threats and viral attacks. SIEM technologies play an important role in increasing threats Detection and incident response capabilities in cloud environments. Providing centralized detection, advanced analytics, and automation Responsive systems, SIEM solutions enable organizations Effectively monitor, detect and mitigate security threats cloud services and infrastructure components.Embracing best practices To implement and manage SIEM solutions in cloud environments, . Organizations can strengthen and weaken their overall level of security Risks associated with cloud computing, protection from it and. Run Remover Again Cloud deployment is resilient to evolving cyber threats. Figure 4 shows how SIEM (Security Information and Event Management) tools contribute to cloud security by performing several key functions. Among these, threat detection stands out as the most effective, followed closely by incident response, centralized logging, and risk analysis. Automation and compliance monitoring are also important but come second. Overall, this number shows the way SIEM protects companies by staying one step ahead of security threats, being able to handle risks, and with greater visibility throughout their cloud infrastructure.

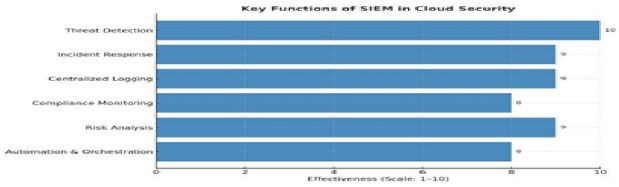


Figure 4 : Important role of SIEM in cloud security

Table1 illustrates the key SIEMtool capabilities and how they help in cloud security. Threat detection, for instance, identifies suspicious behavior inadvance using analyticsandmachinelearning, all owing for quicker actiononthreats.Incidentresponse revolves around managing security events well, and centralized logging brings information from all over the cloud onto a single point for easier inspection.Riskanalysis helps to prioritize threats,andcompliancemonitoring helps keep theorganization in linecrit icalregulations like GDPR and HIPAA. Last but not least, automation and orchestration allow teams

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

to act faster and more consistently by using standardized processes.At the same time, all of these functionalities makeSIEMa feasible solution for cloud security assurance.

| Function | Purpose | Benefit |
|---|---|---|
| Threat Detection | Identifies abnormal activity using logs, analytics, and ML. | Early detection of potential attacks. |
| Incident Response | Automates and manages security events. | Early detection of potential attacks. |
| Centralized Logging | Collects logs from diverse cloud components. | Unified visibility for analysis. |
| Risk Analysis | Evaluates and prioritizes threats using correlation rules. | Proactive mitigation of vulnerabilities. |
| Compliance Monitoring | Tracks activity for regulatory reporting. | Ensures GDPR, HIPAA, PCI DSS adherence. |
| Automation & Orchestration | Enables rapid, coordinated action using playbooks | Faster, consistent incident handling. |

Table 1: Core Functions of SIEM and Their Security Benefits in the Cloud

## III. RESULTS AND DISCUSSION

This research indicates the continued requirement for Identity and Access Management (IAM) to protect cloud infrastructures. Although cloud providers such as AWS, Azure, and Google Cloud possess robust IAM controls, how effectively they work entirely depends on the security access policies organisations implement and maintain. Certain of the shared blunders such as permissive access rights, lack of frequent audits, and roles being incorrectly assigned remain to render cloud systems vulnerable to attacks. Implementation of best practices such as the principle of least privilege, role-based access control (RBAC), and permission checks on a recurring cycle can go a long way in yielding security outcomes.Apart from IAM, more research is exploring new technologies to combat new threats against the cloud. Of special interest, current research is now focused on three areas:Machine Learning Threat Detection: Researchers employ machine learning techniques more and more to meet cloud security. These models can scan the system activity in huge volumes and search for abnormal patterns that represent possible attacks. Spikes in access request logins, for instance, from unknown sources, or strange data transfer may all be signs of an attack. By detecting such anomalies in advance, machine learning systems allow for earlier investigation and response, which could prevent breach expansions further. Zero Trust Security Models: Zero Trust is becoming more popular as an end-to-end cloud security model. Unlike historical models of security, which are often rooted in default trust within the network location or perimeter, Zero Trust requires constant verification of all users and devices before providing access. This pool of research has a concentration on how best to implement Zero Trust in advanced, multi-cloud environments to reduce risk and optimize control overall. Blockchain for Safer Clouds: Blockchain is also gaining momentum as a possible solution to battle greater transparency, data integrity, and trust in cloud infrastructure. Blockchain records an unalterable history of transactions, and as such it can be used to seal logs, authenticate data origin, and offer tamper-proof audit trails. Research has begun on integrating blockchain into existing cloud infrastructure to boost accountability and help with compliance. Concert, these trends are indicating that cloud security will shift towards more proactive, intelligent, and decentralized solutions. IAM is still the platform, but marrying it with more newer-generation technologies like machine learning and blockchain could offer more robust, more flexible defenses. It's a matter of tying all of these tools together intelligently—having them feed off each other and tackle each organization's specific cloud plan. Figure 5 reflects some of the most critical areas currently being researched to increase cloud security. Identity and Access Management (IAM) is one of the key areas, where proper roles must be assigned to users and provide only those roles to people that they need access to information. Machine learning also is drawing interest for its capability to identify abnormal patterns, forecast, and initiate real-time notifications in order to prevent threats from inflicting harm.The second growing focus area is the Zero Trust model, based on the principle of never trusting anyone by default, and authenticating each access request in real time. Lastly, blockchain is being explored for its ability to keep secure, tamper-evident records, track data provenance, and facilitate open, trustworthy

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

auditing. Collectively, these subjects reflect the direction that the space is heading to meet the advanced security needs of today in the cloud. Figure 6 shows the distribution of security duties between the cloud provider (CSP) and the customer. The CSP, or vendor, will see to the back-end operations like physical security, network management, and maintenance of the underlying infrastructure and core systems that power the cloud. On the other hand, the customer will see to proper access controls being put in place, their data protected, and proper compliance regulations being adhered to. They also need to define who receives access to what through IAM (Identity and Access Management) policies. This joint approach makes both the user and the provider both equally responsible for keeping the cloud environment safe and under control.

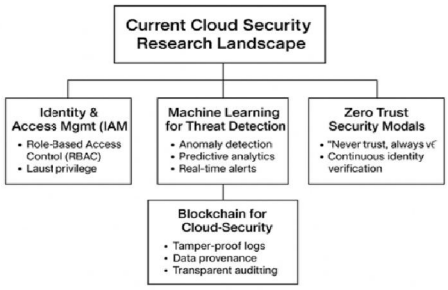


Figure 5 : Main Areas of Ongoing Research in Cloud Security

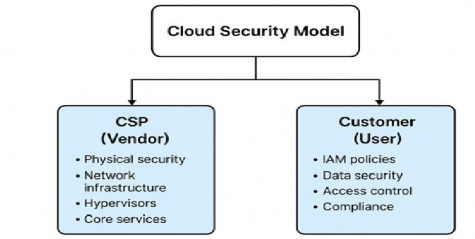


Figure 6 : Division of Responsibilities in the Cloud Security Model

Table 2 depicts real-world examples of how large organizations are using SIEM tools to support their cloud security efforts. Netflix, for instance, runs on AWS and employs Splunk and internal tools to speed up how they can detect and respond to threats in their complex microservices environment. NASA operates a hybrid cloud model on both AWS and Azure, and they've deployed IBM Radar to keep close tabs on sensitive mission information and meet very strict requirements. Airbnb relies on Datadog, integrated with SIEM, to stay ahead of threats in real time across their fast-changing infrastructure. Spotify, which uses Google Cloud, benefits from Chronicle SIEM to streamline log analysis and get faster alerts when something suspicious happens. General Electric works in a multi-cloud setup and uses Azure Sentinel to automate threat investigaions, helping their security teams work more efficiently. These examples show how SIEM tools are being adapted to fit each organization's unique cloud environment and security needs.

Figure7shows how different companies have experienced the benefits of using SIEM tools in their cloud environments. As the chart illustrates, Netflix and Spotify have seen the most noticeable improvements, each scoring 9 out of 10 in terms of security effectiveness. This probably demonstrates the effectiveness of their systems in detecting threats and responding to incidents. NASA, Airbnb, and General Electric all rated an 8, which is still a good indication of high performance, particularly in specific areas such as compliance, monitoring, and automating away the work from their teams. Overall, the number clearly indicates that deploying SIEM solutions has actually improved the cloud security of all these companies in significant ways

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

| Cloud Environment | SIEM Solution Used | Outcome / Benefit |
|---|---|---|
| AWS | Splunk + Custom Tools | Improved incident response time and threat visibility in a microservices architecture |
| AWS / Azure Hybrid | IBM Radar | Enhanced monitoring of sensitive mission data and regulatory compliance |
| AWS | Datadog + SIEM Integrations | Real-time threat detection across dynamic infrastructure |
| Google Cloud Platform | Chronicle SIEM (Google) | Centralized log analysis with scalable threat detection and fast alerting |
| Multi-cloud (AWS, Azure) | Azure Sentinel | Automated threat investigation and reduced manual workload for security teams |

Table 2 : SIEM Implementation in Cloud Security Environments


Figure 7: Real-Life Impact of SIEM on Cloud Security Across Organizations

## IV. CONCLUSION

This research has been a stimulating journey through the actual concerns of cloud computing security. Cloud computing has become the standard of storing, retrieving, and managing information, and therefore safeguarding personal data has never been more essential. With reference to studying reference models such as Identity and Access Management (IAM), Zero Trust Architecture, Blockchain technology, and the Shared Responsibility Model, this book tried to learn and spread effective means of securing the cloud.IAM transformed into a critical enabler for maintaining who does what within a world of the cloud. Without strong identity and access controls, even the finest technology is vulnerable. Grasping onto that, the Zero Trust model redefines the traditional mind-set by not trusting any user or system at all times. This mindset encourages continuous authentication and helps to voluntary prevent in and out risks. Blockchain, historically associated with cryptocurrencies, has tremendous potential to offer in the space of security. Its open and immutable recording component makes it a much-needed utility for validating access logs and maintaining data integrity in the cloud. With such technologies, the Shared Responsibility Model also has an essential role in revealing the security responsibility gap between cloud service providers and users. Awareness of and compliance with such boundaries is the most crucial aspect of avoiding misconfigurations and under-detecting vulnerabilities.

In summary, this research says that cloud security does not equate to reliance on one tool or technique's effectiveness. Instead, it necessitates a multifaceted solution—technology controls, sound policy, and attentiveness all applied in tandem. Its expansion and evolution are certain to grow even larger, and so are the measures we take to protect it. Being well-informed, adaptable, and dedicated to performing our responsibilities is critical in making an online environment that is safer.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

## REFERENCES

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," NIST Special Publication 800-145, Sep. 2011.
[2] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," Information Sciences, vol. 305, pp. 357–383, Jun. 2015.
[3] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592, Mar. 2012.
[4] Amazon Web Services, "Shared Responsibility Model," [Online]. Available: https://aws.amazon.com/compliance/shared-responsibility-model/
[5] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, Jan. 2011.
[6] R. Chow et al., "Controlling data in the cloud: Outsourcing computation without outsourcing control," in Proc. ACM Workshop on Cloud Computing Security, pp. 85–90, 2009.
[7] Microsoft Azure, "Shared responsibility in the cloud," [Online]. Available: https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
[8] ENISA, "Cloud Computing: Benefits, Risks and Recommendations for Information Security," European Union Agency for Cybersecurity, Nov. 2009.
[9] 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, pp. 1–13, Jan. 2013.
[10] C. Modi et al., "A survey of intrusion detection techniques in cloud," J. Netw. Comput. Appl., vol. 36, no. 1, pp. 42–57, Jan. 2013.
[11] SANS Institute, "Top Cloud Security Threats," [Online]. Available: https://www.sans.org/white-papers/388/
[12] M. Hendre and R. Joshi, "A survey on security issues in cloud computing," in Proc. IEEE Int. Conf. Comput. Sci. Inf. Technol., 2011, pp. 69–73.
[13] A. Popovic and Z. Hocenski, "Cloud computing security issues and challenges," in Proc. IEEE MIPRO, 2010, pp. 344–349.
[14] R. Kumar and R. H. Goudar, "Cloud computing – research issues, challenges, architecture, platforms and applications," Int. J. Cloud Comput. Services Sci., vol. 1, no. 2, pp. 1–14, May 2012.
[15] KPMG, "The cloud takes shape: Cloud computing strategy, operational and technology issues," [Online]. Available: https://home.kpmg/
[16] A. Gholami and E. Laure, "Big data security and privacy issues in the cloud," Int. J. Netw. Secure. Appl., vol. 8, no. 1, pp. 59–72, Jan. 2016.
[17] S. Pearson, "Taking account of privacy when designing cloud computing services," in Proc. IEEE CLOUD, 2009, pp. 44–52.
[18] C. Cachin and M. Schunter, "A cloud you can trust," IEEE Spectrum, vol. 48, no. 12, pp. 28–51, Dec. 2011.
[19] M. Hogan et al., "NIST Cloud Computing Standards Roadmap," NIST Special Publication 500-291, Jul. 2013.
[20] R. Gellman, "Privacy in the clouds: Risks to privacy and confidentiality from cloud computing," World Privacy Forum, Feb. 2009.
[21] Cloud Security Alliance (CSA), "Security Guidance for Critical Areas of Focus in Cloud Computing v4.0," 2017.
[22] B. Rimal, E. Choi, and I. Lumb, "A taxonomy and survey of cloud computing systems," in Proc. IEEE Int. Joint Conf. INC, IMS and IDC, 2009, pp. 44–51.
[23] J. Heiser and M. Nicolett, "Assessing the security risks of cloud computing," Gartner, Mar. 2008.
[24] D. Catteddu and G. Hogben, "Cloud computing: Benefits, risks and recommendations for information security," ENISA Report, Nov. 2009.
[25] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, "On technical security issues in cloud computing," in Proc. IEEE CLOUD, 2009, pp. 109–116.
[26] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Comput., vol. 16, no. 1, pp. 69–73, Jan. 2012.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

[27] D. Linthicum, Cloud Computing and SOA Convergence in Your Enterprise: A Step-by-Step Guide, Pearson Education, 2009.
[28] N. Sultan, "Cloud computing for education: A new dawn?," Int. J. Inf. Manage., vol. 30, no. 2, pp. 109–116, Apr. 2010.
[29] B. Rochwerger et al., "The RESERVOIR model and architecture for open federated cloud computing," IBM J. Res. Dev., vol. 53, no. 4, pp. 535–545, Jul. 2009.
[30] A. Juels and A. Oprea, "New approaches to security and availability for cloud data," Commun. ACM, vol. 56, no. 2, pp. 64–73, Feb. 2013.
[31] P. Mell and T. Grance, "The NIST definition of cloud computing," NIST Special Publication 800-145, Sep. 2011.
[32] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," Information Sciences, vol. 305, pp. 357–383, Jun. 2015.
[33] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592, Mar. 2012.
[34] Amazon Web Services, "Shared Responsibility Model," [Online]. Available: https://aws.amazon.com/compliance/shared-responsibility-model/
[35] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, Jan. 2011.
[36] R. Chow et al., "Controlling data in the cloud: Outsourcing computation without outsourcing control," in Proc. ACM Workshop on Cloud Computing Security, pp. 85–90, 2009.
[37] Microsoft Azure, "Shared responsibility in the cloud," [Online]. Available: https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
[38] ENISA, "Cloud Computing: Benefits, Risks and Recommendations for Information Security," European Union Agency for Cybersecurity, Nov. 2009.
[39] 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, pp. 1–13, Jan. 2013.
[40] C. Modi et al., "A survey of intrusion detection techniques in cloud," J. Netw. Comput. Appl., vol. 36, no. 1, pp. 42–57, Jan. 2013