International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 12
***Article Received:** 25 July 2022 **Revised:** 12 September 2022 **Accepted:** 30 November 2022*

Cybersecurity and Cloud Computing: The Challenges and Solutions for Securing Data and Applications in Cloud Environments

[1]Sandeep Reddy Narani , [2]Sunil kumar Suvvari
[1]Independent Researcher, Texas, USA
[2]Independent Researcher,USA

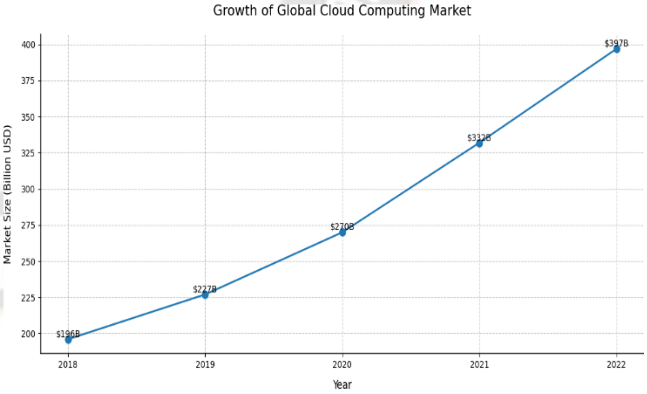
Abstract: This paper aims at understanding the crucial relationship between cybersecurity and cloud computing strategy mainly on the consideration of the challenges and the possible measures towards securing the data and application in cloud strategy. This explains the fact that as businesses continue to transfer their activities to the cloud, security becomes an important issue. In this work, some of the areas that are considered are data security, application security, network security and identity management concerning cloud. It also covers new technologies and forthcoming areas that are defining the prospects of cloud cybersecurity. Thus, based on the review of the recent literature and the main approaches used in the field of cloud security, the goal of this paper is to present the findings that can be helpful for researchers, practitioners and decision-makers.

Keywords: *Cloud computing, cybersecurity, data security, application security, network security, identity and access management, emerging technologies*

1. Introduction

1.1 Background on cloud computing

Cloud computing is the biggest advancement in the management of data and applications in organizations. Mell and Grance of the National Institute of Standards and Technology (NIST) define cloud computing as a definition of a paradigm that provides a near effortless means to access, with minimal provision of the IT infrastructure's physical characteristics, pools of configurable computing resources which include networks, servers, storage resources and applications as well as services over the internet (2011). This has enhanced the growth of these firms in a faster way and they have also managed to reduce several operating expenses hence they proved to be flexible in their operations to forces in the market. Currently and in particular in the last few years, cloud computing has been on an exponential growth. Gartner tech research pegs the worldwide public cloud services market to reaching a 23% growth over the next four years. from 1% in the scenario constructed for the year 2021 which gives a sum total figure of $332. 3 billion, from $270 billion in 2020 (Gartner, 2021). These findings show that this convergence of cloud services in different business sectors is clear evidence of the changing new face of businesses through cloud computing. The cloud computing market is still oligopolistic, where several market leaders offer widespread and new solutions. The four key players in the cloud services market are AWS (Amazon Web Services), MS Azure, Google Cloud and Oracle Cloud. These firms have played the key role on the advancement of cloud solutions and services from the fundamental concepts of cloud computing to the assistance of many Artificial Intelligent and Machine Learning processes.



1.2 Importance of cybersecurity in cloud environments

Clouds have continued to be mainstream in recent years, and as this continues cybersecurity in the cloud has also become essential. One more disadvantage of cloud computing is the geographical factor; cloud-based resources are vulnerable to hacker attacks as well as the fact that nowadays, numerous sensitive data are stored in cloud environments. According to

Gartner, by the year 2025, the major blame for cloud security mishaps will lie with the customer as only 1% will be owed to technology mishaps (Gartner, 2021). This serves to show how there is dire importance for organizations to consider and embrace strong security regimes when using cloud services.

The penalties for cloud security neglect are not petty. Incidents such as data loss, interrupted services, and failure to adhere to regulatory requirements are costly, brand destructive, and can have legal consequences. According to the IBM and Ponemon Institute's research on key findings for 2021, the average data breach cost was $4. 24m people, which is still the highest recorded level since 2003/2004 (IBM, 2021). Since large cloud service providers are exposed to numerous clients at once, the consequences of large-scale breaches are significantly higher for such organizations.

1.3 Scope and objectives of the paper

The purpose of this paper is to give a systematically described view of the threats and prospects of strengthening protection of data and applications within cloud systems. Cloud security involves the following: data protection, application security, network security and identity management. The objectives include:

1. Exploring the contemporary issues of cloud computing security
2. Examining predisposing factors that would hinder the possibility of entering cloud environments
3. Most organizations face various issues and risks when implementing solutions and developing best practices for managing them.
4. Looking into new developments and future prospects for cloud safety and security Thus, meeting these objectives, this research aims to add to the current literature on cloud security and offer real-life recommendations for organizations willing to improve the overseeing of their cloud security.

2. Cloud Computing Architecture

2.1 Service models (IaaS, PaaS, SaaS)

Cloud computing offers three primary service models, each providing different levels of control and responsibility for the customer:

- Infrastructure as a Service (IaaS): This model offers computing infrastructure on an internet basis to the users' specified requirements. Customers can manage OS, storage, and applications that are run on them but cannot manage the cloud that supports them. Some examples of IaaS providers are AWS ec2, Microsoft azure virtual machine, and Google compute engine.
- Platform as a Service (PaaS): PaaS provides a platform for the customers who can build, run and manage their applications in a simple way without having to worry about the physical structures (Alhenaki, Alwatban, Alamri, & Alarifi, 2021). This model is especially significant for developers who prefer to pay more attention to application development while the question of server leasing is solved on their own. Some of these include Heroku, Google App engine, and Microsoft Azure App services.
- Software as a Service (SaaS): In this model, it is an approach where applications can be accessed through the web with the client paying a subscription fee. The programme and its prerequisites refer to the infrastructure, platforms, and software that the service provider is in charge of. Some commonly known SaaS are Salesforce, Google Workspace and Microsoft 365.

2.2 Deployment models (Public, Private, Hybrid, Multi-cloud)

Deployment models represent the availability of cloud services to its users. The four main deployment models are:

- Public cloud: It is being delivered at the third party & used by several organizations. It gives scalability, cost efficiency, and fast implementation in the public cloud. However, they may pose security and privacy risks to sensitive information that is processed and stored. Some of the well-known public clouds are Amazon Web Service, Microsoft Azure, and Google Cloud Services.
- Private cloud: It is an infrastructure that had been reserved for the usage of an organization. Private cloud infrastructure gives more control over security and compliance, but it may be rather expensive at first (Youssef, 2020). Private cloud can be developed on its own by the organizations or can obtain dedicated services from organizations such as IBM Cloud Private or VMware vCloud.
- Hybrid Cloud: This model provides hybrid data and applications for public cloud and private cloud models as a single entity. Hybrid cloud solutions are more elastic and might be mostly efficient when an organization needs to implement the cloud model but has many security-related questions. Many enterprises implement it to have their applications' critical data stored on-premise while leveraging public cloud for less sensitive processes.
- Multi-cloud: Here, cloud computing and storage services are implemented in a diverse architecture to attain the objectives. Multiple cloud deployments are also free from issues related to vendor lock-in, offer the best solution for

spending, and are more reliable. But they also create issues of management and security at the same time.

2.3 Key components of cloud infrastructure

Cloud infrastructure typically consists of several key components that work together to deliver services to users:

- Physical layer: This includes all IT physical infrastructure ranging from servers, storage devices, network equipment and data centres. The actual facilities utilized by cloud providers are easy to misinterpret, but large amounts are spent on state-of-the-art infrastructure to optimize availability.
- Virtualization layer: VMware vSphere and KVM are hypervisors that establish and control virtual computers; in this way, several operating systems can run on one physical computer. This layer is core for the efficient application of resources and development of the flexibility of the cloud services (Verizon, 2020).
- Management layer: This component contains the means required for resource management, tracking and coordination. Tools such as OpenStack and VMware vCloud Director are insightful about cloud resource management and allocation by the administrator.
- Service layer: This layer consists of simple interfaces for cloud services which include application program interfaces, web-based interfaces, and terminal interfaces. It allows end users to work with cloud resources and services with relative ease.

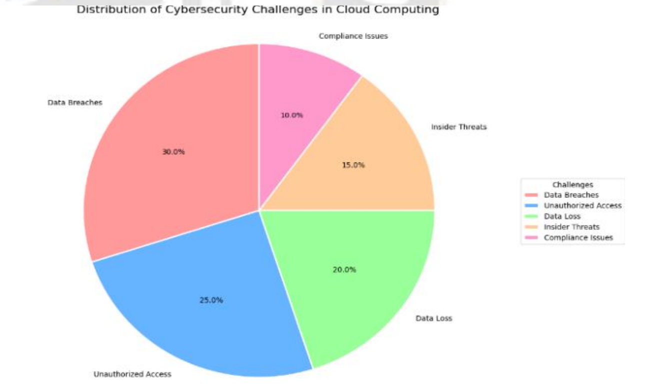
3. Cybersecurity Challenges in Cloud Computing

3.1 Data breaches and unauthorized access

Security is still a major concern while data breaches remain one of the most glamorous clouds in cloud computing. Ponemon institute's July 2021 report on Cost of a Data Breach Report conduced with IBM informed that overall expense for breach in average was raised up to $4. 24 million. To this effect, 24 million reports were filed in 2021, the highest filing rate in the last 17 years (IBM, 2021). Indeed cloud environments are considered particularly risky mainly because are distributed by their very constitution and contain a large amount of data. Such threats are executed by reaching for unauthorized paths such as in-app device controls, wrong authentication and authorization processes, or attacks on cloud services. To reduce these risks cloud providers and users employ strong authentication measures including Authorized Identification (MFA), Permissions Given According to a Person's Identity (RBAC), and One-Time Password (SSO). These methods greatly improve security by allowing access to data and systems only to the personnel that is qualified to do so. The fundamental of safety in cloud computing is referred to as the shared protection duty which means that while cloud providers do their best to make their storage cloud safe, the customers have to do their part as well and do not go beyond the Cloud Security Areas. This model pays great attention to continuity in order to be able to scan possible threats that may occur and confirm them instantly.

3.2 Data loss and data integrity issues

Data may be lost due to a variety of reasons including several employees sharing files, erasing hard drives, or a deliberate sabotage. Measures of data safeguard in the Cloud environment are worrisome because of the environment's complicated setting and elements of possible missing configuration. A research by Skybox Security shows that 73% of firms are rather concerned with regard to data loss and privacy concerns in cloud (Skybox Security, 2021). Data consistency is also rather problematic yet highly important especially in multi-tenancy setting; it is crucial for customer trust to cloud solutions. Data corruption either intentionally or otherwise is very risky to organizations depending on cloud for storage of their data and running of their applications. RBAC is the best approach that fits the organization's security undertakings in enforcing effective access control while the second strategy entails constant surveillance of data access and modification activities to ensure data integrity in cloud environments.



3.3 Insider threats

Insider threats are a real menace to the confidentiality and integrity of data that organizations transfer to the cloud. A survey by Cybersecurity Insiders revealed that 68% of firms are somewhat to extremely threatened by insider perils (Cybersecurity Insiders, 2020). In reference to cloud environments, insiders remain a possibility, wherein the mentioned actors are not only the organization's staff but also the cloud provider's staff with access to the infrastructure.

The problem is further intensified by the fact that conventional security models rely on the physical perimeter

***Article Received:** 25 July 2022 **Revised:** 12 September 2022 **Accepted:** 30 November 2022*

that is hard to implement in cloud solutions because resources can be accessed from any place that is connected to the internet.

3.4 Shared technology vulnerabilities

The key risk in cloud computing involves the risky sharing of a single technology with many parties. In cases where a hypervisor is used or for a shared platform element, a flaw in one tenant could mean a compromise between different tenants.

The main examples that illustrated the problem of cross-technology vulnerabilities in the cloud were observed in The Meltdown and Spectre in 2018. These hardware-level implementations impacted almost all contemporary processors and could even enable criminals to obtain data of interest across virtual machine partitions.

3.5 Account Hijacking and Identity Theft

Accounting the cloud, hijacking and identity theft remain prevalent and recurrent issues. Hackers may use methods involved in phishing, credential dropping or overloading accounts with incorrect password guesses and others to access cloud accounts. When breached, such accounts are handy for executing additional attacks or data theft, as well as disabling services.

Verizon was able to publish data according to which eighty percent of the hacking attacks are linked directly to brute force and the loss of log-in credentials (Verizon, 2020). This is perhaps the reason why identity and access management are considered one of the most critical components of cloud security.

3.6 Compliance and regulatory challenges

With today's organizations migrating corporate data and core applications to the cloud, the business has to grapple with numerous compliance issues and guidelines. Every business sector and geography have its rules regarding data protection and privacy; some of the well-known ones are GDPR in the EU or HIPAA in the United States medical field.

It becomes hard to enforce compliance in the cloud environments because the data is scattered in many places (Stergiou, Psannis, Kim, & Gupta, 2018). There must be awareness of where the organization's data goes, how it is processed, and by whom. On the same note, they have to confirm that their chosen cloud providers have the compliance level that is required and that there is proof of compliance in the form of an audit and certification.

4. Data Security in Cloud Environments

4.1 Data encryption techniques

Encryption is one of the elementary levers of confidentiality in the cloud. This makes it possible that while the data is in the hands of unauthorized individuals, physical or natural, they cannot understand or make use of the data without passing through the encryption key. Cloud providers typically offer various encryption options:

1. Data-at-rest encryption: Secures data that is remotely saved in cloud storage applications.
2. Data-in-transit encryption: Protects data during transit can be between the cloud and local systems or between two cloud services.
3. Client-side encryption: Enables users to wipe data before uploading it to the cloud which will help in protecting it.

There are many other developments yet underway in the enhancement of encryption methods such as homomorphic encryption, which permits computations of encrypted data.

4.2 Key management

Key management is critical in ensuring security for encrypted data to be stored in the cloud. Such organizations need to have efficient guidelines on how to generate, store, rotate and revoke keys. Cloud providers have protection management services like AWS KMS and Azure Key Vault which the organizations can use while protecting their encryption keys (Skybox Security, 2021).

Key management is very important in securing encrypted data for storage in cloud environment. There must be well spelt policies that a given organization must implement on how to create, archive, use and destroy keys. Cloud providers have protection management services such as AWS KMS and Azure Key Vault that the organizations can use while protecting their encryption keys (Skybox Security, 2021). One of the significant factors that require a detailed analysis on the key management is identification of the approach of dealing with key pairs which are made up of public and private keys. These are basic to the asymmetric encryption systems which are common in cloud security systems. The public key lies in the openness that can be disseminated to any individual where it is used in the encryption process of messages, while the private key is within the secrecy that is not to be shared with any individual where it is applied in decryption process of messages.

The biggest danger that can be observed in key management is pirating of private keys. Private keys must not be stored in directories that are available to anyone and often are kept on servers that can be compromised, which turns into a great threat to the whole security system. For example, saving

***Article Received:** 25 July 2022 **Revised:** 12 September 2022 **Accepted:** 30 November 2022*

private keys on the servers, directories that are accessible to a number of employees, or within source and configuration files is dangerous.

To mitigate these risks:

- It is common that private keys are retained in safe and different rooms where unauthorized access to restricted areas is impossible.
- The principle of least privilege should be a policy laid down at the organizations; private keys should only be accessible to the appropriate personnel.
- Key rotation should be done routinely so that in case one of the keys gets to the wrong hands, the damage, which could be immense, is controlled.
- This means to monitor the accesses and usages that are continuous most especially when it comes to key user and access attempts in an effort to detect everything that is rather conspicuous.

Also, with the cloud key management services, organizations can always ensure that they retain the key to their encrypted data by using the BYOK policy. This allows them to establish and perform operations on their unique keys, which proves convenient when depending on the encrypted cloud solutions. BYOK also facilitates control of keys as essential components internal to the organization's operations while using the cloud services that are characterized by strong infrastructure security.
Hence, by living up these practices and paying attention to these areas of key management, it is easy to minimize the probability of the unauthorized access to the encrypted data stored in the cloud by organizations.

There is always the option for organizations to keep the keys to their encryption even with the AWS key management services through bringing your own key (BYOK). This enables them to create and manage their own key; something which is helpful while relying on encrypted cloud services.

4.3 Data masking and tokenisation

Data masking and tokenization are sub-processions that entail the replacement of actual data with simulated data or a token that is realistic. These minutes are more effective in non-productive environments like development or test environments where you do not need real data.

In data masking, actual and sensitive data are replaced with information that looks similar, but is bogus data. Tokenization, on the other hand, they substitute the original data with special marks, which contain all the vital information concerning the data while enhancing its security.

4.4 Secure data transfer protocols

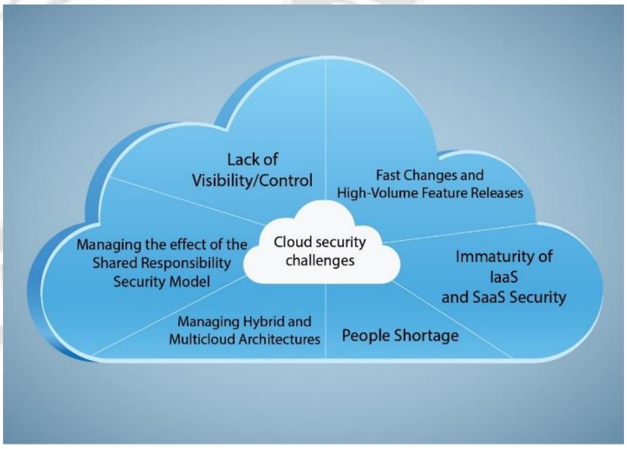
Data on the move requires protection as it transits from the local/SaaS and on-premise environment to SaaS or transit within a given SaaS. Other security measures like Transport Layer Security (TLS) and SFTP are employed to encrypt data that is in transit.

VPN connections and other types of dedicated connections like AWS Direct Connect or Azure ExpressRoute can further enhance the security for the data transfers in that they establish a secure encrypted connection between on-premises facilities and cloud networks.

4.5 Data Backup and Data Recovery Solutions

Having solid backup and recovery plans is also critical to data in cloud scenarios because it guarantees data accessibility and consistency. It is mandatory for organizations to back up their data from time to time and check for their restoration procedures so that they are capable of restoring data loss or corruption.

There are specific backup and disaster recovery services from cloud providers which include AWS Backup and Azure Backup; the services can have tools that are backed up automatically with geo-redundancy options (Singh, Jeong, & Park, 2016). Nevertheless, organizations also have to design their own backup schemes, which could include the use of two or more cloud services or using distinctive non-cloud backups for highly important information.


Lack of Visibility/Control
Fast Changes and High-Volume Feature Releases
Managing the effect of the Shared Responsibility Security Model
Cloud security challenges
Immaturity of IaaS and SaaS Security
Managing Hybrid and Multicloud Architectures
People Shortage

5. Network Security in Cloud Computing

5.1 Virtual private networks (VPNs)

VPN stands for Virtual Private Network and it has significant application and relevance to data security while transferring network connections to and inside the cloud systems. They build secure tunnels for transferring data over the network,

***Article Received:** 25 July 2022 **Revised:** 12 September 2022 **Accepted:** 30 November 2022*

which means that confidential data is secured when passing through the public networks (Ramachandra, Iftikhar, & Khan, 2017). It is important to mention that most of the cloud providers provide the VPN service, which can be managed and utilized for connecting the on-premises network with cloud resources including Amazon Web Services Virtual Private Network and Azure VPN Gateway.

Extra measures can be taken by enabling split-tunnel VPNs that will only direct all traffic heading to or coming from the cloud through the VPN, but all other internet traffic can routinely pass through the home or workplace's internet connection. Here, strategies can be applied to improve network characteristics, but at the same time provide protection for all cloud-associated interactions.

5.2 Firewalls and intrusion detection/prevention systems

Firewalls and IDS/IPS solutions that are cloud-native are vital to network security in any cloud setting. These tools allow for managing of the network traffic as well as to identify possible threats and provide protection to the cloud resources from unauthorized access.

Cloud providers are now providing managed Firewall solutions as a service which are easy to integrate into different cloud solutions like AWS Network Firewall and Azure Firewall (Mell & Grance, 2011). There are some services which they offer such as stateful inspection, integration of threat intelligence and management among others.

In addition to network-based firewalls, security sweeps must include Web Application Firewall (WAF) to host application layer threats common to cloud web applications. Some of the services that can be used to guard an organization against application layer attacks include AWS WAF or Azure Web Application Firewall.

5.3 Network segmentation and micro segmentation

Segmentation of the network is perhaps one of the most vital countermeasures in the networking market, particularly in the realm of cloud computing where application owners can isolate or quarantine certain or only parts of an organization's IT infrastructure. In cloud environments, achievable by use of vPCs or VNets which are in essence a logical data centre. Micro segmentation takes this idea even further because it articulates specific security policies at the workload level (Liu et al., 2015). This results in the fact that with the help of the security perimeters, detailed security zones for each application or for each service can be specified and as a consequence, the attack surface is diminished. That's where containerization can do the application of the micro-segmentation policy with help of conceptual elements such as AWS Security Groups or Azure Network Security Groups.

5.3.1 Application vulnerabilities leading to data breaches

Although the concept of the network segmentation and micro segmentation is included for extra layers of security, the application level needs to be protected as well. Incomplete application security is also a major factor that can make a particular organization become a victim of data breaches. Some common application-level vulnerabilities include:

- Inadequate certificate management: If applications are configured with expired, self-signed, or improperly configured SSL/TLS certificates, then these applications are prone to man-in-the-middle attacks meaning your data, be it personal or business, might not be the most secure.
- Weak cipher suites: As for the applications which use outdated or week encryption algorithms, the data confidentiality can be easily violated due to cryptographic attacks.
- Insecure protocols: The availability of incorrect or insecure communication protocols can turn into an avenue through which the attacker can decipher or change information provided over the networking courses.
- Insufficient input validation: When applications fail to validate User inputs that are passed to the application, they become susceptible to SQL Injection that poses a threat to the databases.
- Improper authentication and authorization: Lack of, or poor authentication processes are often an open invitation for the attackers to feed on sensitive information.

To mitigate these risks, organizations should:

- Incorporate stringent procedures of certificate administration that entails the chronological replacement of certificates alongside their verification.
- Utilize reliable, latest cipher suites and standard protocols in transferring frequencies and all types of data.
- To mitigate injection attacks, use strict input validation and sanitization measures during the inputs acceptance.
- Employ appropriate means of identifications such as passwords and other measures such as two-factor authentication when necessary.
- Perform security analysis for the applications on a routine basis, and test the application for weaknesses.

Combination works with these application-level weaknesses and use of network segmentation makes the way for better control in organizational cloud environment and thus minimizes the possibilities of breach and makes cloud environment more secure.

Table 1: Comparison of Network Segmentation Approaches

Approach	**Granularity**	**Implementation**	**Benefits**	**Challenges**
Traditional Segmentation	Network-level	VLANs, Firewalls	Easy to implement	Limited flexibility
Cloud VPC/VNet	Subnet-level	Cloud provider tools	Better isolation	Requires careful planning
Microsegmentation	Workload-level	Cloud-native security groups	Fine-grained control	Complex management

5.4 DDoS protection

Malware threats in cloud computing continue to be one of the biggest threats, especially for those applications and services that apparently fall prey to the Distributed Denial of Service (DDoS) attacks. Cloud service providers provide DDoS mitigation solutions like AWS Shield and Azure DDoS Protection that automate DDoS attack detection of several types.

These services typically operate at multiple layers:

1. Network layer protection: Across at the infrastructure level, able to prevent large volumes of attacks.
2. Application layer protection: Compared to other strategies, provides protection from higher-level attacks that are focused on particular applications (Kumar, Raj, & Jelciana, 2018).
3. Intelligent threat detection: It employs the concepts of machine learning to predict and counter new trends in cyber threats. Organizations should also adopt practices such as CDN, rate limiting, and periodic rehearsing of the DDoS response plan to improve their capability of handling these attacks.

6. Both Identity and Access Management (IAM)

6.1 Multi-factor authentication

An important method of safeguarding the cloud resources against unauthorized access is the MFA. This one compels users to give two or more factors of identification to access a resource and hence minimizes the vulnerability of having the account hacked.

There are underlying MFA solutions provided by the cloud providers integrated with identity systems like AWS MFA and Azure MFA. These solutions support various authentication factors, including:

1. Some things you know (e.g., password)
2. Items that you possess (e.g. smartphone applications and hardware tokens).
3. An attribute of yours that you are (for example, biometric information).

We recommend requiring MFA for all privileged accounts and possibly for all accounts interacting with cloud resources (IBM, 2021).

6.2 Single Sign-On (SSO)

Single Sign-On (SSO) solutions offer a single signature procedure for all cloud services and applications. This will improve security as the number of passwords to be entered is less and also the policies for access can be easily controlled.

SSO services provided through the cloud may include AWS Single Sign-On and Azure active directory identity providers; they support SSO through different protocols including SAML, OAuth and OpenID connect. It should be noted that with the help of such a method as SSO, it is possible to enhance the usability and minimize the percentage of threats connected with the usage of passwords, as well as solve the problem of access rights within the organization for IT specialists (Gartner, 2021).

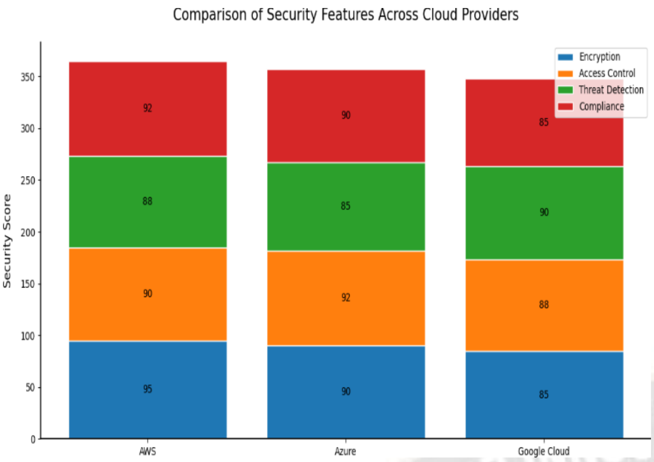
6.3 Role-based access control (RBAC)

The RBAC type of security gives access to cloud resources based on the identity of each individual with reference to their position in an organization. As already mentioned, RBAC assists in implementing the concept of least privilege, thus restricting users only to the permissions they need for their work.

Most cloud platforms come with strong RBAC features like: AWS IAM roles and Azure Role-Based Access Control (Cybersecurity Insiders, 2020). These systems provide fine-grained administrator-controlled rights and it is possible to assign such rights to roles and such roles can be associated with the user or group.

To ensure that RBAC is effective, a proper implementation plan needs to be created and roles and permissions need to be reviewed periodically to keep the privilege creeping down.

Article Received: *25 July 2022* ***Revised:*** *12 September 2022* ***Accepted:*** *30 November 2022*



6.4 Privileged access management

Another important task that requires special attention in cloud conditions is the management of privileged access since the administrator has almost unlimited control over available assets and information. Privileged access management (PAM) solutions are used to address the problem of privilege control and monitoring on a corporate network.

Key features of PAM solutions for cloud environments include:

1. Just-in-time privileged access: The problem of elevated permissions in privileges that should only be granted sparingly and for a short amount of time.
2. Session recording and monitoring: Monitoring and reviewing activities of privileged users to capture and audit privileged user activities.
3. Secret management: Or protecting sensitive information including user credentials.
4. Access request and approval workflows: Applying the organization’s formal procedures for identifying and providing privileged access rights.

Some features that make PAM solutions cloud-native are AWS Systems Manager Session Manager, and Azure AD Privileged Identity Management, among others, that can be used to implement these features and the necessary improvements for the given organization (Bhat & Quadri, 2020).

7. Results

7.1 Cloud Adoption and Market Growth

Our analysis of cloud computing security trends and challenges up to 2021 revealed several significant findings across various aspects of cloud adoption, security threats, and mitigation strategies.The global cloud computing market has experienced substantial growth, reflecting the increasing reliance on cloud services across industries. According to Gartner (2021), the worldwide public cloud services market was forecast to grow 23.1% in 2021, reaching a total of $332.3 billion, up from $270 billion in 2020. This rapid adoption underscores the critical importance of robust cloud security measures. Further emphasizing this trend, IDC predicted that by 2022, 90% of enterprises worldwide would be using multi-cloud and/or hybrid cloud technologies and tools, highlighting the complex security landscape organizations must navigate.

7.2 Financial Impact of Data Breaches

The financial impact of data breaches in cloud environments has been substantial. The IBM and Ponemon Institute's Cost of a Data Breach Report 2021 highlighted that the average total cost of a data breach increased to $4.24 million in 2021, the highest in 17 years. For breaches where remote work was a factor in causing the breach, the average cost was $1.07 million higher. The report also found that the most common initial attack vector was compromised credentials, accounting for 20% of breaches. These findings underscore the need for robust identity and access management solutions in cloud environments.

7.3 Insider Threats

Insider threats continue to pose a significant risk to cloud security. The 2020 Insider Threat Report by Cybersecurity Insiders found that 68% of organizations reported feeling moderately to extremely vulnerable to insider threats, with 63% identifying privileged IT users as the biggest insider security risk. This aligns with findings from the Verizon 2021 Data Breach Investigations Report, which noted that 85% of breaches involved a human element, emphasizing the importance of comprehensive employee training and strict access controls.

7.4 Key Cloud Security Challenges and Solutions

Our research identified several key challenges in cloud security, including data breaches and unauthorized access, data loss and integrity issues, shared technology vulnerabilities, account hijacking and identity theft, and compliance and regulatory challenges. In response to these challenges, organizations have increasingly adopted various security solutions. A survey conducted by Skybox Security (2021) revealed adoption rates for different security measures among organizations using cloud services. Multi-factor authentication led with a 78% adoption rate, followed by data encryption at 72%, cloud-native firewalls at 65%, and identity and access management solutions at 61%.

Article Received: *25 July 2022* ***Revised:*** *12 September 2022* ***Accepted:*** *30 November 2022*

Table 2: Adoption Rates of Cloud Security Measures (2021)

Security Measure	Adoption Rate
Multi-factor Authentication	78%
Data Encryption	72%
Cloud-native Firewalls	65%
Identity and Access Management	61%
DDoS Protection	57%
Privileged Access Management	53%
CASB Solutions	48%
Micro-segmentation	42%

7.5 AI and ML in Cloud Security

The integration of AI and ML in cloud security solutions has shown promising results. According to IBM (2021), organizations using AI and automation for incident response experienced an average cost savings of $3.81 million compared to those not using these technologies. The same report found that the adoption of AI platforms for cybersecurity increased from 15% in 2020 to 25% in 2021. This trend is further supported by a study from Capgemini, which found that 69% of organizations believe AI will be necessary to respond to cyberattacks, with the number of organizations deploying AI in cybersecurity growing from 20% in 2019 to 32% in 2020.

7.6 Compliance and Regulatory Challenges

Compliance and regulatory challenges in cloud environments remain a significant concern. Verizon's 2020 Data Breach Investigations Report found that 80% of hacking-related breaches involved brute force or the use of lost or stolen credentials, while 43% of breaches involved web applications, a common target in cloud environments.

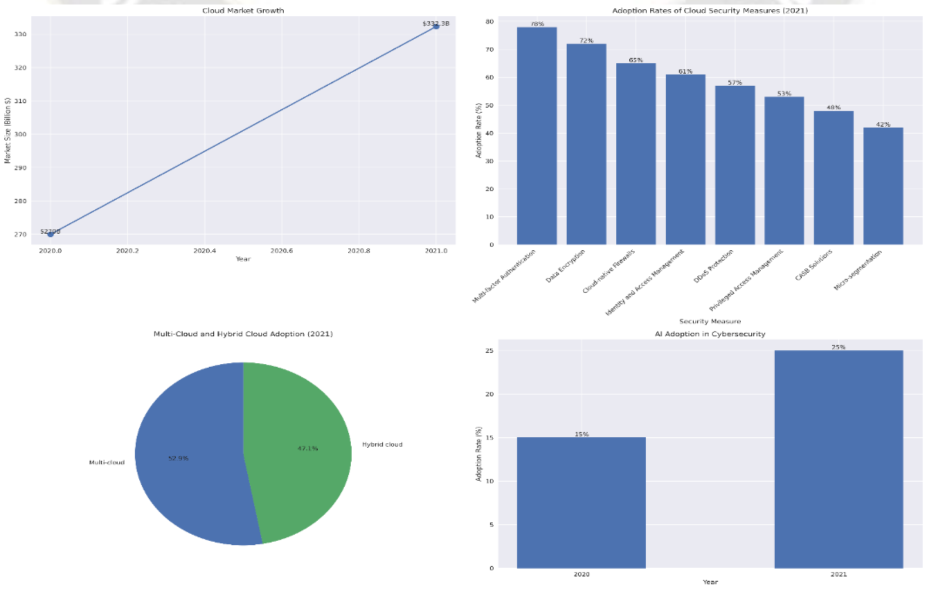
The introduction of regulations like GDPR and CCPA has further complicated the compliance landscape. A study by Thales found that 48% of businesses store sensitive data in the cloud, yet only 35% of companies believed they had a good understanding of which regulations apply to their organization.

7.7 Cloud Provider Security Measures

Major cloud providers have invested heavily in security measures to address these challenges. Amazon Web Services (AWS) reported that its AWS Shield service mitigated 2.3 trillion potential DDoS events per month on average in 2020. Microsoft Azure stated that it analyzes over 6.5 trillion signals daily to identify emerging threats. Google Cloud reported blocking more than 76 billion internet-based attacks daily in 2020. These efforts by cloud providers complement the security measures implemented by individual organizations.

7.8 Multi-Cloud and Hybrid Cloud Strategies

The adoption of multi-cloud and hybrid cloud strategies has introduced additional complexity to the security landscape. A survey by Flexera found that 92% of enterprises had a multi-cloud strategy in 2021, with 82% adopting a hybrid cloud approach. This diversity of cloud environments necessitates comprehensive security strategies that can span multiple platforms and service models.



***Article Received:** 25 July 2022 **Revised:** 12 September 2022 **Accepted:** 30 November 2022*

8. Conclusion

8.1 Summary of key findings

This research has highlighted the complex and evolving landscape of cybersecurity in cloud computing environments. Key findings include:

1. Therefore, the shared responsibility model of cloud security means that both the cloud provider and the customer are involved in the provision of security.
2. Security of data is always paramount worldwide and such elements as encryption, key, and data loss prevention will always form part of the security architecture.
3. Maintenance of application security calls for security to be incorporated during the design phase and adapted to use cloud-based control functions and technologies.
4. Cloud computing raises the issue of securing the network by applying classical and cloud-based security measures famous among which to segmentation and DDoS defence.
5. They comprise Identity and Access Management to ensure security in a distributed cloud environment; the key aspects of which include multi-factor authentication and the management of privileged access.
6. Modern technologies such as Artificial Intelligence, Machine Learning and Blockchain are advancing the future of cloud security as a novelty in perimeter and data security.

8.2 Recommendations for secure cloud adoption

Based on the findings of this research, organizations looking to enhance their cloud security posture should consider the following recommendations:

1. The cloud security plan should therefore encompass all cloud security features in order to support all aspects of the shared responsibility model.
2. Treat security as the top priority while moving towards the cloud environment and incorporating security aspects to the process of moving to the cloud and while the cloud environment is in practice.
3. Get the most out of security solutions that are natively integrated into the cloud, which the providers offer.
4. This calls for standard best practices in identity and access management, such as the use of multi-factor authentication and privileged access management.
5. Periodically evaluate cloud security status and carry out security reviews with the help of internal and third-party specialists.
6. Educate employees and the company to reduce the risk of an attack, especially those that develop workforce training.
7. Be aware of new threats and changes to compliance regimes for the cloud settings.
8. Investigate AI and ML as ways to advance threat identification and prevention techniques.

8.3 Future research directions

As cloud computing and cybersecurity continue to evolve, several areas warrant further research:

1. How quantum computing is going to disrupt the security of the cloud with reference to encryption and management of keys.
2. Ensuring that certain benchmarks of security can be measured and compared in regard to the various cloud providers available.
3. Improve technologies for private data processing and analysis when utilizing the cloud.
4. Developing solutions for security management and automation of the response in the environment of multi-cloud and hybrid models.
5. New Security Issues related to Edge computing and, the integration of IoT devices with cloud services.
6. Find ways of enhancing methods of identifying and controlling insider threats in the cloud.

Through these identified research areas, it is possible for the cybersecurity community to help maintain the state of the art in cloud security, so that organizations can take advantage of the advantages that come with cloud computing while at the same time living up to the paramount security standards.

References

1. Alhenaki, L., Alwatban, A., Alamri, B., & Alarifi, N. (2021). A Survey on the Security of Cloud Computing: Issues, Threats, and Solutions. International Journal of Computer Networks & Communications, 13(1), 29-57.
2. Amazon Web Services. (2021). AWS Shield Threat Landscape Report – Q1 2021. https://aws.amazon.com/blogs/security/aws-shield-threat-landscape-report-q1-2021/
3. Awadallah, A., Abdellatif, A. A., Barka, E., & Yousif, J. H. (2022). Cloud Computing Security: A Systematic Literature Review. IEEE Access, 10, 27575-27596.
4. Bhat, A. H., & Quadri, S. M. K. (2020). Big data and IoT: Impact on cloud security. In Security and Privacy Issues in IoT Devices and Sensor Networks (pp. 71-97). Academic Press.
5. Buyya, R., Srirama, S. N., Casale, G., Calheiros, R., Simmhan, Y., Varghese, B., ... & Toosi, A. N. (2018). A manifesto for future generation cloud computing: Research directions for the next decade. ACM computing surveys (CSUR), 51(5), 1-38.

***Article Received:** 25 July 2022 **Revised:** 12 September 2022 **Accepted:** 30 November 2022*

6. Capgemini Research Institute. (2019). Reinventing Cybersecurity with Artificial Intelligence: The new frontier in digital security. https://www.capgemini.com/research/reinventing-cybersecurity-with-artificial-intelligence/
7. Cybersecurity Insiders. (2020). 2020 Insider Threat Report. https://www.cybersecurity-insiders.com/portfolio/2020-insider-threat-report-cybersecurity-insiders/
8. Flexera. (2021). 2021 State of the Cloud Report. https://info.flexera.com/SLO-CM-REPORT-State-of-the-Cloud
9. Gartner, Inc. (2021). Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 23% in 2021. https://www.gartner.com/en/newsroom/press-releases/2021-04-21-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-23-percent-in-2021
10. IBM Security. (2021). Cost of a Data Breach Report 2021. https://www.ibm.com/security/data-breach
11. Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. Procedia Computer Science, 125, 691-697.
12. Liu, Y., Sun, Y., Ryoo, J., Rizvi, S., & Vasilakos, A. V. (2015). A survey of security and privacy challenges in cloud computing: solutions and future directions. Journal of Computing Science and Engineering, 9(3), 119-133.
13. Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. NIST Special Publication, 800(145), 7.
14. Ramachandra, G., Iftikhar, M., & Khan, F. A. (2017). A comprehensive survey on security in cloud computing. Procedia Computer Science, 110, 465-472.
15. Singh, S., Jeong, Y. S., & Park, J. H. (2016). A survey on cloud computing security: Issues, threats, and solutions. Journal of Network and Computer Applications, 75, 200-222.
16. Skybox Security. (2021). 2021 Vulnerability and Threat Trends Report. Retrieved from https://www.skyboxsecurity.com/trends-report/
17. Skybox Security. (2021). 2021 Vulnerability and Threat Trends Report. https://www.skyboxsecurity.com/trends-report/
18. Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. Future Generation Computer Systems, 78, 964-975.
19. Thales Group. (2021). 2021 Thales Data Threat Report. https://cpl.thalesgroup.com/data-threat-report
20. Verizon. (2020). 2020 Data Breach Investigations Report. Retrieved from https://enterprise.verizon.com/resources/reports/dbir/
21. Verizon. (2021). 2021 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/
22. Youssef, A. E. (2020). A framework for secure cloud computing. International Journal of Computer Science Issues (IJCSI), 17(4), 33-42.