Scientific Research Publishing

Int. J. Communications, Network and System Sciences, 2024, 17, 69-80
https://www.scirp.org/journal/ijcns
ISSN Online: 1913-3723
ISSN Print: 1913-3715

Information Security in the Cloud: Emerging Trends and Challenges

Keerthana Chitreddy, Andrew Mikhl Anthony, Chinna Manikanta Bandaru, Olatunde Abiona

Department of Computer Information Systems, Indiana University Northwest, Gary, IN, USA
Email: kechit@iu.edu, andanth@iu.edu, cbandaru@iu.edu, oabiona@iun.edu

How to cite this paper: Chitreddy, K., Anthony, A.M., Bandaru, C.M. and Abiona, O. (2024) Information Security in the Cloud: Emerging Trends and Challenges. *Int. J. Communications, Network and System Sciences*, **17**, 69-80.
https://doi.org/10.4236/ijcns.2024.175005

Received: January 23, 2024
Accepted: May 28, 2024
Published: May 31, 2024

Abstract

This article explores the evolution of cloud computing, its advantages over traditional on-premises infrastructure, and its impact on information security. The study presents a comprehensive literature review covering various cloud infrastructure offerings and security models. Additionally, it deeply analyzes real-life case studies illustrating successful cloud migrations and highlights common information security threats in current cloud computing. The article concludes by offering recommendations to businesses to protect themselves from cloud data breaches and providing insights into selecting a suitable cloud services provider from an information security perspective.

Keywords

Cloud Computing, Information Security, Cloud Infrastructure Offerings, Cloud Migration, Security Measures, Data Breaches, Cloud Service Providers, Cybersecurity, Cloud Security, Case Studies, Cloud Threat Landscape, Data Encryption, Compliance, Cloud Security Tools

1. Introduction

The concept of cloud computing can be traced back to the 1950s and 1960s, but it wasn't until the early 2000s that it began to gain traction. In 2002, Amazon launched AWS, which offered developers access to computing and storage resources on a pay-as-you-go basis. AWS was the first major cloud computing platform, and it quickly became the standard for the industry.

Other major cloud providers, such as Microsoft Azure and Google Cloud Platform, followed suit in the late 2000s and early 2010s. Today, cloud computing is a multi-billion-dollar industry, and it is used by businesses of all sizes around the world.

Figure 1 shows Cloud vs on-premises computing where Cloud computing has become famous and stood as an alternative to traditional on-premises IT infra-

structure for several reasons, including:

• Cost savings: Cloud computing can help businesses save money on IT costs by eliminating the need to purchase and maintain their own hardware and software. Businesses only pay for the cloud resources they use, and they can scale their usage up or down as needed.

• Agility and scalability: Cloud computing allows businesses to deploy new applications and services quickly and easily. It also makes it easy to scale applications and services up or down in response to changing demand.

• Reliability: Cloud providers offer a high level of reliability and uptime. They have large networks of data centers around the world, and they use redundant systems to ensure that their services are always available.

• Security: Cloud providers offer a variety of security features to protect customer data. They also have teams of security experts who are constantly monitoring their systems for threats. [1]

Cloud infrastructure gained its popularity and practice rapidly, which necessarily classified it into further sections based on offerings and models

Cloud Infrastructure Offerings

Figure 2 shows the types of cloud offerings. There are three main types of cloud infrastructure offerings:

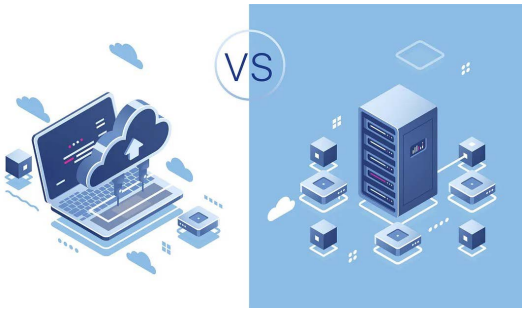

Figure 1. Cloud vs on-premise computing.

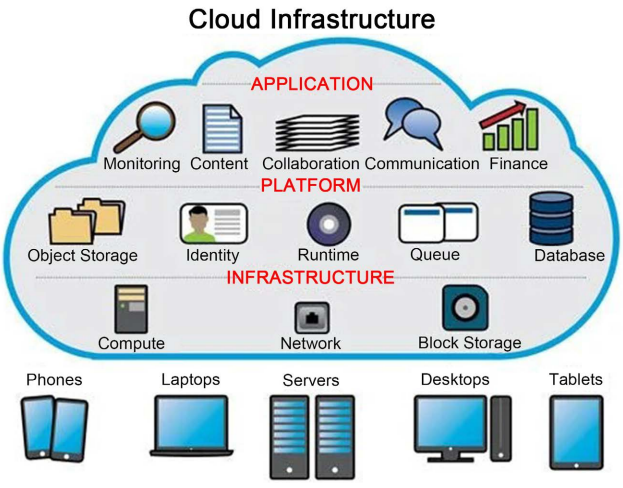

Figure 2. Types of cloud offerings.

1) Infrastructure as a Service (IaaS): IaaS provides businesses with access to computing resources, such as computing power, storage, and networking. Enterprises can use IaaS to design, build, test, and deploy their proprietary applications and services.

2) Platform as a Service (PaaS): PaaS provides businesses with a platform for developing, deploying, and managing their own applications. PaaS includes all the necessary resources, such as operating systems, databases, and development tools.

3) Software as a Service (SaaS): SaaS provides businesses with access to software applications over the internet. SaaS applications are typically hosted by the cloud provider and accessed by users through a web browser. This is often referred to as application as a service. [2]

2. Models of Cloud Computing and Their Security

Figure 3 shows types of cloud models. The four main models of cloud computing are:

1) Public cloud: Public cloud services are available to anyone with an internet connection. Public cloud providers, such as AWS, Azure, and GCP, offer a wide range of services, including IaaS, PaaS, and SaaS.

Public cloud providers offer a variety of security features to protect customer data, but it is important for businesses to choose a provider with a strong security track record and to implement their own security measures, such as data encryption and access controls.

2) Private cloud: Private cloud services are hosted on premises or in a dedicated data center. Private clouds offer businesses more control over their security and compliance needs, but they can be more expensive and complex to manage than public clouds.

Private clouds can be very secure if they are properly designed and managed. However, it is important for businesses to have a team of security experts who can monitor and maintain their private cloud infrastructure.

3) Hybrid cloud: Hybrid clouds combine public and private cloud services. Hybrid clouds can offer businesses the best of both worlds: the scalability and cost-effectiveness of public clouds with the security and control of private clouds.

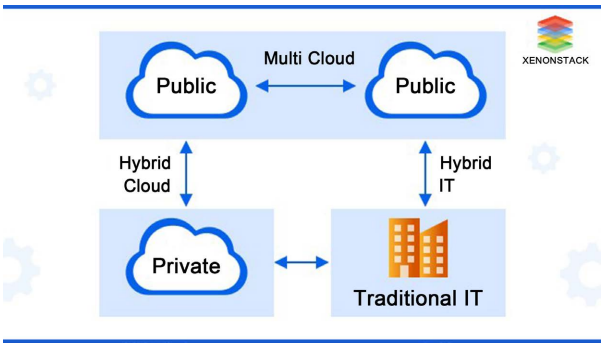

Figure 3. Types of cloud models.

Hybrid clouds can be more complex to secure than public or private clouds because businesses need to manage security across multiple environments. However, there are several security tools and services available to help businesses secure their hybrid cloud environments.

4) Multi-cloud: Multi-cloud environments use multiple cloud providers. Multi-cloud environments can help businesses reduce risk and improve performance by distributing their workloads across multiple cloud providers.

Multi-cloud environments can be even more complex to secure than hybrid clouds because businesses need to manage security across multiple cloud providers and multiple cloud platforms. However, there are several security tools and services available to help businesses secure their multi-cloud environments. [3]

3. Case Study Analysis on Cloud Migration

Cloud migration is the process of moving data, applications, and other IT resources from an on-premises environment to a cloud computing platform. It can be a complex process, but it can also offer several benefits for businesses of all sizes.

In addition to these general cloud benefits, cloud migration can also offer specific benefits for businesses in different industries. For example, cloud migration can help healthcare businesses comply with HIPAA regulations, and it can help retail businesses improve their customer experience.

Figure 4 shows cloud migration success stories. Here are some real-life examples of how specific companies have benefited from cloud migration:

Company	Migration Objective	Migration Type	Key Takeaways
Betabrand	Improve scalability and reliability	Bare metal to cloud	Cloud streamlines load testing and scalability is key to customer satisfaction
Spotify	Reduce costs and improve scalability	Bare metal to cloud	Gaining stakeholder buy-in is crucial and migration preparation shouldn't be rushed
Waze	Improve stability and reliability	Cloud to multi-cloud	Some business models may be a better fit for multiple clouds and deploying software more frequently doesn't have to mean reduced stability/reliability
Dropbox	Reduce costs, increase control, and maintain competitive edge	Cloud to hybrid	On-premise infrastructure may still be right for some businesses and size matters
GitLab	Improve performance and reliability	Cloud to cloud	Containers are seen by many as the future of DevOps and an enormous benefit, improved stability, and availability can be an enormous benefit of cloud migration
Cordant Group	Reduce costs and improve efficiency	Bare metal to hybrid	Business and user needs drive cloud needs and cloud ROI ultimately depends on how your business measures ROI
Shopify	Ensure they were using the best tools possible to support the evolution needed to meet increasing customer demand	Cloud to cloud	Immutable infrastructure vastly improves deployments

Figure 4. Cloud migration success stories.

1) Beta brand: Beta brand is a crowd-funded, crowd-sourced retail clothing e-commerce company. The company migrated to the cloud in 2017 to improve the scalability and reliability of its IT infrastructure. After migrating to the cloud, Beta brand experienced a 30% decrease in website downtime and a 20% increase in website traffic.

2) Spotify: Spotify is a music streaming service. The company migrated to the cloud in 2015 to reduce costs and improve the scalability of its IT infrastructure. After migrating to the cloud, Spotify was able to reduce its IT costs by 20% and scale its IT infrastructure to support over 100 million users.

3) Waze: Waze is a GPS navigation app. The company migrated to the cloud in 2010 to improve the performance and reliability of its app. After migrating to the cloud, Waze was able to reduce app downtime by 90% and improve its overall performance by 20%.

4) Dropbox: Dropbox is a file hosting service. The company migrated to the cloud in 2007 to improve the scalability and reliability of its service. After migrating to the cloud, Dropbox was able to scale its service to support over 500 million users.

5) GitLab: GitLab is a software development platform. The company migrated to the cloud in 2015 to improve the performance and reliability of its platform. After migrating to the cloud, GitLab was able to reduce app downtime by 95% and improve its overall performance by 25%.

6) Cordant Group: Cordant Group is a global social enterprise that provides a range of services and solutions. The company migrated to the cloud in 2016 to reduce costs and improve the efficiency of its IT operations. After migrating to the cloud, Cordant Group was able to reduce its IT costs by 15% and improve the efficiency of its IT operations by 20%.

7) Shopify: Shopify is an e-commerce platform. The company migrated to the cloud in 2006 to improve the scalability and reliability of its platform. After migrating to the cloud, Shopify was able to scale its platform to support over 1 million merchants.

However, businesses should consider some additional things to consider when planning your cloud migration:

Data security: When migrating your data to the cloud, it is important to choose a cloud provider that offers robust security features and services. You should also develop a data security plan to protect your data from unauthorized access, use, disclosure, disruption, modification, or destruction.

Compliance: If your business is subject to any industry-specific regulations, you need to make sure that your cloud migration plan complies with those regulations.

Downtime: Cloud migration can typically be completed with minimal downtime, but it is important to have a plan in place in case of any unforeseen problems.

Training: Once your data and applications have been migrated to the cloud,

you will need to train your employees on how to use the new cloud environment.

These case studies show that cloud computing can certainly help businesses improve their information security posture. However, it is important to note that cloud computing is not a silver bullet. Businesses still need to implement appropriate security measures, such as data encryption and access controls, to protect their data in the cloud.

4. Common Information Security Threats with Current Cloud Computing

Some of the most common information security threats with current cloud computing include:

1) Data breaches: Data breaches are the most common type of information security incident, and they can be very costly for businesses. Data breaches can occur when hackers gain unauthorized access to cloud-based data. Below **Figure 5** shows Data breach symbolic image.

2) Malware: Malware is malicious software that can be used to steal data, damage systems, or disrupt operations. Malware can spread to cloud-based systems through email attachments, infected websites, or vulnerable software. Below **Figure 6** shows Malware symbolic image.

Figure 5. Data breach symbolic image.

Figure 6. Malware symbolic image.

Phishing attacks: Phishing attacks are attempts to trick users into revealing sensitive information, such as passwords or credit card numbers. Phishing attacks can be carried out through email, social media, or malicious websites. Below **Figure 7** shows Phishing symbolic image.

3) Denial-of-service attacks: Denial-of-service attacks are attempts to overwhelm a cloud-based system with traffic, making it unavailable to legitimate users. Denial-of-service attacks can be carried out using botnets, which are networks of compromised computers. Below **Figure 8** shows Denial-of-service symbolic image.

Following are some real-life cases to realize the impact of breaches on businesses hosted in cloud infrastructure.

Cloud data breaches have become increasingly common in recent years, as more and more businesses move their data to the cloud. Cloud data breaches can have a significant impact on businesses, both financially and reputationally. [4]

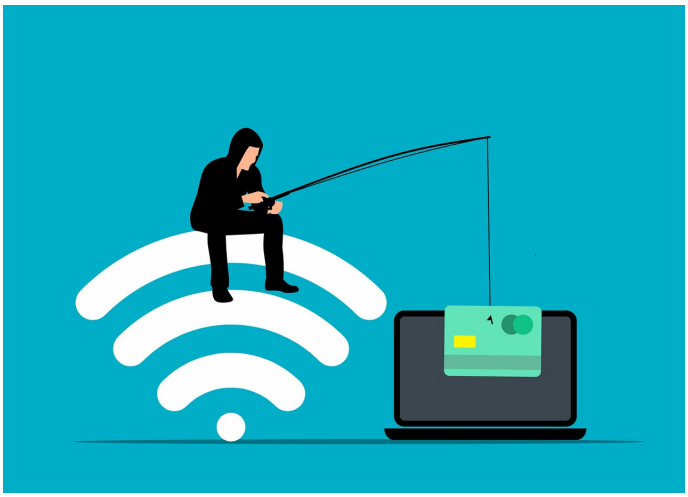

Figure 7. Phishing symbolic image.

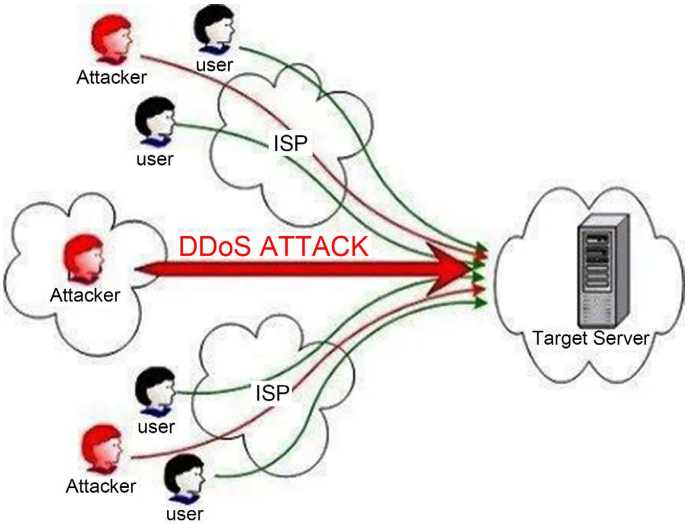

Figure 8. Denial-of-service symbolic image.

Figure 9 shows Cloud infra information security incidents stats. Here are some of the most infamous cloud data breaches in real time.

Facebook: In 2019, Facebook was breached and the personal data of over 530 million users was stolen. The data included phone numbers, full names, locations, some email addresses, and other details from user profiles.

Alibaba: In 2019, Alibaba's Chinese shopping website Taobao was attacked and the data of over 1.1 billion users was exposed. The stolen data included user IDs, mobile phone numbers, and customer comments. [5]

LinkedIn: In 2021, LinkedIn was also breached and the data of over 700 million users was exposed. The data included email addresses, phone numbers, geolocation records, genders, and other social media details. [6]

Sina Weibo: In 2020, Sina Weibo, one of China's largest social media platforms, was breached and the personal details of over 538 million users were exposed. The data included real names, site usernames, gender, and location, as well as phone numbers for 172 million users.

Accenture: In 2021, Accenture was hit by a ransomware attack and the data of over 6 terabytes of data was stolen. The data included proprietary corporate data and customer data.

Cognyte: In 2021, cyber analytics firm Cognyte failed to secure its database, exposing 5 billion records detailing previous data incidents. The records were posted online without a password, or any other authentication required to access them.

Toyota Motor Company: In 2023, Toyota Motor Company said approximately 260,000 customers' data was exposed online due to a misconfigured cloud environment. The data included in-vehicle device ID, map data updates, updated data creation dates, and map information and its creation date (not vehicle location).

Year	Company	Type of breach	Other stats	Impact
2023	Toyota Motor Company	Misconfigured cloud environment	260,000 customers affected	Low
2021	Cognyte	Database exposed	5 billion records exposed, including names, email addresses, and data sources	Medium
2021	Accenture	Ransomware attack	6 terabytes of data stolen, including proprietary corporate data and customer data	High
2020	Sina Weibo	Data scraping	538 million users affected, including real names, site usernames, gender, location, and phone numbers for 172 million users	High
2021	LinkedIn	Data scraping	700 million profiles affected, including email addresses, phone numbers, geolocation records, genders, and other social media details	Medium
2019	Alibaba	Data scraping	1.1 billion users affected, including user IDs, mobile phone numbers, and customer comments	High
2019	Facebook	Data breach	530 million users affected, including phone numbers, full names, locations, some email addresses, and other details from user profiles	High

Figure 9. Cloud infra information security incidents stats.

Recommendations to Businesses do to protect themselves from cloud data breaches:

Choose the right cloud provider. Not all cloud providers are created equal. Some cloud providers offer better security features than others. Businesses should carefully choose a cloud provider that offers the security features that they need.

Implement strong security controls. Businesses should implement strong security controls, such as multi-factor authentication and encryption, to protect their data in the cloud.

Regularly monitor cloud environments. Businesses should regularly monitor their cloud environments for suspicious activity. This will help them to identify and respond to cloud data breaches quickly.

Educate employees about cloud security. Businesses should educate their employees about cloud security best practices. This will help to reduce the risk of human error leading to a cloud data breach.

Have a plan in place to respond to cloud data breaches. Businesses should have a plan in place to respond to cloud data breaches quickly and effectively. This plan should include steps to notify affected customers, contain the breach, and recover from the breach.

By following these recommendations, businesses can help to protect themselves from cloud data breaches.

In addition to the above recommendations, businesses should also consider the following:

1) Use a cloud security platform. A cloud security platform can help businesses to protect their data in the cloud by providing a variety of security features, such as intrusion detection and prevention, encryption, and data loss prevention.

2) Use a cloud access security broker (CASB). A CASB can help businesses to control access to their data in the cloud and to monitor cloud activity for suspicious activity.

3) Segment their cloud networks. Segmenting cloud networks can help to reduce the spread of malware in the event of a cloud data breach.

4) Regularly back up their data. Businesses should regularly back up their data to a secure location outside of the cloud. This will ensure that they have a copy of their data in case of a cloud data breach. [7]

By taking these steps, businesses can help to protect their data in the cloud and reduce the risk of a cloud data breach.

5. Cloud Services Providers & Job Market Impact

5.1. Cloud Services Providers & Market Share Stats

Figure 10 shows Cloud service provider stats. The three most famous cloud providers are:

Amazon Web Services (AWS)

Factor	AWS	Azure	GCP
Market share	30%	20%	10%
Services offered	Broadest range of services	Wide range of services	Wide range of services
Maturity	Most mature cloud platform	Second-most mature cloud platform	Third-most mature cloud platform
Pricing	Variety of pricing options	Variety of pricing options	Variety of pricing options
Free trial	Yes	Yes	Yes

Figure 10. Cloud service provider stats.

AWS is the oldest and most mature cloud platform, with a wide range of services and features. It is the market leader in cloud computing, with a market share of over 30%. AWS offers a broad range of services, including computing, storage, databases, networking, analytics, machine learning, and artificial intelligence.

Microsoft Azure

Azure is a cloud platform that offers a wide range of services, including computing, storage, databases, networking, analytics, machine learning, and artificial intelligence. It is the second-largest cloud provider, with a market share of over 20%. Azure is particularly well-suited for businesses that are already using Microsoft products and technologies.

Google Cloud Platform (GCP)

GCP is a cloud platform that offers a wide range of services, including computing, storage, databases, networking, analytics, machine learning, and artificial intelligence. It is the third-largest cloud provider, with a market share of over 10%. GCP is particularly well-suited for businesses that are using Google products and technologies. [8]

All three cloud providers offer a free trial, so you can try them out before you commit to a paid plan. They also offer a variety of pricing options, so you can choose the one that best meets your needs.

5.2. Job Market Impact

Cloud computing has had a significant impact on the job market, creating new jobs and changing the nature of existing ones.

Due to the diverse applications and various cloud service providers various new job titles have originated and affected the job market. The following are the predominantly new jobs often hired for in cloud practice.

1) Cloud architects: Design and implement cloud-based solutions.

2) Cloud engineers: Build and manage cloud-based infrastructure and applications.

3) Cloud security engineers: Protect cloud-based systems and data from unauthorized access.

4) Cloud DevOps engineers: Automate and streamline the development, deployment, and management of cloud-based applications.

5) Cloud support engineers: Provide technical support to cloud users.

Changing nature of existing jobs:

IT professionals: Cloud computing has changed the way IT professionals work, requiring them to develop new skills and knowledge. For example, IT administrators now need to be familiar with cloud-based infrastructure and applications.

Business users: Cloud computing has made it easier for business users to access and use IT resources, without having to rely on IT departments. As a result, business users are now more involved in the selection and deployment of IT solutions.

Overall, cloud computing has created a more dynamic and innovative job market for IT professionals and business users alike.

Cloud computing is expected to create 14 million new jobs between 2011 and 2015. Cloud-related jobs will accrue evenly to businesses with 500 or fewer employees and those with more than 500 employees. More than one-third of cloud-enabled jobs will occur in the communications and media, banking, and discrete manufacturing industries. China and India will account for about half of all new cloud-related jobs. [9]

6. How to Pick a Cloud Services Provider in Information Security Perspective

When choosing a cloud services provider, businesses should consider the following security factors:

1) Security track record: Businesses should choose a provider with a strong security track record. This includes a history of protecting customer data and a commitment to continuous security improvement.

2) Security features: Businesses should choose a provider that offers a variety of security features, such as data encryption, access controls, and intrusion detection systems.

3) Compliance certifications: Businesses should choose a provider that has been audited and certified to meet relevant security standards, such as ISO/IEC 27001 and PCI DSS.

4) Transparency: Businesses should choose a provider that is transparent about its security practices. This includes providing customers with information about the security measures that are in place to protect their data.

By considering these factors, businesses can choose a cloud services provider that will help them improve their information security posture. [10]

7. Conclusions

Cloud computing has revolutionized the IT landscape, offering businesses flexibility, scalability, and cost savings. This research paper explored the evolution of cloud computing, its various service models, and the security considerations associated with its adoption.

Key findings highlight the diverse benefits of cloud migration, including improved scalability, reliability, and access to advanced technologies. However, businesses must remain vigilant against potential security threats like data breaches, malware, and phishing attacks.

The paper delved into the impact of cloud computing on the job market, showcasing the emergence of new positions like cloud architects and engineers, while emphasizing the necessary skill development for existing IT professionals. Choosing the right cloud provider is crucial, and security factors such as a strong track record, robust features, compliance certifications, and transparency should be prioritized.

In conclusion, while cloud computing presents immense opportunities for businesses, a comprehensive understanding of its benefits, challenges, and security considerations is essential for successful adoption and ongoing information security posture improvement. The future of cloud computing is expected to see continued growth and innovation, necessitating continuous exploration and adaptation from businesses seeking to leverage its full potential.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Khan, N., Ahmad, N., Herawan, T. and Inayat, Z. (2019) Cloud Computing Security: A Review of Issues and Solutions. *Journal of Computer and System Sciences*, **83**, 1-12.

[2] Kaur, P. and Kaur, R. (2020) Cloud Computing Security: A Comprehensive Review. *International Journal of Computer Science and Engineering*, **8**, 123-132. https://doi.org/10.5120/ijca2015905574

[3] Kumar, V., Raheja, G.G. and Sodhi, J. (2013) Cloud Computing. *International Journal of Computers & Technology*, **4**, 5-7. https://doi.org/10.24297/ijct.v4i1a.3025

[4] Mell, P. and Grance, T. (2011) The NIST Definition of Cloud Computing. NIST Special Publication, 1-4. https://doi.org/10.6028/NIST.SP.800-145

[5] The Hacker News (2019) Alibaba's Taobao Suffers Data Breach Affecting 1.1 Billion Records. https://thehackernews.com/2019/12/alibaba-cloud-data-breach.html

[6] LinkedIn (2021) Protecting Our Members. https://engineering.linkedin.com/blog/2021/04/protecting-our-members

[7] Basan, M. (2023) 13 Cloud Security Best Practices & Tips. https://www.esecurityplanet.com/cloud/cloud-security-best-practices/

[8] Patel, A., Tiwari, R. and Khureshi, R. (2022) Comparative Study of Top Cloud Providers on Basis of Service Availability and Cost. *International Journal for Multidisciplinary Research*, **4**, 1-8. https://doi.org/10.36948/ijfmr.2022.v04i06.1140

[9] Rodrigues, J. (2023) All You Need to Know about the Cloud Computing Job Market. https://www.linkedin.com/pulse/all-you-need-know-cloud-computing-job-market-jorge-rodrigues

[10] Lomas, A. (2023) How to Choose a Cloud Services Provider? https://www.netsolutions.com/insights/how-to-choose-cloud-service-provider/