Original Research Article

Security Concerns and Solutions for Enterprise Cloud Computing Applications

Abstract:

Computing in the cloud is now one of the most interesting developments in technology owing to the fact that it is both flexible and cost-effective. Despite the enormous stakes, the implementation of cloud computing into an existing business model creates significant safety risks. Enterprises need to foresee and account for possible risks, threats, vulnerabilities, and mitigation strategies before using cloud computing. The concept of cloud computing may be simplified by dividing it into three separate models: "Infrastructure as a Service," "Software as a Service," and "Platform as a Service." It also talks about the current crop of cloud-based security tools. Before using this technology, we think businesses should assess their security risks, threats, and existing defences. We've also discussed the advantages and drawbacks of cloud computing as well as places where it might be used for information risk management.

Keywords: Enterprise cloud computing, security risks, SaaS, Implementation of Cloud Security

1. Introduction:

In this research, We will deep dive on Enterprise Cloud Security overview, Implementation techniques and methodologies and Security Vulnerabilities and solutions. Despite the advent of cloud computing, corporations have experienced and will continue to experience many system losses throughout the years. Considering recent reports of attacks on cloud computing services, this paper examines the pros and cons of using the cloud for information security management and provides recommendations for discussing issues such as cloud security, things to consider before using the cloud, a governance plan, and effective governance technologies [1].

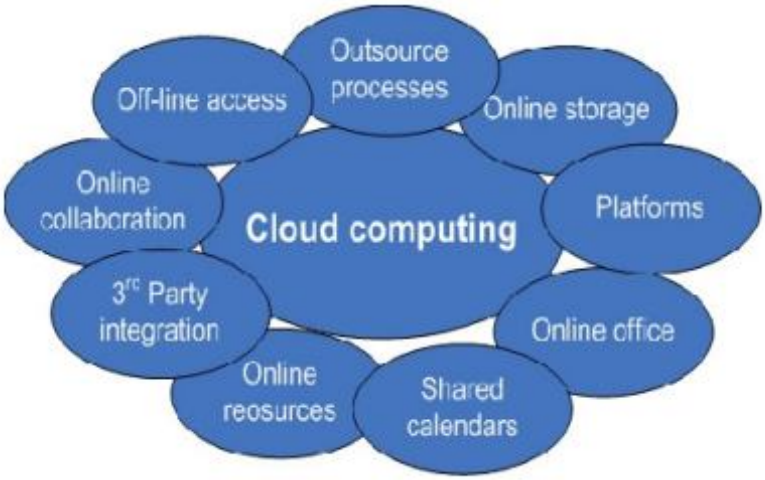

Figure 1: Cloud computing Resources

Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Storage-as-a-Service, and Infrastructure-as-a-Service (IaaS) are just a few of the many services that major cloud computing providers like Amazon, Google, Microsoft, Yahoo, and others are offering. Some of these services have already been discussed in this paper. There are a lot of academic studies, publications, and magazines about cloud computing security. Security concerns, potential threats, vulnerabilities, and potential countermeasures in business cloud computing are continually being researched and worked on by security experts and professionals.

2. Enterprise Cloud Security

Enterprise cloud security is the collection of tools, guidelines, and procedures that a company employs to safeguard its data and online assets. It encompasses a range of security measures, including network security, vulnerability management, identity and access management, and encryption. The purpose of business cloud security is to safeguard sensitive data from being stolen by hackers [2].

2.1 Cloud security can be broken down into three main areas:

Infrastructure security: This include protecting the network, storage, and server components that make up the cloud architecture. Network security, access control, encryption, and disaster recovery are all examples of infrastructure security measures.

Application security: This entails protecting the online, mobile, and API (Application Programming Interface) applications that are executing on the cloud infrastructure. Secure coding procedures, vulnerability scanning, and authentication and authorisation systems are all examples of application security methods.

Data security: This entails protecting the sensitive consumer data, financial information, and intellectual property that is stored and processed in the cloud. Data encryption, access control, and data loss prevention are all examples of data security procedures.

2.2 Importance of Enterprise cloud Security:

It is crucial to make sure your cloud environment is safe as businesses transfer their activities to the cloud. Cloud environments are vulnerable to these vulnerabilities as cyberattacks get increasingly sophisticated. In reality, enterprises now face additional security risks brought on by the move to the cloud, including data loss as a result of improperly configured cloud resources and unauthorized access to sensitive information [3].

Enterprise cloud security is critical for several reasons:

Protecting sensitive data: large volumes of confidential information, including customer, financial, and intellectual property data, are kept by businesses on the cloud. Financial loss, reputational damage, and legal liability are just some of the potential outcomes of a data breach.

Compliance requirements: Strict regulatory compliance standards for data privacy and security apply to many businesses. Heavy penalties and legal repercussions may follow failure to comply with these rules.

Cyber threats: Cyber dangers like ransomware, phishing, and malware may affect cloud infrastructure and data. Enterprise data may be protected from these attacks with the aid of a strong cloud security policy.

Business continuity: When the cloud is unavailable, it may have a big impact on the company's finances, output, and reputation. In the case of a cloud outage, business continuity may be guaranteed through a disaster recovery strategy and backup procedures.

3. Threats And Vulnerabilities

A threat is something that has a significant risk of adversely affecting a system or an organization. Vulnerabilities relate to any weak spots in an asset or system that might be exploited by an adversary. The use of cloud computing is susceptible to a variety of dangers and flaws, which are discovered after a comprehensive review of the relevant literature. They are broken down into further specifics down below:

Data Breaches:

A data breach happens when an unauthorized third-party gains access to, and then uses, personally identifiable information (PII) of an individual or organization. This may happen when the data is in the possession of an unauthorized party. A data breach is a hazard that carries a high level of risk and is considered as the most significant risk associated with cloud computing. At least 143 million customers of Equifax had their personal information compromised. In May of 2017, hackers broke into the database of OneLogin, a company that offers capabilities for identity management and single sign-on for cloud services. Data breaches may be caused by targeted assaults, simple human mistake, application vulnerabilities, or inadequate security procedures. All of these factors can contribute to the loss of sensitive information [25][26].

Data Loss:

Data corruption or inaccessibility may be caused by a variety of events, including simple human mistake, such as a cloud administrator unintentionally deleting files, a hard drive failure, a power outage, or malware infection, as well as natural catastrophes like floods and earthquakes. The most effective method for preventing the loss of data is to make copies of it and store them in several different places. This way, even if data is lost or damaged in one area, it may be restored from a duplicate stored in another site.

Malicious Insiders:

A malevolent insider has the potential for the greatest amount of damage and the highest level of danger. A former employee, the system administrator, a third-party contractor, a business partner, or even a business partner themselves may all pose a risk to a company as an insider threat. A danger from inside may have catastrophic effects. As an example, a recent leak of insider information at Sage led to a decrease of 4.3% in the company's stock price, which resulted in losses of many millions of dollars. Systems whose safety is wholly reliant on the protection offered by cloud service providers are at an unacceptable level of danger [4].

Denial of Service

A DoS (Denial of Service) attack may have a detrimental effect on a system's availability, as seen in Figure 2. In a denial of service (DoS) assault, there is only one source computer from which the attack originates, and this machine may be mitigated against. The goal of a denial-of-service attack (DoS) is to prohibit authorized users of a service from accessing the data or apps they need to do their jobs. Through the use of various forms of malware, the attacker in a distributed denial of service assault is able to take control of several target computers, often known as zombies or slaves.

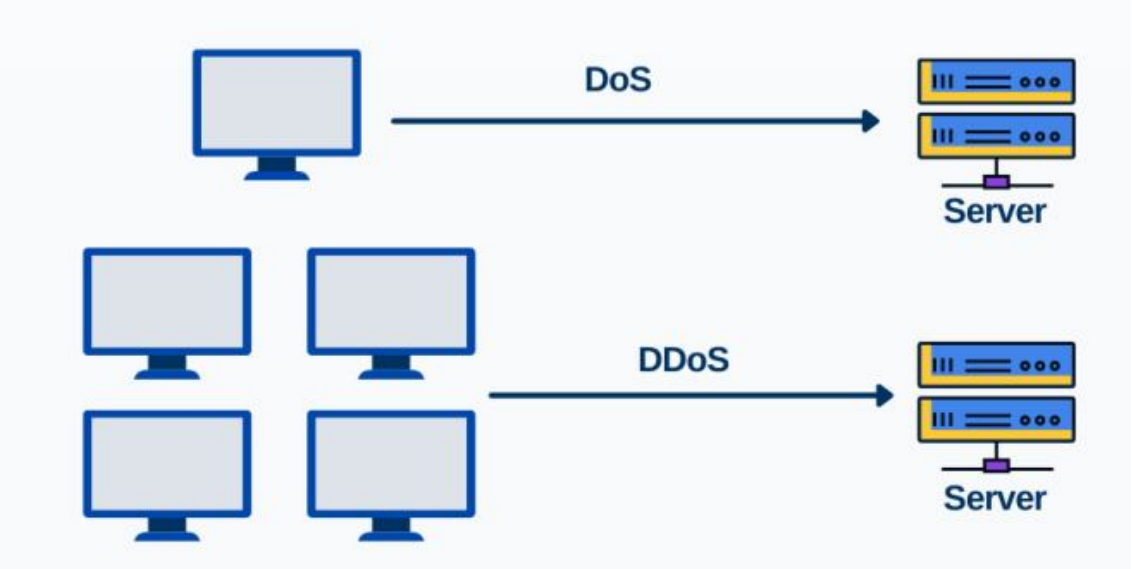

Figure 2. DoS and DDos [5]

The term "botnet" refers to this network of slaves collectively. By ordering botnet slaves to send fake traffic, an attacker may now knock down a cloud service. This activity makes legitimate users' data, applications, and other cloud services unavailable by being spoofed.

Vulnerable Systems and APIs:

Application Programming Interfaces (APIs) for the cloud are like a door that's always been left open for the public to enter your cloud application. Customers can connect with cloud services via the use of application programming interfaces (APIs), which are made available by cloud service providers (CSP). These application programming interfaces must be developed to withstand both inadvertent and intentional efforts.

Weak Authentication and Identity Management:

When businesses or organizations strive to provide the right permissions to every user's job function, they often run into problems with identity management. Because of the data breach at Anthem Inc., cybercriminals gained access to 80 million records including personal as well as medical information. The vulnerability in this system was that user credentials had been compromised.

Account Hijacking

The panorama of account or service hijacking now includes a new danger that is introduced by cloud services. The act of stealing the login credentials of a valid user to exploit those credentials for unethical reasons is known as "account hijacking." If an attacker gets their hands on certain stolen credentials, they could be able to undermine the availability, confidentiality, or integrity of the cloud services. Phishing and other fraudulent schemes are two of the most common ways that account

credentials may be stolen. Enterprises must put safeguards in place to prevent Credentials for user accounts are traded between end users and cloud services should allow multifactor authentication whenever it is feasible to do so.

Advanced Persistent Threats

A sort of cyberattack known as an Advanced Persistent Threat, or APT, is one in which the perpetrator infiltrates networks to worm their way into an organization's cloud-based systems and steal sensitive information. APTs pursue their targets covertly for long periods of time, often changing to the security mechanisms that are supposed to protect against them as they go. These kinds of assaults are very difficult to detect as the targets' defences continue to develop. APTs may get access to cloud services via a variety of methods, including spear phishing, direct hacking, attack code on USB devices, network penetration, and the use of insecure third-party APIs. The protection of cloud infrastructure from this danger requires the implementation of sophisticated security measures, regular infrastructure monitoring, and stringent process management.

4. Security Techniques for Threats Protection

In this part, we will go over the many security measures that may be implemented to prevent the exploitation of the dangers that were covered in the previous section. To protect cloud computing from potential dangers, we discuss the many levels at which these security approaches might be implemented [6].

A. Data Security

1) Protection from Data Breaches: To prevent a data breach in the cloud, several precautions and strategies for data protection have been recommended. One of them is to encrypt data before storing it on the network or on the cloud. This will need a key management technique that is both efficient and effective, as well as the security of the key in the cloud. To stop sensitive data from leaking out of virtual machines in the cloud, it is necessary to provide sufficient isolation between them. A risk assessment of the cloud environment may reveal where sensitive data is kept and how it is transported across different services and networks, and effective access controls can prevent unwanted access.

2) Protection from Data Loss: There are a variety of various security precautions that may be taken in order to stop the loss of data on the cloud. Maintaining a backup of all data on the cloud, where it can be accessible in the event that data is lost, is one of the most crucial precautions to take. However, in order to preserve the security qualities of the data, such as its integrity and confidentiality, the backup of the data must also be safeguarded. Various data loss prevention (DLP) strategies have been

developed in research and academic circles with the purpose of preventing the loss of data during the network's processing, storage, or both processes.

B. Network Security

1) Protection from Account or Service Hijacking: Taking use of the many different security mechanisms that are available on cloud networks is one way to prevent having your account or service compromised. The efficiency of the cloud, compatibility with other systems, and the context of virtualization need to be taken into account during the design process of intrusion detection and other network security systems. Combining methodologies for system-level virtualization with virtual machine monitoring led to the development of an IDS (Intrusion Detection System) for cloud environments. IDS keeps track of the VMs' workloads and monitors their state; the management system of IDS allows the virtual machines to be launched, terminated, and recovered at any moment [7].
2) Protection from Denial of Service: It is essential to determine and carry out all of the fundamental security needs of the cloud network, as well as those of the apps, databases, and other services, in order to prevent DOS assaults. After an application has been designed, it should undergo testing to ensure that it does not have any vulnerabilities that an adversary may use to gain an advantage. It is possible to thwart DDOS assaults by installing more network capacity, putting in place an intrusion detection system (IDS) that verifies network requests before they reach the cloud server, and storing a backup of IP pools for use in times of emergency. Various suppliers have also developed industrial countermeasures to stop Distributed Denial of Service attacks [8].

C. Cloud Environment Security

1) Protection from Insecure Interfaces and APIs: It is essential for the developers of these APIs to build them in accordance with the principles of trusted computing if they want to shield the cloud from the dangers posed by insecure APIs. In addition to this, cloud service providers are obligated to guarantee that all of the application programming interfaces (APIs) that are used in cloud environments are built with security in mind. Implementing robust authentication procedures and access restrictions is also required in order to protect data and services from being exposed via insecure interfaces and application programming interfaces (APIs). The Open Web Application Security Project (OWASP) offers standards and recommendations for the development of safe apps, which may assist users in avoiding application dangers like those described above. In addition, before transferring data to the cloud, users must evaluate the interfaces and APIs provided by the cloud provider [9].

2) Protection from Malicious Insiders: Only authorized individuals should be allowed access to the network's hardware and infrastructure to successfully secure the network from the risks described above. It is the responsibility of the service provider to establish stringent access control and division

of tasks at the management layer to limit administrator access to just the data and software that are within his or her purview. It is also important to conduct audits on the staff members in order to check for any questionable behaviour on their part. In addition, the standards for appropriate employee behaviour should be included into the legal contract, and disciplinary action should be taken against anybody who is engaged in illegal or unethical behaviour. Encryption may also be used in storage and public networks to protect data from being accessed by nefarious individuals who are authorized to access the data [10].

3) Protection from Abuse of Cloud Services:

The identification of dishonest customers may be facilitated using stringent initial registration and validation procedures. The user and the service provider need to come to an agreement on what is called a service level agreement (SLA), and this agreement must include the organization's rules for protecting its valuable assets. The user will obtain an understanding of the various legal measures that may be taken against him if he breaches the agreement because of reading this. The Service Level Agreement specification language, often known as SLAng, makes it possible to offer capabilities for monitoring, validating, and enforcing Service Level Agreements. In addition, the monitoring of the network should be thorough in order to identify malicious packets, and all of the most recent security updates should be put on the network's various security devices [11].

4) Protection from Insufficient Due Diligence: Before moving their operations and essential assets such as data to the cloud, businesses should make sure they have a comprehensive understanding of the nature and extent of the dangers connected with the cloud. In order for customers to take precautions for the safety of their applications and data, service providers are obligated to provide any relevant logs and infrastructure, such as firewalls. In addition, the cloud service provider is obligated to establish specifications for the implementation of industry-standard cloud applications and services. A risk assessment should also be carried out by the cloud provider on a regular basis, utilizing qualitative and quantitative methodologies to monitor the storage, flow, and processing of data at predetermined intervals [12].

5) Protection from Shared Technology Vulnerabilities: In cloud computing, the hypervisor is in charge of mediating communications between virtual machines and the hardware they are running on. As a result, the hypervisor has to be protected in order to guarantee that the other components of virtualization will operate correctly and to achieve isolation between VMs. In addition, a plan must be devised and put into action for each of the service models in order to protect against shared technology risks in the cloud. This strategy must include user security, infrastructure security, platform security, and software security. It is necessary to formulate and include baseline criteria for each component of the cloud while designing the architecture of the cloud. In addition to this, the

service provider has to keep a close eye on any vulnerabilities that may exist in the cloud environment and frequently provide fixes to address any problems that may arise.

5. Implementing cloud security:

There are some Variety Cloud Computing Models available to choose from:

There are three primary cloud computing models: Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS). IaaS is a model in which cloud service providers offer virtualized computing resources, including servers, storage, and networking. SaaS is a model in which cloud service providers deliver software applications to end-users over the internet. PaaS is a model in which cloud service providers offer a platform for developers to build, test, and deploy applications [22][23][24].

A multi-layered strategy that considers:

many elements of cloud security is necessary for implementing business cloud security. The following are some top recommendations for adopting business cloud security [13]:

Identity and Access Management (IAM): Security of the cloud depends on IAM. It gives businesses the ability to limit who has access to and what they can do with their cloud resources. To make sure that only authorized people have access to critical data and systems, organizations should establish robust authentication techniques, such as multi-factor authentication, and frequently evaluate access rights.

Encryption: Encryption is a method of encoding data to make it unreadable to anybody except the intended recipient. The use of encryption to safeguard data at both rest and in transit is a must for businesses today. Additionally, they must make sure that encryption keys are safely stored and handled.

Network Security: For cloud settings to be protected from online attacks, network security is essential. To safeguard their networks, businesses should put in place firewalls, intrusion detection and prevention systems, and other security measures.

Vulnerability Management: Identification, prioritization, and remediation of vulnerabilities in cloud settings are all part of vulnerability management. Organizations should routinely check the resources in the cloud for vulnerabilities and apply fixes and updates to fix them.

Security Monitoring: Monitoring cloud systems for suspicious behaviour and quickly reacting to security issues are both parts of security monitoring. To identify and address security risks, organizations should employ security monitoring tools and procedures [14].

6. Cloud Computation Implementation Guidelines:

♦ To fully understand the cloud, one must be aware of how its distinctively loose structure impacts the safety of data stored there. To do this, one must have an intimate familiarity with the data transmission and management processes inherent to cloud computing.

♦ Insist on complete openness from your cloud service provider by requiring that they disclose full documentation of their security setup and agree to periodic audits. An impartial organization or government agency should conduct the routine security inspection.

♦ When deciding what to store on the cloud, it's important to think about the legal implications.

♦ Keep an eye out for changes in cloud storage and computing processes that might compromise the safety of your data and react accordingly.

Concerns that Need to Be Addressed Prior to the Implementation of Cloud Computing

The global leader in IT research and consulting services, Gartner, Inc., has outlined seven security risks that businesses should discuss with cloud computing service providers before adopting the technology (Edwards, 2009) [27]:

♦ User Access. Inquire about the providers' employment and monitoring of privileged administrators, as well as the limitations placed on their access to sensitive data. Companies of a significant size should set and adhere to their own standards when employing employees to manage their cloud infrastructures.

♦ Regulatory Compliance. Insist that your service provider participate in third-party audits and get appropriate security certifications.

♦ Data location. Businesses should insist that their cloud service provider adhere to the data privacy laws of the countries where their data will be stored and processed.

♦ Data Segregation. Learn the steps used to keep your information secure and demand evidence that appropriate encryption measures are in place.

♦ Disaster Recovery. Inquire about the provider's track record of effectively supporting investigations like those conducted during the discovery phase of a lawsuit and get a written guarantee that they will do so in the future. You shouldn't just assume it can do that without proof.

♦ Long-term Viability. If a potential service provider fails or is bought, find out how you can get your data and if it will be in a format, you can simply transfer into a new service.

Cloud-based Security Tools

It's more crucial than ever to keep your network secure. Hackers don't care about the size of your network; they just want entry. Today, implementing security policies for your business is simpler than

ever thanks to current technologies like software-as-a-service and security-as-a-service. The best accessible security tools are listed below [15].

SilverSky is a security service that operates in the cloud. It helps your business conform to regulations like HIPPA and PCI, as well as provide services like email monitoring and protection and network security.

When data leaves the Vaultive network, it is encrypted using the Advanced Encryption Standard. You don't need any special equipment at your location to have it sitting between your network and the Internet. The firm provides protection for Office 365 and Exchange, two popular cloud-based services.

When used with services like Box or SharePoint, DocTrackr adds an extra degree of protection to your files. Once you've sent a document out of your system, you normally lose all authority over it. DocTrackr, on the other hand, allows you to reclaim authority by customizing access levels for each collaborator. It keeps tabs on who has seen your work and gives you the option to "unshare" it [16].

Proofpoint is an email security company that offers exclusively cloud-based services. It protects any incoming and outgoing data. While Proofpoint does say it stores your data, they say it's purely for backup purposes and that they don't have access to the encryption keys.

Centrify's main purpose is to manage user identities across a wide variety of platforms and software. It consolidates your staff and/or clientele into one easily managed and monitored location. Centrify can secure your network with either locally installed software or cloud-based services.

In addition to Qualys and White Hat Security, which concentrate on securing websites from the bottom up, including in the development process, there are additional security solutions available today, such as Okta, which is only concerned with identity management and therefore knows who has access to what and why.

Future considerations:

The suggestions and techniques listed below may also be utilized to access cloud computing in organizations. These suggestions and techniques were put out to help its departments and units in their approach to analyzing the wisdom and viability of using cloud services.

Risk/benefit analysis: Units interested in experimenting with novel cloud-based services or university services that may be offered using this technology should be aware of and prepared to deal with any potential drawbacks. Recognize that vendor security lapses may affect, if not the institution, then at least the university will be affected. Imagine the consequences of failing to meet the security and privacy objectives of maintaining the system's secrecy, availability, and control over the system's use. When evaluating the costs of internal vs external services, it is important to include in the time and

money required to manage the vendor relationship and incorporate the service into already internal services and processes [17].

Lower risk candidates: University services that involve public information, are not mission-critical to operations, and would otherwise Services that would, in other contexts, need a sizable in-house infrastructure or ongoing investment are prime candidates for delivery through cloud technology. These are perhaps the finest possibilities to maximize gain while lowering risk [18].

Higher risk candidates: Services provided by universities that are essential to the institution's operations, include distinctive or core competences such as Payroll and Student Information, or involve sensitive information or intellectual property are always higher risk candidates and need close examination [19].

Consider "internal cloud" alternatives: Some effort duplication is unavoidable given the university's dispersed structure. It is recommended that organizations consider implementing their own private cloud services as a cost-cutting measure. For instance, departments that run their own email servers and/or server infrastructure should seriously consider migrating to centralized services provided by the university. Until they can develop internal and hybrid cloud architecture, large enterprises should generally avoid storing sensitive data in public clouds [20].

Vendor agreement: Always aim to get some kind of service level agreement or contract with your service provider. It may be attainable to employ a cloud service for non-critical services that deal with public data if the vendor is prepared to offer adequate assurances, but a cloud vendor must not provide services that are essential to the university and/or deal with more sensitive data without an appropriate agreement in place. When creating such agreements,

Proportionality of safeguards: The physical, technological, and administrative security measures used by the vendor should be at least as good as those used internally for comparable services and data. Examine any gaps that were found [21].

Due diligence: Due diligence is necessary to determine the vendor's or service provider's reliability. Think about the vendor's credibility, transparency, references, financial stability, and availability of resources, as well as the results of any independent third-party audits of the vendor's safeguards and processes.

Exit strategy: It is not recommended to employ cloud services without first developing an exit strategy for cutting connections with the provider or service and including the service into business continuity and disaster recovery plans. In the case of a provider outage, you should give special thought to how you will retrieve your data.

7 . Conclusion:

A few important technologies that have developed and matured through time are combined in cloud computing. Cloud computing can save organizations money, but there are also significant security dangers. Despite the potential benefits of cloud computing for cutting expenses and increasing profits, businesses must weigh the potential security risks before making any decisions.

The central risk management capabilities offered by cloud computing are an advantage when it comes to protecting sensitive data. If a security vulnerability is discovered, the ability to effectively apply security updates and new patches provides business continuity. Weaknesses of cloud computing include worries about data security and privacy when using remote data centres, platform lock-in, reliability/performance issues, and the fear of making the wrong decision before the market matures. Before using the technology, businesses must verify and understand cloud security, conduct a full analysis of the associated security risks, and plan for ways to mitigate those risks. Successfully addressing security issues and concerns requires the establishment of pilot projects and the implementation of strong governance.

References:

1. Kazim, M., & Zhu, S. Y. (2015). A survey on top security threats in cloud computing. International Journal of Advanced Computer Science and Applications, 6(3), 109-113.
2. 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.
3. Parekh, M. D. H., & Sridaran, R. (2013). An analysis of security challenges in cloud computing. International Journal of Advanced Computer Science and Applications, 4(1).
4. Ertaul, L., Singhal, S., & Saldamli, G. (2010, July). Security Challenges in Cloud Computing. In Security and Management (pp. 36-42).
5. https://www.cobalt.io/blog/what-is-denial-of-service-attack
6. Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, 79, 88-115.
7. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of internet services and applications, 4, 1-13.
8. Suryateja, P. S. (2018). Threats and vulnerabilities of cloud computing: a review. International Journal of Computer Sciences and Engineering, 6(3), 297-302.
9. Alani, M. M. (2014). Securing the cloud: Threats, attacks and mitigation techniques. Journal of Advanced Computer Science & Technology, 3(2), 202.
10. Subramanian, N., & Jeyaraj, A. (2018). Recent security challenges in cloud computing. Computers & Electrical Engineering, 71, 28-42.

11. Lee, K. (2012). Security threats in cloud computing environments. International journal of security and its applications, 6(4), 25-32.
12. Malik, A., & Nazir, M. M. (2012). Security framework for cloud computing environment: A review. Journal of Emerging Trends in Computing and Information Sciences, 3(3), 390-394.
13. Chouhan, P., & Singh, R. (2016). Security attacks on cloud computing with possible solution. International Journal of Advanced Research in Computer Science and Software Engineering, 6(1).
14. Ashktorab, V., & Taghizadeh, S. R. (2012). Security threats and countermeasures in cloud computing. International Journal of Application or Innovation in Engineering & Management (IJAIEM), 1(2), 234-245.
15. Shahzad, F. (2014). State-of-the-art survey on cloud computing security challenges, approaches and solutions. Procedia Computer Science, 37, 357-362.
16. Piplode, R., & Singh, U. K. (2012). An overview and study of security issues & challenges in cloud computing. International Journal of Advanced Research in Computer Science and Software Engineering, ISSN, 2277.
17. Xiao, Z., & Xiao, Y. (2012). Security and privacy in cloud computing. IEEE communications surveys & tutorials, 15(2), 843-859.
18. Barron, C., Yu, H., & Zhan, J. (2013, July). Cloud computing security case studies and research. In Proceedings of the world congress on engineering (Vol. 2, No. 2, pp. 1-6).
19. Jain, P., & Jaiswal, A. (2012). Security Issues and their solution in cloud computing. International Journal of Computing & Business Research, 2229-6166.
20. Srinivasamurthy, S., & Liu, D. Q. (2010, November). Survey on cloud computing security. In Proc. Conf. on Cloud Computing, CloudCom (Vol. 10).
21. Gupta, S., & Kumar, P. (2013). Taxonomy of cloud security. Int. J. Comput. Sci. Eng. Appl, 3(5), 47-67.
22. Zhang, Q., Cheng, L., & Boutaba, R. (2022). Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications, 13(1), 1-28.
23. Li, B., Liu, J., Wu, J., & Li, C. (2021). Dynamic pricing for cost optimization in cloud computing: A survey. Journal of Systems Architecture, 112, 101981.
24. Kumar, S., Khatri, S. K., & Garg, S. (2019). Security and privacy issues in cloud computing: A systematic literature review. Future Generation Computer Systems, 94, 962-977.
25. Anderson, J. (2019). The anatomy of a data breach. Journal of Accountancy. https://www.journalofaccountancy.com/news/2019/jul/data-breach-anatomy.html
26. Ponemon Institute. (2021). 2021 Cost of a Data Breach Report. IBM Security. https://www.ibm.com/security/data-breach
27. Edwards, J. (2009). Gartner: Seven cloud-computing security risks. CIO. https://www.cio.com/article/2429864/gartner--seven-cloud-computing-security-risks.html