Data Security In Cloud Computing For Critical Applications*

POOJA M
Dept. of AI &ML
RNSIT
Bengaluru, Karnataka, India
pooja.m@rnsit.ac.in

KAVYASHREE H L
Dept. of AI &ML
RNSIT
Bengaluru, Karnataka,India
kavyashree.hl@rnsit.ac.i

PRATHAM M
Dept. of Computer Science.
Christ University
Bengaluru, Karnataka, India
pratham.m@mca.christuniversity.in

***Abstract*—Recently, a new paradigm known as "Cloud Computing" has emerged in which resources from computing infrastructures are offered as services over the Internet. However, this paradigm also poses a number of brand-new problems for access control and data security. If a company or organization outsources its data to the cloud, they are not within the same reliable space as their established infrastructures. This thesis contributes to overcome the data security challenges and issues due to using the cloud for critical applications. The next generation of IT enterprise design will be based on cloud computing.**

***Index Terms*—component, formatting, style, styling, insert**

I. Introduction

Cloud Computing : A model for ubiquitous, convenient, on-demand network access to a pool of configurable computing resources.Cloud computing refers to the utilization of computers, networks, storage, applications, and services. With minimal administrative effort or service provider engagement, it makes it possible for these resources to be swiftly provisioned and released.. The term "the cloud" describes the software and databases that run on servers that may be accessed via the Internet. Data all throughout the world house cloud servers. In simple words The on-demand delivery of computing capacity, databases, storage, applications, and other IT resources via the internet with pay- as-you-go pricing is known as cloud computing.

II. Cloud Computing Characteristics

• Measured services • Rapid elasticity • Massive scale • Re- source pooling • Easy maintainance • Geographic Distribution
• Low cost software • Advanced security

III. DATA SECURITY IN CLOUD COMPUTING

What is data security in Cloud Computing? When you adopt technology solutions, policies, and procedures to safeguard cloud-based systems, applications, and data user access that go with them, you are implementing cloud data security.

A. Why data security important in Cloud Computing?

Your data and applications are accessible to authorised users to cloud security. You'll always have a dependable way to access your cloud applications and data, enabling you to address any possible security issues right away.

Fig. 1. Data Security

B. How can we protect data security

- A few doable actions you can do right away to strengthen your data security
- Make a backup of your data
- Use secure passwords.
- When working remotely, use caution.
- Be aware of emails that seem off
- Install malware and antivirus protection.
- Never leave work documents or laptops unattended
- Ensure that your Wi-Fi is protected

C. CLOUD SECURITY

DATABASE SECURITY A set of practices and tools known as cloud security were created to handle both internal and external security threats to businesses. Cloud security is essential for organizations as they develop their digital transformation strategy and integrate cloud-based tools and services into their infrastructure. The security risks related to cloud computing can affect on both enterprises and individuals. Customers can utilize the public cloud, for instance, to store and back up files (using SaaS services like Dropbox), for office apps and services like email, or even to complete tax forms and accounts.

D. CLOUD SECURITY CHALLENGES

- Lack of visibility
- Multi tenancy
- Access management and shadow IT
- Compliance
- Mis Configurations

IV METHODOLOGY

A. What types of cloud security solutions are available?

- **Identity and Access Management(IAM)** Enterprises using Identity and Access Management (IAM) technologies and services to establish policy-driven enforcement techniques for each user trying to access both on-premises and cloud-based services to provide all users with digital identities, which is IAM's main purpose they might be actively monitored and regulated throughout all data exchange. as needed.
- **Prevention of Data Loss (DLP)** A collection of instruments and services known as data loss prevention (DLP) services guarantee the security of controlled cloud data. DLP systems protect all data stored, whether at rest or in motion, through a combination of remediation warnings, data encryption, and other preventative measures.
- **Security Information and Event Management(SIEM)** Security Information and Event Management (SIEM) is a comprehensive security orchestration system that automates threat monitoring, detection, and response in cloud-based environments. IT teams can effectively apply their network security standards with the help of SIEM technology, and They can respond to any issue swiftly possible threats. The SIEM solution correlates log data across many platforms and digital assets using AI-driven tech- nologies.
- **Continuity of Operations and Disaster Recovery** Regardless of security measures businesses have in place for their on-premise and cloud-based infrastructures, data breaches and disruptive disruptions are still possible. When newly discovered vulnerabilities or significant system failures occur, businesses must be prepared to respond as quickly as feasible. Disaster recovery solutions are a pillar of cloud security and provide companies with the tools, standards, and services necessary to quickly recover lost data and resume regular operations.

.

B. CLOUD DATA PROTECTION

The term "cloud data protection" refers to a group of data storage and security techniques used to safeguard data as it is stored, transferred, and accessed in a cloud environment. Regarding the information in data that is stored is referred to as "data at rest" and data that is in motion as "data in motion."

In contrast to data security, data protection relates to the copying of your data as opposed to its real security. A data protection programme is designed to guarantee that your private information is still intact in the event of loss or damage, whereas data security prevents data from being accessed or distributed by unauthorized parties in the first place. The technique of protecting a firm's data in a cloud environment, regardless of where it is situated, whether it is in motion or at rest, and whether it is handled internally by the company or externally by a third party, is known as cloud data protection. Perhaps

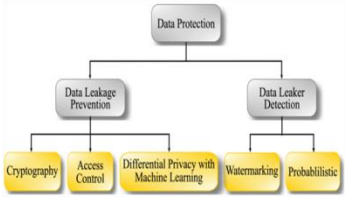

Fig. 2. Data Protection

the software we design for safeguarding data in the cloud will succeed , now that we have started, regard data security more as an exercise in risk mitigation and provide workable solutions with people.

C. CHALLENGES WITH DATA MIGRATION

After you decide to rollout a cloud service within the company you need to migrate some and login, profile de- tails, user data, and corporate data to the cloud. Cloud providers must be templates and procedures to conveniently migrate in house data to public clouds. However we must be aware of inherent challenges during and after migration
,are as follows: i. Liability Concerns: Cloud providers have a maximum data value for damage claims in a SLA. This value may be much lesser than the data value or the effort needed to fix data integrity problems.

ii. Compliance Concerns: The cloud service supplier needs tocomply with various regulatory and important requirements, such as the Federal Information Security Management Act(FISMA), the Hereby Insurance Portability and Accountability Act (HIPAA), and the International organization in Standardiza- tion(ISO), mandated by your business vertical for data protec- tion and proxcy.

iii. Connectivity Concerns: There can be several faults in WAN links between the consumer and the provider. It is supported by various connectivity providers and is outside the contract of the consumer or the provider.

D. CHALLENGES WITH DATA SECURITY

[Img] The following are data security challenges: **Security Risks**- Due to inherent it can easy access and multiple tenants within a cloud the data subjected to various security risks, which continues to be a serious concern. **Quality of Service**- The second concerns, after security is quality of service. Apprehensions about performance, long response time, and wan induced latency, inhibit many potential customers from readily accepting cloud service. The cloud provider must be able to ensure that response time and performance do not pose any impediment to cloud adoption. **Data Availability**- The third concern, after security and quality of service, is data availability. After a customer starts using cloud service and data, there are chances of unexpected downtime. There have been several outages at cloud providers despite their reduncy and replication.

Fig. 3. Cloud Security Challenges

Fig. 4. Other Security Challenges

SECURITY ISSUES IN CLOUD COMPUTING

Undoubtedly, cloud computing offers numerous benefits, there are certain security risks as well. These Security problems with Cloud Computing are listed below.

i. **Data Loss**: One of the problems with cloud computing is data loss. This is often referred to as a data leak. We are aware that someone else has access to our sensitive data and that our database is not entirely within our control.. Therefore, it is feasible that hackers will access our sensitive data or personal files if the security of a cloud service is breached.

ii. **Hackers' interference and Insecure APIs** –To the best of our knowledge, if we are discussing the cloud and its services, we are also discussing the Internet. Additionally, we are aware that using API is the simplest way to interface with the cloud. Therefore, it is crucial to protect the APIs and interfaces that external users use. However, there aren't many services accessible to the general public in cloud computing either .The vulnerability of cloud computing lies in the potential for third parties to get access to these services. Therefore, it's likely that hackers could simply harm or hack our data using these services.

iii. **User Account Hijacking-** The primary security risk with cloud computing is user account hijacking. if a hacker manages to take control of a user's or an organization's account. The hacker is then completely free to engage in Unauthorized Activities.

iv. **Changing Service Provider**-Another significant security concern with cloud computing is the inability to switch service providers or vendors. Changing vendors will present a variety of challenges for many enterprises. For instance, if a company wants to switch from Amazon Web Services (AWS) to Google Cloud Services, they will encounter a number of issues, such as need to transfer all of their data, along with concerns pertaining to the reality that the two cloud services utilise various different techniques and functions. Additionally, it's probable that AWS costs are different from those of Google Cloud and other services.

v. **Lack of Skill:** The primary issues faced by an IT company with unskilled employees include challenges with changing to a different service provider, needing an extra function, not knowing how to use a feature, etc. So, in order to work, one needs to be skilled.

vi. **Denial Of Service (DOS) Attack**- An excessive amount of traffic on the system can result in a denial of service (DOS) attack. Large companies like those in the banking industry, the government sector, etc. are the primary targets of DOS assaults. Data loss occurs during a DOS attack. Therefore, it costs a lot of money and takes a lot of time to handle data recovery.

THREATS TO CLOUD SECURITY

- **Misconfiguration**- Any flaws, holes, or faults in cloud configuration could put your environment at danger when you utilize the cloud. Security lapses, external hackers, ransom ware, malware, or insider threats that gain getting into your network through weaknesses are some examples of these cyber threats.
- **Unauthorized Access**- Once someone has gained illegal access to data or computer networks, they can harm a company in several distinct ways. They might blatantly take documents, data, or other data. They might use that access to further hack user accounts.
- **Insecure Interfaces/APIs**- Although APIs are increasingly useful for streamlining cloud computing procedures, they frequently raise security issues, especially if left unprotected. Insecure APIs can be used by adversaries to compromise or steal private and sensitive data.
- **Hijacking of Accounts**- In the cloud services, account or service hijacking continues to pose a severe security risk. When someone pilfers your private data and makes use of it to access your accounts, this is known as account hijacking (bank account, e-mail account or social media account).
- **Lack of Visibility**- The term "cloud visibility" describes the capacity to have a thorough understanding of all the activity within your cloud network. You now possess greater authority over your cloud infrastructure, allowing you to keep an eye on concerns with performance and cost-effectiveness while also monitoring cloud security.
- **External Sharing of Data**- Data sharing is made simple with the hlp of the cloud. Many clouds provide users the choice of sending an explicit email invitation to a collaborator or sending a link to a shared resource that anybody with the URL can access.

Fig. 5. Threats to Cloud Security

Fig. 6. Common Security Threats for Cloud Services

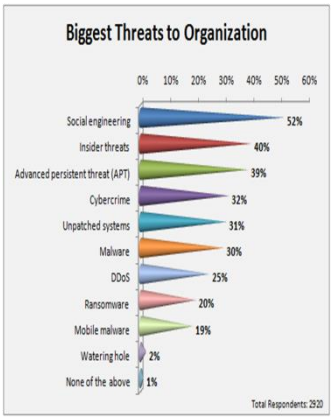

Fig. 7. Enter Caption

- **Malicious Insiders Threats**- Every company that works with them faces serious security risks. A malevolent insider already has authorized access to a network's sensitive resources and data within an organization. It is difficult for an unprepared business to identify a malicious insider because attempts to get this degree of access are what most attackers use to show themselves to their target. It is significantly more challenging to identify a malicious insider on the cloud. Many conventional security solutions are less effective with cloud deployments due to the lack of control businesses have the underlying infrastructure. This makes it much more challenging to identify malevolent insiders because cloud-based technology is frequently vulnerable to security flaws and is directly accessible from the public Internet.
- **Cyber attacks**- Because cybercrime is a business, the targets that the criminals choose are those who will be most profitable to them when they launch their attacks. Cloud-based infrastructure can be accessed directly from the public Internet, but it also frequently lacks adequate security and holds a lot of confidential and priceless data. A successful attack can likely be performed numerous times with a high probability of success because the cloud is utilised by numerous differ- ent companies. The cloud deployments of businesses are so frequently the target of hackers.
- **DOS Attacks**- Many firms' capacity to conduct business depends on the cloud. They run significant internal and customer-facing applications as well as keep business- critical data in the cloud. This indicates that a successful Denial of Service (DoS) attack against cloud infrastructure is probably going to have a significant effect on a variety of different companies. The cloud-based resources of a company are thus seriously threatened by DoS attacks where the attacker requests a ransom to end the attack.

FUTURE ENHANCEMENT

Post-Quantum Cryptography: In a world where quantum computers threaten existing encryption techniques, research and development towards post-quantum cryptographic algorithms will offer strong protection.

Automated Security Orchestration and Response (SOAR): As security incident detection and response become more automated, response times will get faster and the overall state of security will get better.

Data Privacy Regulations: As data privacy laws continue to evolve, better compliance controls, data protection, and secure cloud processing of personal data will be necessary.

Cloud-Native Security Services: Providers of cloud services will continue to advance their built-in security services and sup- plying more reliable, comprehensive data security solutions.

Security for containers: As containerization and microservices proliferate, security solutions will concentrate on safeguarding data inside containers and orchestrating settings.

User and Entity activity Analytics (UEBA): As UEBA systems advance, it will be easier to identify insider threats and unusual activity patterns in cloud environments.

DevSecOps (secure DevOps): Integrating security into the DevOps pipeline will need to guarantee that security is incorporated into cloud applications and infrastructure from the outset.

Continuous security monitoring: Threat hunting and real-time monitoring will become more proactive and predictive, assisting firms in staying ahead of new dangers.

Human-Centric Security: In recognition of the signifi-

cance of user awareness and training in preventing social engineering assaults, there will be a focus on human elements in security.

Sharing of global threat intelligence will enable more enterprises and security communities to work together more effectively in the fight against advanced threats.

CONCLUSION

In the fields of cloud computing and information security, data protection is a tough task. The thorough examination of the current answers, however, falls short. In this light a thorough examination of the most effective methods for functionality and pertinent solutions to transfer data securely for data protection in the cloud environment. For each discussed option the most pertinent and sufficient information is highlighted, along with any knowledge gaps and potential future study avenues. The refereed procedures are also subjected to a thorough analysis and comparison. Each technique's applicability is evaluated in light of the surrounding circumstances. According to the research, no single technique is capable of guaranteeing the data's complete security from all parties involved in the system, whether they are directly or indirectly. Integrating the methods for giving the system total security in the sharing environment will enable the development of a solid solution. Furthermore, it is anticipated that the disclosed analysis will act as a turning point for future academics in the field and other developing applications that need to exchange and store data securely in order to protect it. This is due to the set of highlights of the addressed remarkable solutions.

REFERENCES

[1].Bhardwaj, A., & Goundar, S. (2019). A framework to define the relationship between cyber security and cloud performance. Computer Fraud & Security, 2019(2), 12-19.

[2] Blau, I., & Caspi, A. (2009). What type of collaboration helps? Psychological ownership, perceived learning and outcome quality of collaboration using Google Docs. Paper presented at the Proceedings of the Chais conference on instructional technologies research.

[3] Bora, U. J., & Ahmed, M. (2013). E-learning using cloud computing. International Journal of Science and Modern Engineering, 1(2), 9-12.

[4] Clark, R. C., & Mayer, R. E. (2016). E-learning and the science of instruction: Proven guidelines for consumers and designers of multimedia learning: john Wiley & sons.