IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 7, July 2023

DOI: 10.17148/IJARCCE.2023.12730

Survey paper on security issue in cloud computing

Trupti Kavadimatti[1], Soumya Udoshi[2], Vijayalaxmi Patil[3]

Student, Master of Computer Application, KLS Gogte Institute of Technology, Belgavi, India[1,2]

Assistant Professor, Master of Computer Application, KLS Gogte Institute of Technology, Belgavi, India[3]

Abstract: Organizations can now access computing resources, software, and services through the internet on a pay- as-you-go basis thanks to the revolutionary technology known as cloud computing. Even though cloud computing has many benefits, such as cost savings, scalability, and flexibility, it also presents particular security challenges. In- depth analysis and exploration of the vulnerabilities that arise due to the virtualized nature of cloud environments, data breaches, insider threats, and regulatory compliance concerns are provided in this technical seminar report, which delves into the various security issues faced by cloud computing providers and users. The study also covers a number of best practices and mitigation measures to guarantee a secure and reliable cloud computing environment.

Keywords: Security issue, Cloud security, Cloud Architecture, Challenges, Automation of IT industry.

I. INTRODUCTION

Similar to utility-based systems like electricity, water, and sewage, cloud computing offers a centralized pool of reconfiguration computing resources and computing outsourcing methods that enable various computing services to various persons. Using middleware, cloud computing isolated the application from the operating system and hardware. As a result, with cloud computing, the application services continue even if the hardware or operating system fail.

There is no denying that a company can benefit greatly from cloud computing. Cloud computing has some fundamental components, including virtualization, on-demand services, quick adaptability, wide-ranging network access, resource groups, and measurable service.

Clouds provide several advantages for both consumers and businesses. Clouds provide resource pooling,outsourcing techniques, cost savings, accessibility from anywhere at any time.

Fig 1. Overview of cloud computing

The term cloud computing was first influenced by Google's CEO Eric Schmidt in late 2006. From this we can understand that cloud is a new phenomenon formed by amalgamating the old ideas and concepts. Cloud is generally built on grid based architecture using the grid services and other technologies like virtualization and models. The main enabling technology of cloud computing is virtualization which separates physical computing devices into two or more virtual devices, so that it can easily manage the computing tasks. Cloud services are provided as major utility services like water, telephone, electricity using pay-as-you-use model. These services are generally described as XaaS where X can be

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 7, July 2023
DOI: 10.17148/IJARCCE.2023.12730

anything like a Software or Infrastructure or platform etc. According to the past researches and results, in 2009 , the availability of high-capacity networks, low-cost computers and devices as well as the widespread adoption of hardware Virtualization, Service-Oriented Architecture, Automatic and Utility computing led to a growth in Cloud Computing. In the year 2013 , it was observed that Cloud Computing had become a highly obtained service due to the advantages like High Computing Power, low service costs, scalability, high performance and accessibility.

Background of cloud computing

The way that organizations and people access and use computing resources has been changed by cloud computing. It makes it possible to offer computing power, storage, and applications without the requirement for substantial infrastructure investments up front. The study gives a highlevel overview of the fundamental ideas and traits of cloud computing, including on-demand self-service, resource pooling, quick elasticity, and wide network access

II. ARCHITECTURE

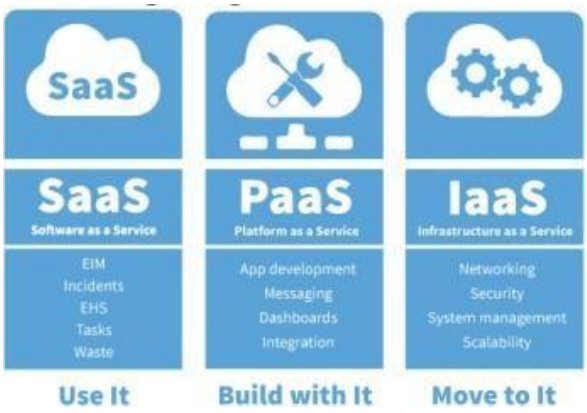

Fig 2. Cloud Service models

Cloud deployment model

In-depth explanations of the various cloud deployment models, such as public, private, hybrid, and community clouds, are provided, along with information on any security concerns. Private clouds are reserved for a single organization, but public clouds are open to everyone.

Community clouds cater to a particular group of users, while hybrid clouds contain characteristics of both public and private clouds

Cloud Service models:

Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) are the three different cloud service models that are described in the paper. The security duties of each service model are highlighted, highlighting the shared accountability structure between cloud service providers and clients. In an IaaS model, the cloud provider administers the basic infrastructure, but users are in charge of protecting the virtual machines and applications they deploy. The supplier assumes increased security responsibility in PaaS and SaaS models, but users are still responsible for protecting their apps and data.

1. Software as a service (S-a-a-S):

S-a-a-S is also known as Cloud application Services which utilizes the web to deliver applications that are managed by thirdparty seller and whose interface is accessed on the customer side. Most S-a-a-S applications can be run directly from a web browser without any downloads or installation process, some require plugins. It is simple for S-a-a-S to keep up and bolster the endeavors since vendors deal with the works like applications, run time, data, middleware, OSes, virtualization, servers, storage and networking. The S-a-a-S has four common approaches:

1. Single instance
2. Flex tenancy

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 7, July 2023

DOI: 10.17148/IJARCCE.2023.12730

3. Multi instance
4. Multitenant

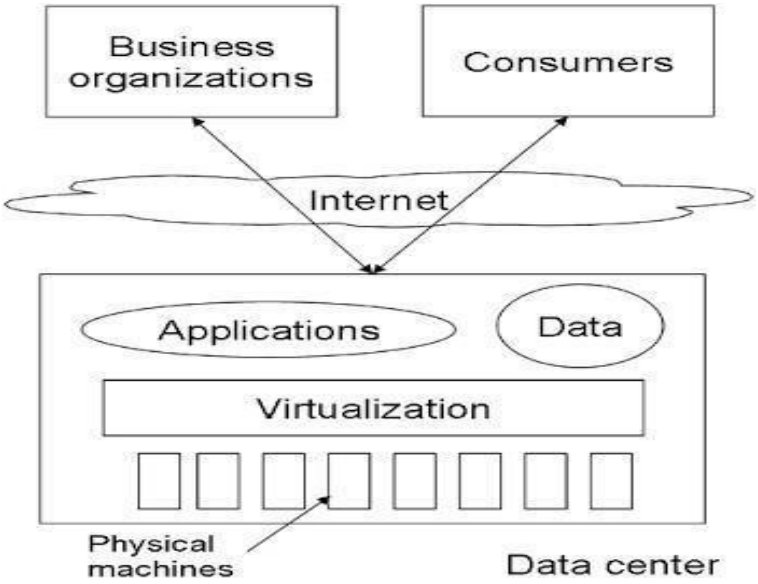

Fig 3: Basic cloud computing Architecture.

Examples: Google Apps, Go-To Meeting, concur, Sales forceworkday, Citrix, WebEx, Cisco.

2. Infrastructure as a service (I-a-a-S):

I-a-a-S, otherwise known as Cloud Infrastructure Services are models which perform tasks by themselves for accessing and monitoring which helps in incorporating the compute, storage, networking and networking services. Many I-a-a-S providers now offer databases, messaging queues, and other services above the virtualization layers. When compared to Sa-a-S and P-a-a-S, I-a-a-S clients are responsible for managing applications, data, runtime, middleware, and OSes.

Examples: Computer Compute Engine (GCE), Amazon webservices (AWS), Cisco Meta-pod Microsoft Azure, Joynet.

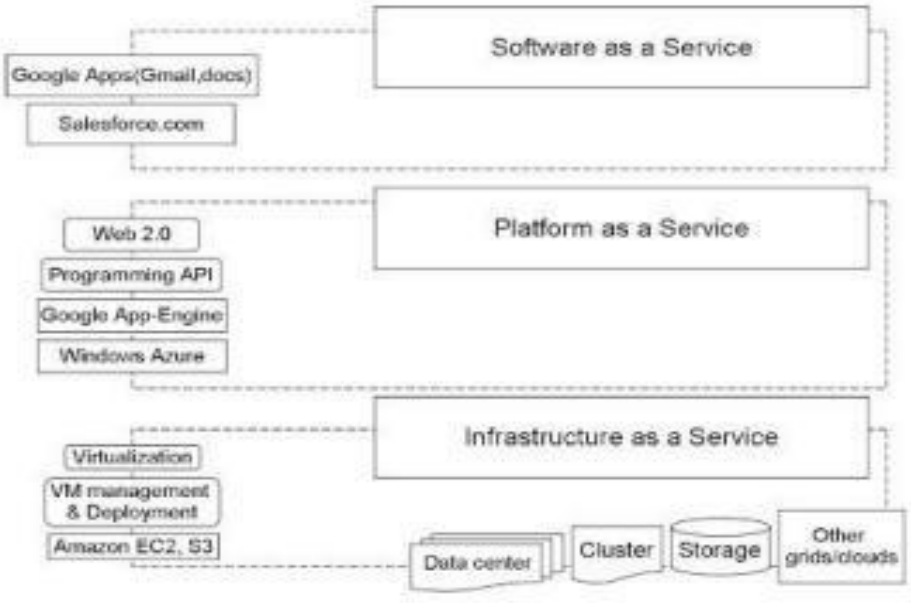

Fig 3: Services provided by Cloud Computing.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 7, July 2023

DOI: 10.17148/IJARCCE.2023.12730

3. Platform as a service (P-a-a-S):

Cloud platform services, or P-a-a-S are generally used for application and other developments while providing cloud components to software. It makes the development, deployment of applications quick, testing, simple, and cost- effective. With P-a-a-S, enterprise operations, or third-party provider, can manage many services like servers, O.Ses, virtualization, storage and networking.
Examples: Apprenda

III. SECURITY CHALLENGES IN CLOUD COMPUTING

Security challenges in cloud computing refer to the various risks and vulnerabilities that can arise when organizations utilize cloud services to store, process, and manage their data and applications. These challenges stem from the unique characteristics and shared infrastructure of cloud environments, which create opportunities for potential security breaches and unauthorized access. Some of the key security challenges in cloud computing include:

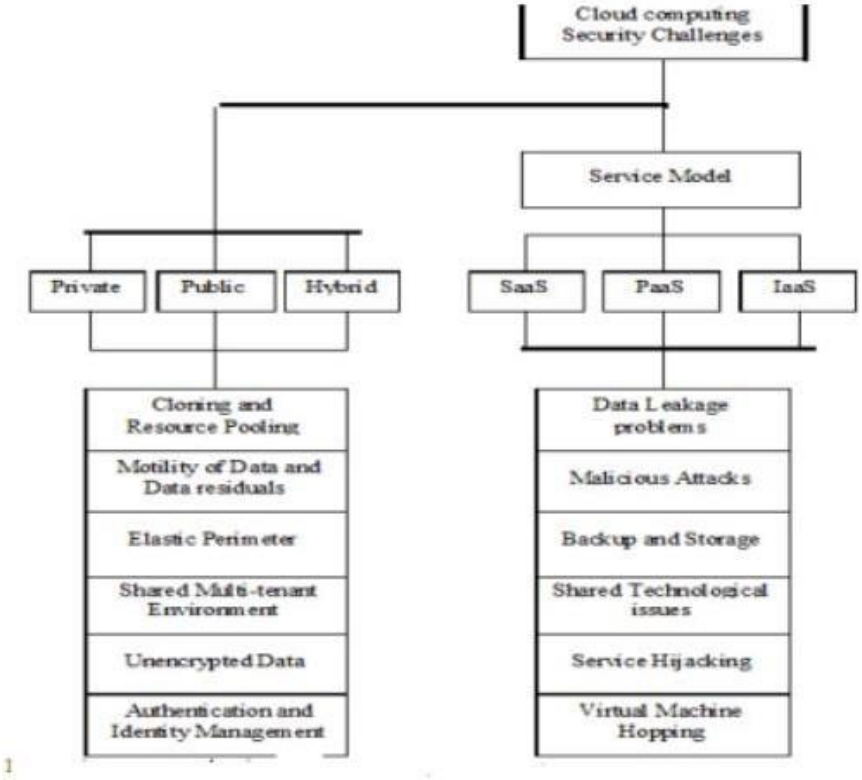

Fig 4. Cloud computing security challenges

1. Data breaches: Because cloud systems contain such large amounts of sensitive data from numerous clients, fraudsters find them to be appealing targets. Unauthorized access to sensitive information due to a data breach can result in financial losses and reputational harm for an organization.

2. Data loss: Despite the fact that cloud service providers use strong redundancy and backup systems, data loss can stillhappen for a variety of reasons, including hardware malfunctions, natural disasters, or even human mistake.

3. Threats from insiders: Individuals having insider access to cloud resources, such as staff members or contractors, can represent serious security hazards. Data breaches, data tampering, or other harmful behaviors may come from purposeful or unintentional misuse of privileges.

4. APIs and interfaces that aren't secure: Application Programming Interfaces (APIs) are provided by cloud service providers to make it easier for consumers to engage with their services. Attackers may use any flaws in these APIs to obtain unauthorized access to cloud resources.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 7, July 2023
DOI: 10.17148/IJARCCE.2023.12730

5. **Adequate identity and access management (IAM):** It is necessary to prevent unauthorized access to resources and sensitive data. In cloud environments, it's crucial to manage user access, authentication, and authorization properly.

6. **Vulnerabilities in shared technology:** Since cloud providers serve a number of clients on the same infrastructure, a flaw in an application or virtual machine owned by one client may have an impact on other clients using the same resources.

7. **With compliance and regulation:** Businesses using cloud services are subject to a number of data protection laws and standards. Due to the scattered nature of data and apps, ensuring compliance in a cloud environment can be difficult.

8. **Lack of transparency and control:** Cloud users frequently have limited access to and control over the provider's security protocols and underlying infrastructure, which raises questions about data governance and compliance.

9. **Security of cloud service providers:** Prior to entrusting them with sensitive data, organizations must thoroughly assess their security procedures. Different suppliers offer varying degrees of security precautions and certifications.

10. **Denial of Service (DoS) attacks:** Attackers can overwhelm a system's resources to prevent it from being used by authorized users. DoS attacks can affect cloud services.

11. **Data protection:**Cloud providers must protect data from malicious insiders. This can be difficult, as insiders have legitimate access to data.

12. **Account or service traffic hijacking:**This type of attack can steal users' personal data, such as bank credentials.

13. **Spoofing:**Spoofing is a type of attack in which an attacker pretends to be someone else. This can be done by falsifying data, such as an IP address or email address. Spoofing can be used to gain unauthorized access to systems or data.

14. **Inappropriate system use:** This is the use of cloud resources for unauthorized or malicious purposes. Inappropriate system use can include the unauthorized access of data, the use of cloud resources tolaunch attacks, or the misuse of cloud resources for personal gain.

15. **Network intrusion:** This is the unauthorized access to a computer network. Network intrusions can be used to steal data, install malware,or disrupt network operations.

16. **Fragmentation attacks:**These are attacks that target the fragmentation of data in the cloud. Fragmentation attacks can be used to disrupt the availability of data or to make it more difficult to recover data from a cloud outage.

17. **Cloud access control issues:**These are issues that can arise with the management of cloud access control. Cloud access control issues can allow unauthorized users to access cloud resources or can make it difficult to track who has access to cloud resources.

18. **Database integrity issues:**These are issues that can arise with the integrity of data inthe cloud. Database integrity issues can allow unauthorized users to modify or delete data in the cloud or can make it difficult to ensure the accuracy of data in the cloud.

19. **Back-door:**This is a hidden way to access a computer system or network. Back-doors can be used to gain unauthorized access to a system or network or to bypass security controls

IV. SECURITY MEASURES AND BEST PRACTICS 1.Data Security and Encryption

A crucial security measure for securing data in the cloud is encryption. In-depth discussion of data-at-rest and data-in-transit encryption is included in the paper, which guarantees that data is kept private even when it is stored on cloud servers or sent over the internet. For encryption keys toremain private, key management procedures such safe key generation, storage, and rotation are essential.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 7, July 2023
DOI: 10.17148/IJARCCE.2023.12730

2. Access Regulation and Identity Control

For cloud security to be effective, access control and identity management are essential. The significance of role- based access control (RBAC), which gives permissions based on job roles and responsibilities, is discussed in the report. RBAC prevents unauthorized access to sensitive information and resources. In order to prevent unwanted access, multi- factor authentication (MFA), which requires users to give multiple forms of authentication, adds another layer of security.Single Sign-on (SSO) simplifies user authentication and lowers the chance of security problems involving passwords.

3. Network Monitoring and Security

The research examines the use of firewalls, intrusion detection/prevention systems (IDS/IPS), network segmentation, and traffic analysis approaches to protect cloudenvironments from network-based threats. By filtering incoming and outgoing traffic, firewalls serve as a barrier between the cloud environment and external networks. IDS/IPS can automatically stop possible threats by watching network activity for suspicious behavior. By dividing the cloud environment into separate segments, network segmentation lowers the attack surface. Potential security incidents and breaches are identified with the aid of traffic analysis and anomaly detection.

4. Disaster Recovery and Data Backup

For data availability and business continuity, disaster recovery planning and backups are crucial. In order to prevent data loss in the event of hardware failures or data corruption, the paper outlines routine backups, in which data is periodically copied and stored in a different location. Planning for redundancy entails providing backup systems or resources to guarantee continuity of service even if a component fails. The procedures to be followed in the event of a security breach or unanticipated outage are outlined in incident response planning.

5. Managing Third-Party Risk

For a variety of services, cloud service providers frequentlyuse outside vendors. In order to properly manage third- party risks, the paper looks at the significance of vendor security evaluations, contractual duties, and Service-Level Agreements (SLAs). Potential vendors should be carefully screened by organizations, who should also evaluate their security procedures and check that the vendor's security measures comply with their own security needs.

6. Compliance with regulations and auditing

In cloud computing, compliance with regulatory regulations is crucial. The report examines data complianceaudits, compliance tools, and the value of routine security evaluations. Employing tools and services that support monitoring and enforcing compliance with pertinent legislation is a good idea for organizations. Periodic compliance audits assist discover areas for improvement while ensuring that the cloud environment complies with the necessary requirements.

V. CASE STUDIES

Case Study 1: Target Data Breach (2013)

Target, one of the biggest retail companies in the US, had a significant data breach in December 2013 that affected millions of customers. Through a vendor with access to Target's systems, attackers were able to penetrate the company's network. Later, the attackers made lateral moves inside Target's network, eventually infiltrating a computer that was in charge of controlling HVAC systems. Theythen gained credentials and made their way to the point-of- sale (POS) systems, which housed the customer data.

About 40 million credit and debit card records, containing personal data such names, card numbers, expiration dates, and CVV codes, were exposed as a result of the incident. Inaddition, almost 70 million consumers' personal data, including names, addresses, phone numbers, and email addresses,

Security Concerns
Inadequate Network Segmentation: Once an attacker got access to a system, they were able to travel between multiple systems since the target’s network was not properly segmented.

Insufficient third-party vendor security: The attackers penetrated Target's systems by taking advantage of a weakness in one of the third-party vendor's networks.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 7, July 2023
DOI: 10.17148/IJARCCE.2023.12730

Weak Access Controls: Because of lax access control policies, the attackers were able to get greater access and gain entry to important systems.

Lessons Learned: To prevent lateral movement within the network, this example emphasizes the significance of adequate network segmentation, thorough vendor security assessments, the requirement for ongoing monitoring, and access control management.

Case Study 2 :Drop box Data Breach(2012)

In 2012, a security flaw in the well-known cloud storage provider Dropbox exposed the login information for roughly68 million user accounts. A Drop box employee reused the same password on other accounts, which led to the breach. Attackers were able to access a project document containinguser email addresses and hashed passwords without authorization by taking advantage of this password's vulnerability.

Security Concerns
Weak Password Management: When one of those accounts is compromised, using weak passwords or reusing passwords by staff might have disastrous results.

Inadequate Hashing and Salting: Dropbox did not salt the hashed passwords it kept, making it simpler for hackers to decipher the hashes and access the plain-text passwords.

Lessons Learned: This instance highlights the significance ofstrong password management procedures, particularly the usage of distinct passwords for each account and the adoption of reliable password hashing methods such salted hashes.

Case Study 3: AWS S3 Bucket Misconfiguration (2017)

Misconfigured Amazon Web Services (AWS) S3 buckets were to blame for a sizable number of data breaches in 2017 that exposed sensitive information from numerous organizations. Many businesses unintentionally made their S3 buckets public, allowing anyone to see, download, and alter the data contained inside.

Security Concerns
Misconfigured Access Controls: Businesses neglected to properly establish the access controls on their S3 buckets, leaving them accessible to the general public.

Lack of Monitoring and Audit: To quickly identify and address misconfigurations, many businesses lacked adequate monitoring and audit procedures.

These case studies show that a variety of reasons, such as lax access controls, incorrect settings, and human mistake, can contribute to security vulnerabilities in cloud computing. To reduce such dangers and guarantee the security of cloud-based systems and data, strong security measures, ongoing monitoring, and best practices must be implemented.

VI. FUTURE TRENDS AND SOLUTIONS

The seminar report also discusses upcoming development sand trends in cloud security, such as securityautomation, the application of blockchain technology, encryption, and zero-trust architecture, as well as the integration of AI and ML in security. These cutting- edge ideas and technology have the potential to improvecloud security while addressing the changing threat environment. Certainly! Let's learn more about the upcoming developments and approaches in cloud security.

1. Security Automation and AI/ML

The complexity and dynamic nature of cloud systems may make it difficult for traditional security measures to keep up with the tempo and scope of threats. Cloud security is being improved through security automation, which is becoming more and more effective when combined with AIand ML technologies.

Automated Threat Detection and Response: AI and MLalgorithms are capable of analyzing enormous volumes of data and seeing patterns that point to security concerns. Automated systems can respond to security problems quickly and identify anomalies in real-time, reducing the severity of possible breaches.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 7, July 2023
DOI: 10.17148/IJARCCE.2023.12730

AI-powered behavioral analysis can establish user baseline habits and spot deviations that can indicate shady activity.Insider risks and zero-day assaults are easier to spot because to this proactive strategy.

Using past data and trends, AI/ML can identify potential security vulnerabilities, allowing businesses to take preventative measures to safeguard their cloud resources.

2. Homomorphic Encryption and Secure Computation

A cryptographic method called homomorphic encryption enables computations to be conducted directly on encrypted material without the need to first decode it. With this method, even when processing is contracted out to cloud service providers, sensitive data is kept encrypted. Secure computing methods, such secure multi-party computation, let several people collaborate on a computation without disclosing the details of their individual contributions. Computing that protects privacy and secrecy is made possible by homomorphic encryption and secure computation techniques, which allow businesses to process and analyze encrypted data Cloud service providers can run calculations on client data using homomorphic encryption without having access to the unencrypted data, allaying concerns about data privacy in the cloud.

3. Blockchain in Cloud Security:

Cloud security is benefiting from the decentralized, tamper- resistant characteristics of blockchain technology.

Blockchain-based identity and access management (IAM) systems can offer a safe and decentralized way to manage user identities and access privileges across various cloud services. Blockchain's distributed ledger capabilities provide an immutable record of all transactions and modifications made to cloud resources, assisting forensic investigationsand compliance audits.

Secure Data Sharing: Blockchain enables transparent and secure data sharing between numerous parties, preserving data integrity

4. Zero-Trust Architecture

A security model known as zero-trust architecture bases its assumptions on the idea that no entity, internal or external, can be trusted by default. All users, devices, and programs attempting to access cloud resources must strictly be verifiedand authorized. Micro-Segmentation: To prevent possible attackers from moving laterally, Zero-Trust Architecture encourages the division of network resources into smaller, isolated segments.

Continuous Authentication: To lower the risk ofunwanted access, users and devices are continually authenticated throughout their interactions with cloud services. Zero-Trust Architecture upholds the principle of least privilege by simply allowing users the minimal amount of access necessary to complete their activities

VII. CONCLUSION

Cloud computing's security challenges are always changingas well. To maintain a stable and safe cloud computing environment, it will be essential to adopt future trends and solutions in cloud security, such as security automation using AI/ML, homomorphic encryption, blockchain applications, and the deployment of Zero-TrustArchitecture. To keep ahead of new dangers in the constantly evolving cloud environment, organizations must maintain vigilance, update their security procedures, and use cutting-edge technologies. The seminar report highlights that even while cloud computing has many advantages, its security issues should not be disregarded. To guarantee the privacy, integrity, and accessibility of their data and cloud services, organizations need to be aware of these issues and take appropriate action. Cloud users can build trust and confidence in their cloud deployments while realizing the advantages of this game- changing technology by putting the necessary security measures and best practices in place. In the future, keeping a secure and reliable cloud computing environment will also require being up to date on new security trends and solution

REFERENCES

[1] Sajid Habib Gill, Mirza Abdur Razzaq , Muneer Ahmad, Fahad M. Almansour , Ikram Ul Haq , NZ Jhanjhi, Malik Zaib Alam, Mehedi Masud (2021).”Security and Privacy Aspects of Cloud Computing: A Smart Campus Case Study”.Intelligent Automation & Soft Computing DOI:10.32604/iasc.2022.016597

[2] Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy(2011).”Cloud Computing: Security Issues and Research Challenges”. IRACST - International Journal of Computer Science and Information Technology &

DOI: 10.17148/IJARCCE.2023.12730

Security(IJCSITS) Vol. 1, No. 2, December 2011

[3].Garima Gupta1, P.R.Laxmi, Shubhanjali Sharma(2011).”ASurvey on Cloud Security Issues and Techniques”.Department of Computer Engineering,Government Engineering College, Ajmer

[4].Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina, Eduardo B Fernandez(2013).”An analysis of security issues for cloud computing”.Hashizume et al. Journal of Internet Services and Applications 2013

[5].KALLU VENKATA DINESH,Dr N GOPALA KRISHNA.”CLOUD COMPUTING AND ITS VARIABLE TECHNIQUES IN OBTAINING DATA SECURITY PARAMETER”.Vol 13, Issue 01, Jan /2022 ISSN NO:0377-9254

[6].Jaydip Kumar.Cloud Computing Security Issues and ItsChallenges: A Comprehensive Research.International Journal of Recent Technology and Engineering (IJRTE)ISSN: 2277-3878, Volume-8, Issue-1S4, June 2019

[7].Dhanamma SHANKAR Jagli. “Cloud Computing andSecurity Issues”. Article in International Journal of Engineering Research and Applications,June 2017

[8].Ambati Hemalatha,N. Vijaya Gopal. “LIGHT WEIGHTDATA SHARING SCHEME FOR CLOUD COMPUTING”.Vol 13, Issue 01, Jan /2022 ISSN NO:0377-9254.JOURNAL OF ENGENEERING SCIENCE.

[9].Vaikunth Pai T, P. S. Aithal.”Cloud Computing Security Issues - Challenges and Opportunities”. International Journalof Management, Technology and Social Sciences (IJMTS), ISSN: 2581-6012, Vol. 1, No. 1, 2016.

[10].Sura Khalil Abd, Rawia Tahrir Salih, S.A.R AlHaddad, Fazirulhisyam Hashi, Azizol B HJ Abdullah, Salman Yussof.”Cloud Computing Security Risks with Authorization Access for Secure Multi-Tenancy Based onAAAS Protocol”.

[11]. KENNEDY A. TORKURA , MUHAMMAD I. H.SUKMANA , FENG CHENG, AND CHRISTOPH MEINEL.”CloudStrike: Chaos Engineering for Security and Resiliency in Cloud Infrastructure”.July 17, 2020.IEEEAccess.

[12].IANG LI , QIXU WANG , XIAO LAN , XINGSHUCHEN , NING ZHANG , (Member, IEEE), DAJIANGCHEN. “Enhancing Cloud-Based IoT Security Through Trustworthy Cloud Service: An Integration of Security andReputation Approach”(2019).IEEE Access.

[13].Mr. Gopala Krishna Sriram.”RESOLVING SECURITY AND DATA CONCERNS IN CLOUD COMPUTING BYUTILIZING A DECENTRALIZED CLOUD COMPUTING OPTION”(2022).International Research Journal of Modernization in Engineering Technology andScience

[14].AANSHI BHARDWAJ, VEENU MANGAT , (Member,IEEE), AND RENU VIG. “Hyperband Tuned Deep Neural Network With Well Posed Stacked Sparse AutoEncoder for Detection of DDoS Attacks in Cloud”(2020).IEEE Access.

[15].Prof.S.S Dhule , Durga Nehare , Komal Ballewar , PunamBangade , Riddhi Raut , Mamta Sidam , Punam Pawar. “Implementation of Cryptographic Algorithm for Cloud Data Security”.International Journal of Aquatic Science ISSN: 2008-8019 Vol 12, Issue 02, 2021.

[16].”RESEARCH PAPER ON SECURITY ISSUES IN CLOUD COMPUTING”(2021). International journal of creative research thought(IJCRT).

[17].Harish Chandan Sharma,Pradeep Semwal .”REVIEW OFCLOUD COMPUTING DATA SECURITY AND THREATS” (January 2022).Research Gate.

[18].Tushar Budhwani, Durga Bhagwan Boli. “An Analysis ofCloud Security”(Feb 2022). Research Gate.

[19].EESHAN SIDDIQUI , OMAR TAYAN, MUHAMMAD KHURRAM KHAN. “Security Analysis of Smartphone and Cloud Computing Authentication Frameworks and Protocols”(2018).SPECIAL SECTION ON SECURITY ANALYTICS AND INTELLIGENCE FOR CYBER PHYSICAL SYSTEMS.IEEE Access.

[20].Ali Nafea, Ayat Saleh Hasan, Hassan Muayad Ibrahim, Methaq Abdullah Shyaa.”The Impact of Cloud Computingon Network Security and the Risk for Organization Behaviors”. (jan 2022).

[21].SEONGMO AN , ASHER LEUNG , JIN B. HONG , TAEHOON EOM , AND JONG SOU PARK.”Toward Automated Security Analysis and Enforcement for CloudComputing Using Graphical Models for Security”.(July 2022).IEEE Access.

[22].Moulika Bollinadi, Vijay Kumar Damera. “Cloud Computing: Security Issues and Research Challenges”.Journal of Network Communications andEmerging Technologies (JNCET) Volume 7, Issue 11,November (2017).

[23].BADER ALOUFFI , MUHAMMAD HASNAIN , ABDULLAH ALHARBI, WAEL ALOSAIMI , HASHEM ALYAMI, AND MUHAMMAD AYAZ. “A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies”(2021).IEEE Access