Journal of Management & Entrepreneurship UGC Care Group I Journal
ISSN 2229-5348 Vol-10 Issue-01 Jan 2021

Data Security in Cloud Computing

Chayan Bhatt

Assistant Professor

Computer Science Engineering

Arya Institute of Engineering & Technology

Yogyata Agrawal

Assistant Professor

Department of Humanities

Arya Institute of Engineering & Technology

Abstract:

This article explores the security of data in cloud computing. It examines various aspects related to data in the cloud and focuses on ensuring maximum data protection by mitigating risks and threats through data protection methods and approaches used worldwide. While the availability of data in the cloud offers benefits for many applications, it also exposes data to potential risks when exposed to applications that may have security vulnerabilities. Additionally, the use of virtualization in cloud computing can pose data risks when a guest operating system runs over a hypervisor without verifying the reliability of the guest OS, which could potentially have security vulnerabilities. The article also provides insights into data security aspects for Data-in-Transit and Data-at-Rest. The study encompasses all levels of SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service).

Keywords— Data Security, Cloud Computing, Data Protection, Privacy, Risks and threats

Introduction:-

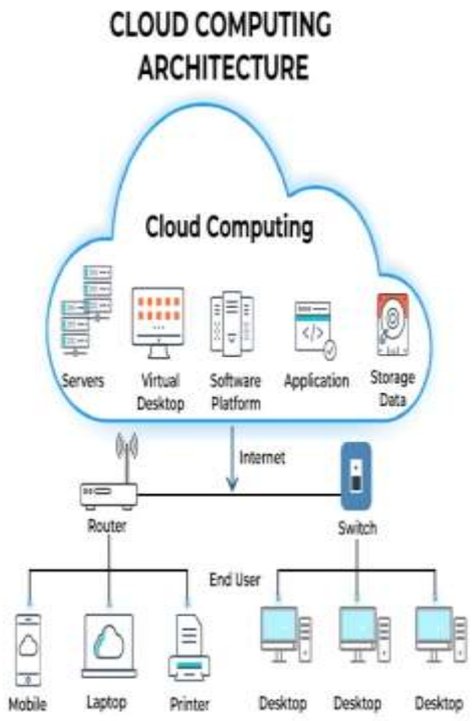

Fig 1: cloud computing architecture

Cloud computing, a relatively new term, is not yet widely used. Among the various definitions available, one of the simplest describes it as a network solutionthat provides affordable, reliable, and easy access to IT resources . Unlike being application-oriented, cloud computing is considered to be service-oriented. This service-oriented approach not only reduces infrastructure overhead and ownership costs but also offers flexibility and improved performance for end users . However, one major concern when adopting cloud computing for data storage is security and privacy . It is crucial for cloud service providers to ensure data integrity, privacy, and protection. Different policies and mechanisms are employed by service providers depending on the nature, type, and size of the data. One advantage of cloud computing is the ability to share data among multiple organizations. However, this advantage also poses risks to the data. To mitigate potential risks, it is necessary to protect data repositories. A key question arises when using the cloud for data storage: should a third-party cloud service be used or should an internal organizational cloud be created? There are instances where the sensitivity of the data makes storing it on a public cloud inappropriate, such as national security data or highly confidential future product details. Exposing such sensitive data on a public cloud can have serious consequences. In such cases, it is highly recommended to store the data using an internal organizational cloud, which can enforce on-premises data usage policies. However, even with this approach, full data security and privacy cannot be ensured, as many organizations lack the qualifications to add all layers of protection to sensitive data. This paper focuses on studying data security techniques used to protect and secure data in the cloud globally. It discusses the potential threats to data in the cloud and the solutions adopted by various service providers to safeguard data. The remainder of the paper is organized as follows: Section 2 provides a review of the existing literature to establish a foundation for discussing various data security aspects. Section 3 examines the types of threats to data in the cloud. Section 4 explores efficient data security techniques implemented worldwide. Finally, the conclusion in the last section summarizes the study

Challenges and solutions:-

Cloud computing is a hot topic at the moment, and there is a lot of ambiguity when it comes to managing its features and resources. Technology is evolving, and as companies scale up, their need to use the latest Cloud frameworks also increases. Some of the benefits introduced by cloud solutions include data security, flexibility, efficiency, and high performance. Smoother processes and improved collaboration between enterprises while reducing costs are among its perks. However, the Cloud is not perfect and has its own set of drawbacks when it comes to data management and privacy concerns. Thus, there are various benefits and challenges of cloud computing. The list below discusses some of the key challenges in the adoption of cloud computing.

Data Security and Privacy

Data security is a major concern when working with Cloud environments. It is one of the major challenges in cloud computing as users have to take accountability for their data, and not all Cloud providers can assure 100% data privacy. Lack of visibility and control tools, no identity access management, data misuse, and Cloud misconfiguration are the common causes behind Cloud privacy leaks. There are also concerns with insecure APIs, malicious insiders, and oversights or neglect in Cloud data management.

Solution: Configure network hardware and install the latest software updates to prevent security vulnerabilities. Using firewalls, antivirus, and increasing bandwidth for Cloud data availability are some ways to prevent data security risks.

2. Multi-Cloud Environments

Common cloud computing issues and challenges with multi-cloud environments are - configuration errors, lack of security patches, data governance, and no granularity. It is difficult to track the security requirements of multi-clouds and apply data management policies across various boards.

Solution: Using a multi-cloud data management solution is a good start for enterprises. Not all tools will offer specific security functionalities, and multi-cloud environments grow highly sophisticated and complex. Open-source products like Terraform provide a great deal of control over multi-cloud architectures.

3. Performance Challenges

The performance of Cloud computing solutions depends on the vendors who offer these services to clients, and if a Cloud vendor goes down, the business gets affected too. It is one of the major challenges associated with cloud computing.

Solution: Sign up with Cloud Service Providers who have real-time SaaS monitoring policies.

4. Interoperability and Flexibility

Interoperability is a challenge when you try to move applications between two or multiple Cloud ecosystems. It is one of the challenges faced in cloud computing. Some common issues faced are:

Rebuilding application stacks to match the target cloud environment's specifications

Handling data encryption during migration

Setting up networks in the target cloud for operations

Managing apps and services in the target cloud ecosystem

Solution: Setting Cloud interoperability and portability standards in organizations before getting to work on projects can help solve this problem. The use of multi-layer authentication and authorization tools is also encouraged for account verifications in public, private, and hybrid cloud ecosystems.

5. High Dependence on Network

Lack of sufficient internet bandwidth is a common problem when transferring large volumes of information to and from Cloud data servers. It is one of the various challenges in cloud computing. Data is highly vulnerable, and there is a risk of sudden outages. Enterprises that want to lower hardware costs without sacrificing performance need to ensure there is high bandwidth, which will help prevent business losses from sudden outages.

Solution: Pay more for higher bandwidth and focus on improving operational efficiency to address network dependencies.

6. Lack of Knowledge and Expertise

Organizations are finding it tough to find and hire the right Cloud talent, which is another common challenge in cloud computing. There is a shortage of professionals with the required qualifications in the industry. Workloads are increasing, and the number of tools launched in the market is increasing. Enterprises need good expertise in order to use these tools and find out which ones are ideal for them.

Solution: Hire Cloud professionals with specializations in DevOps and automation

7. Reliability and Availability

High unavailability of Cloud services and a lack of reliability are two major concerns in these ecosystems. Organizations are forced to seek additional computing resources in order to keep up with changing business requirements. If a Cloud vendor gets hacked or affected, the data of organizations using their services gets compromised. It is another one of the many cloud security risks and challenges faced by the industry.

Solution: Implementing the NIST Framework standards in Cloud environments can greatly improve both aspects.

8. Password Security

Account managers use the same passwords to manage all their Cloud accounts. Password management is a critical problem, and it is often found that users resort to using reused and weak passwords.

Solution: Use a strong password management solution to secure all your accounts. To further improve security, use Multifactor Authentication (MFA) in addition to a password manager. Good cloud-based password managers alert users of security risks and leaks.

9. Cost Management

Even though Cloud Service Providers (CSPs) offer a pay-as-you-go subscription for services, the costs can add up. Hidden costs appear in the form of underutilized resources in enterprises.

Solution: Auditing systems regularly and implementing resource utilization monitoring tools are some ways organizations can fix this. It's one of the most effective ways to manage budgets and deal with major challenges in cloud computing.

10. Lack of expertise

Cloud computing is a highly competitive field, and there are many professionals who lack the required skills and knowledge to work in the industry. There is also a huge gap in supply and demand for certified individuals and many job vacancies.

Solution: Companies should retrain their existing IT staff and help them in upskilling their careers by investing in Cloud training programs.

Literature Review

To grasp the fundamentals of cloud computing and ensure the secure storage of data on the cloud, we have consulted multiple resources. This section offers a literature review to establish a foundation for discussing various aspects of data security. Srinivas, Venkata, and Moiz provide valuable insights into the basic principles of cloud computing.

Their paper explores several key concepts and provides examples of applications that can be developed using cloud computing. Additionally, they highlight how this emerging technology can benefit developing nations . On the other hand, Chen and Zhao address consumer concerns regarding data migration to the cloud. According to them, one of the primary reasons why large enterprises are hesitant to move their data to the cloud is security issues. The authors conduct an exceptional analysis on data security and privacy protection concerns associated with the cloud. They also discuss available solutions to mitigate these issues However, Hu and A. Klein propose a standard method to ensure secure data transfer in the cloud. They present a benchmark for encryption to safeguard data during migration. While additional encryption is necessary for robust security, it does involve additional computational overhead. The benchmark discussed in their study strikes a balance between security and encryption overhead Tjoa, A.M. and Huemer examine the privacy issue by preserving data control to the end user to surge confidence. Several Cloud computing attacks are reviewed and some solutions are proposed to overcome these attacks .

Therefore, Abdelkader and Etriby propose a data security model for cloud computing based on cloud architecture. They also developed software to enrich the effort in data security model for cloud computing further. Cloud computing is a paradigm that changes the way computing resources are distributed and used. The literature on cloud computing encompasses a wide range of topics, reflecting the challenges and opportunities associated with this technology. A major theme in the literature revolves around the benefits of cloud computing, such as scalability, cost, and scalability. Researchers highlight how cloud services enable organizations to dynamically adapt their services based on demand, thereby improving resource utilization and reducing operating costs. The ability to access computing resources over the Internet transforms traditional IT environments, and enables companies to focus on core competencies Capable Security and privacy concerns are recurring themes in the literature, reflecting the importance of data in the cloud. Researchers analyze potential vulnerabilities and threats in cloud infrastructure, and propose strategies and technologies to enhance data security. Encryption, access control methods, and secure networking are areas of active exploration to address the challenges posed by data sharing in the cloud involving multiple tenants. Important measures described in the literature to ensure seamless integration and accessibility of applications across cloud platforms include interoperability standards Standardization efforts aim to prevent vendor lock-in, and enable users to switch between cloud providers effortlessly. The study highlights the need for open standards that encourage interoperability and interoperability across cloud services. The environmental impact of cloud computing has been highlighted, and researchers are exploring various options

Methodologies Used:

The methodologies used in cloud computing research are diverse and multifaceted, encompassing a variety of strategies for addressing the complex challenges and opportunities presented by this technology Below are key strategies approaches to cloud computing research.

Book Review:-

Researchers often start with an in-depth analysis of existing literature to gain a comprehensive understanding of the current state of cloud computing. It involves examining academic papers, industry reports and relevant literature to identify knowledge gaps and areas that require further investigation

Case Studies:-

Case studies play an important role in understanding how cloud computing solutions are used in the real world. Researchers can examine specific organizations or enterprises that have adopted cloud technologies, examine the challenges faced, implementation strategies, and outcomes This approach provides valuable insights into the practical implications of cloud a they pass through.

Surveys and Questionnaires:-

Surveys and questionnaires are employed to acquire information from a wide range of stakeholders, inclusive of

IT professionals, companies, and quit-customers. These gear assist researchers collect quantitative and qualitative facts approximately the adoption of cloud computing, person studies, and perceptions. Survey information can make a contribution to information traits, challenges, and possibilities in the cloud computing landscape.

Experimental Research:

Experimental studies involves the design and implementation of managed experiments to assess specific aspects of cloud computing. This can also include overall performance trying out, safety exams, and scalability experiments. Researchers can use various cloud structures to simulate one-of-a-kind eventualities and degree the effect of specific variables on machine behavior.

Simulation:-

Simulation methodologies are hired to version and analyze complicated cloud environments in a controlled and repeatable way. By simulating the conduct of cloud systems underneath various conditions, researchers can gain insights into overall performance, resource allocation, and scalability with out the need for real-global implementation. Simulations are valuable for testing hypotheses and predicting machine conduct in one-of-a-kind eventualities.

Prototyping and Proof-of-Concepts: Researchers regularly develop prototypes or proof-of-concept implementations to validate theoretical principles in actual-global settings. This fingers-on approach involves constructing small-scale systems or programs to demonstrate the feasibility and effectiveness of proposed answers. Prototyping allows researchers and practitioners determine the realistic implications of their ideas.

Data Analytics and Machine Learning:

With large amounts of data generated by cloud environments, analysts use data analytics techniques and machine learning algorithms to extract meaningful insights This approach helps identify patterns, anomalies and trends in big data, and helps provide a deeper understanding of cloud infrastructure practices and best practices

Security Screening and Penetration Testing:

Due to the high importance of security in cloud computing, the methods typically include security audits and penetration testing. Researchers simulate security attacks to assess the robustness of cloud systems and propose solutions to increase data security and mitigate vulnerabilities

Open donations:

Some researchers are actively involved in the open source community of cloud computing. By contributing to open source projects, researchers collaborate with other industry professionals and researchers, gain practical experience, and contribute to the development of cloud technologies

Future scope:-

The future of cloud computing is constantly evolving due to technological advances, emerging features and changing business environments. Several key factors highlight the direction and growth potential of the field:

Edge Computer Integration: The integration of edge computing into cloud services is expected to increase dramatically. Edge computing brings computing resources closer to the data source, reducing latency and improving real-time performance of applications such as IoT devices, autonomous vehicles and smart cities Cloud providers can expand their offerings with edge computing power has added ease.

Quantum Computing in the Cloud: With the advent of quantum computing, there are challenges and opportunities for cloud computing. Cloud providers are expected to find ways to integrate quantum computing capabilities into their services, allowing users to harness the power of quantum processors for specific tasks Quantum-secure cryptography is also possible it is necessary to ensure data security in the age of quantum computing.

Serverless computing development: Serverless computing, where developers focus on writing code without looking at the underlying infrastructure, is expected to continue to grow. The serverless model reduces operational costs and allows for more efficient use of resources. Future improvements will include increased support for programming languages, improved musicianship tools, and wider adoption across industries.

AI and Machine Learning Integration: Cloud computing will continue to play an important role in the development and deployment of artificial intelligence (AI) and machine learning (ML) applications. Cloud providers can enhance their platforms with specialized AI/ML services, .

Conclusion:

The future of cloud computing is constantly evolving due to technological advances, emerging features and changing business environments. Several key factors highlight the direction and growth potential of the field:

Edge Computer Integration: The integration of edge computing into cloud services is expected to increase dramatically. Edge computing brings computing resources closer to the data source, reducing latency and improving real-time performance of applications such as IoT devices, autonomous vehicles and smart cities Cloud providers can expand their offerings with edge computing power has added ease.

Quantum Computing in the Cloud: With the advent of quantum computing, there are challenges and opportunities for cloud computing. Cloud providers are expected to find ways to integrate quantum computing capabilities into their services, allowing users to harness the power of quantum processors for specific tasks Quantum-secure cryptography is also possible it is necessary to ensure data security in the age of quantum computing.

Serverless computing development: Serverless computing, where developers focus on writing code without looking at the underlying infrastructure, is expected to continue to grow. The serverless model reduces operational costs and allows for more efficient use of resources. Future improvements will include increased support for programming languages, improved musicianship tools, and wider adoption across industries.

AI and Machine Learning Integration: Cloud computing will continue to play an important role in the development and deployment of artificial intelligence (AI) and machine learning (ML) applications. Cloud providers can enhance their platforms with specialized AI/ML services, .

Results:-

When you focus on outcomes or outcomes associated with the adoption and use of cloud computing, they may vary depending on specific goals, strategies, and organizational or individual circumstances The most common factors are benefits here are some types commonly associated with cloud computing.

Cost savings: Cloud computing often results in cost savings because organizations can avoid large upfront investments in hardware, maintenance, and infrastructure. Pay-as-you-go models allow for more predictable operating costs, and products can be increased or decreased based on actual usage.

Scalability Changes : Cloud computing offers scalable and flexible solutions, allowing organizations to easily adapt their computing infrastructure to the changing workload. This scalability ensures more efficient use of resources, enabling businesses to better meet demand.

Advanced Manufacturing: Cloud services provide remote access to applications and data, allowing teams to collaborate regardless of geography. This accessibility increases overall productivity, as employees can work from anywhere using an internet connection.

Fast tracking services: Cloud computing facilitates faster deployment of applications and services. Manufacturers can also take advantage of ready-made infrastructure and services, reducing the time it takes to develop new products or bring new products to market.

Innovation and Speed: Cloud computing accelerates innovation by providing a platform for rapid testing and prototyping. Organizations can easily adopt new technologies and test new ideas without having to make significant upfront investments.

Business Continuity and Disaster Recovery: Cloud services provide robust business continuity and disaster recovery solutions

References:

[1] Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." Future Generation Computer

[2] Systems 28, no. 3 (2012): 583-592.

[3] Matthew, Olumuyiwa, Carl Dudley, and Robert Moreton. "A Review Of Multi-Tenant Database And Factors That

[4] Influence Its Adoption." (2014).

[5] WalidRjaibi, Mark Wilding,” Best Practices Data Protection in the Cloud “, IBM® DB2® for Linux®, UNIX®, and

[6] Windows®, February 2011

[7] Kalpana, Parsi, and SudhaSingaraju. "Data security in cloud computing using RSA algorithm" IJRCCT 1,

[8] Wang, Cong, Qian Wang, Kui Ren, and Wenjing Lou. "Privacy-preserving public auditing for data storage security in

[9] cloud computing." In INFOCOM, 2010 Proceedings IEEE, pp. 1-9. Ieee, 2010.

[10] R. K. Kaushik Anjali and D. Sharma, "Analyzing the Effect of Partial Shading on Performance of Grid Connected Solar PV System", 2018 3rd International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE), pp. 1-4, 2018.

[11] R. Kaushik, O. P. Mahela, P. K. Bhatt, B. Khan, S. Padmanaban and F. Blaabjerg, "A Hybrid Algorithm for Recognition of Power Quality Disturbances," in IEEE Access, vol. 8, pp. 229184-229200, 2020.

[12] Kaushik, R. K. "Pragati. Analysis and Case Study of Power Transmission and Distribution." J Adv Res Power Electro Power Sys 7.2 (2020): 1-3.

[13] Akash Rawat, Rajkumar Kaushik and Arpita Tiwari, "An Overview Of MIMO OFDM System For Wireless Communication", International Journal of Technical Research & Science, vol. VI, no. X, pp. 1-4, October 2021.

[14] R. Kaushik, O. P. Mahela and P. K. Bhatt, "Hybrid Algorithm for Detection of Events and Power Quality Disturbances Associated with Distribution Network in the Presence of Wind Energy," 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2021, pp. 415-420.

[15] P. K. Bhatt and R. Kaushik, "Intelligent Transformer Tap Controller for Harmonic

Elimination in Hybrid Distribution Network," 2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2021, pp. 219-225

[16] R. Kaushik, O. P. Mahela and P. K. Bhatt, "Events Recognition and Power Quality Estimation in Distribution Network in the Presence of Solar PV Generation," 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT), Bhopal, India, 2021, pp. 305-311

[17] Jain, B.B., Upadhyay, H. and Kaushik, R., 2021. Identification and Classification of Symmetrical and Unsymmetrical Faults using Stockwell Transform. Design Engineering, pp.8600-8609.

[18] Rajkumar Kaushik, Akash Rawat and Arpita Tiwari, "An Overview on Robotics and Control Systems", International Journal of Technical Research & Science (IJTRS), vol. 6, no. 10, pp. 13-17, October 2021.

[19] Simiran Kuwera, Sunil Agarwal and Rajkumar Kaushik, "Application of Optimization Techniques for Optimal Capacitor Placement and Sizing in Distribution System: A Review", International Journal of Engineering Trends and Applications (IJETA), vol. 8, no. 5, Sep-Oct 2021.

[20] Kumar, R., Verma, S., & Kaushik, R. (2019). Geospatial AI for Environmental Health: Understanding the impact of the environment on public health in Jammu and Kashmir. International Journal of Psychosocial Rehabilitation, 1262–1265