Anusandhanvallari
Vol 2020, No.1
December 2020
ISSN 2229-3388

A Shift from Traditional to On-Demand Access of Computing Resources Through Cloud Computing

Manbir Sandhu

Department of Computer Applications, University Institute of Computing, Chandigarh University, Mohali, India

Abstract

Cloud computing has transformed traditional computing by shifting from infrastructure-based systems to on-demand access to computing resources over the Internet. Unlike conventional computing, which requires significant investment in hardware, software and maintenance, cloud computing provides flexible and scalable resources such as servers, storage, applications and networks on a pay-as-you-go basis. This technology offers numerous advantages, including cost efficiency, remote accessibility, rapid processing, scalability and effective resource utilization. The increasing adoption of cloud computing has revolutionized the way individuals and organizations store, manage and access data and services. However, along with its benefits, cloud computing also introduces major security and privacy concerns, including data breaches, unauthorized access, cyber attacks and data loss. Therefore, security has become a crucial factor in ensuring the reliability and trustworthiness of cloud services. This paper discusses the evolution, benefits and security challenges associated with cloud computing technology.

Keywords: Cloud computing, scalable, computing, resources, data breach, privacy, security.

Introduction

Cloud computing is a distributed computing paradigm that provides access to a shared pool of scalable and virtualized resources such as data storage, servers, networks, computational services and applications. It is an architecture that centralizes hardware and software resources and dynamically reconfigures them to meet the varying on-demand requirements of users while optimizing resource utilization. According to the definition, "Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications and services that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1]. Cloud computing is implemented through technologies such as utility computing, virtualization, service-oriented architecture and parallel computing. In the field of Information Technology, the term "cloud" refers to the integration of networks, hardware, storage systems and interfaces that collectively deliver services to users. Today, companies such as Google, Yahoo and Amazon provide cloud-based services and are known as Cloud Service Providers (CSPs). Apart from CSPs, two other important entities in cloud computing are the Data Owner (DO) and the User. CSPs maintain profiles of both users and data owners while managing all cloud-related operations. Data owners can store their files and information on cloud servers and users can access these resources according to their requirements [2].

Cloud computing delivers applications and IT capabilities over the Internet using third-party infrastructure. Resources such as CPU power and storage are offered as utility services that users can lease and release on a pay-as-you-go and on-demand basis [1]. The technology offers numerous advantages, including flexibility, reliability, virtually unlimited storage capacity, portability, efficient remote accessibility and high processing power. However, because cloud computing relies on shared Internet-based resources, it is also exposed to

several security and privacy threats. These threats include data breaches, malware injection attacks, data loss, insecure application programming interfaces (APIs), hacking, denial-of-service (DoS) attacks, malicious insiders and failures of cloud services. Ensuring the security of cloud networks, resources and stored data remains a major concern for both cloud service providers and users. Although cloud computing technologies and security mechanisms continue to evolve rapidly, there is still a significant need for more robust and reliable cloud security solutions. Several incidents reported in 2019 further demonstrated the vulnerability of cloud environments to various security attacks.

Several major cloud security incidents reported in 2019 highlighted the vulnerabilities associated with cloud-based systems and services. Capital One, the tenth-largest bank in the United States in terms of assets, suffered a breach due to a misconfigured Web Application Firewall (WAF), resulting in the copying of nearly 700 folders and sensitive customer data to an external location. State Farm, an American insurance and financial services organization, experienced a credential stuffing attack that enabled unauthorized access to customer accounts. Although the company stated that no fraud or personally identifiable information (PII) was compromised, concerns regarding the extent of the breach remained. Similarly, Presbyterian Health Services faced a phishing attack in which employees unknowingly responded to malicious emails, leading to unauthorized access to highly confidential health records of nearly a quarter million individuals. In another incident, several Texas Municipalities were affected after attackers exploited vulnerabilities in third-party software providers. The attackers encrypted critical data and demanded a ransom of $2.5 million for restoring access. The compromised information included state statistics, utility records and credit card payment data related to thousands of citizens. Furthermore, Imperva, a leading cyber security company, also experienced a data breach affecting its Web Application Firewall services. The compromised information included email addresses, encrypted passwords, SSL certificates and API keys. These incidents demonstrate the growing need for stronger and more resilient cloud security mechanisms. According to the State of Cloud Security 2020 Report, nearly 93% of organizations in India encountered at least one public cloud security incident during the previous year. Among these incidents, 53% of organizations experienced ransomware attacks, while 49% reported malware infections and an equal percentage faced data exposure incidents. Additionally, 48% of organizations reported cases of compromised accounts, whereas 36% were affected by crypto jacking attacks. The report commissioned by Sophos, a cyber security solutions provider, was based on a survey of 3,500 IT managers across 26 countries, including 227 respondents from India

Objectives

The main objective of the study is to understand security concerns of cloud computing, the existing solutions to handle these concerns and the scope of further study in this area. For this, the paper is outlined as follows – Section –III presents an introduction to cloud computing, its framework based on the service and deployment models followed by the study of existing literature in Section IV. The security issues, the threats that loom over cloud computing and the mitigation techniques being used are presented in Section V. Section VI, discusses the applications of this progressing technology followed by Section VII containing the findings of the study and the paper is concluded in Section VIII.

Overview of Cloud Computing

Cloud Computing Definition

According to the National Institute of Standards and Technology (NIST), cloud computing is “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing

resources such as networks, servers, storage, applications and services that can be rapidly provisioned and released with minimal management effort or service provider interaction" [2].

Cloud computing enables users to access computing resources and services anytime and from anywhere according to their requirements. Rather than establishing and maintaining their own physical infrastructure, users generally rely on third-party service providers for internet-based computing services. In this model, users are charged only for the resources and services they utilize [4][5].

John R. Staten and colleagues described cloud computing as a modern IT outsourcing model that, at the time, had not fully satisfied the requirements of enterprise-level IT systems and lacked support from many major corporate vendors [3][6].

According to Rajkumar Buyya and co-authors, a cloud is a parallel and distributed computing system composed of interconnected and virtualized computers that are dynamically allocated and delivered as unified computing resources in accordance with service-level agreements negotiated between service providers and consumers [3][7].

Cloud Computing Service Delivery Models

As per NIST [2], there are three major categories of services, also known as service models as discussed below:

3.2.1 Software as a Service (SaaS)

Software as a Service (SaaS) represents the topmost application layer of cloud computing, where software applications are delivered to users over the Internet. In this model, applications hosted on the cloud infrastructure of the service provider are made available to multiple users on demand through web browsers. The Cloud Service Provider (CSP) manages the underlying infrastructure, including networks, storage, servers, operating systems and application capabilities, while the consumer is responsible only for application-specific configuration settings. Examples of SaaS include Google Docs and Salesforce.

3.2.2 Platform as a Service (PaaS)

Platform as a Service (PaaS) forms the middle layer of cloud computing and provides a platform for users to develop, test, deploy and manage applications. In this model, users create or acquire applications using programming languages, libraries and tools supported by the CSP and these applications are hosted on the cloud infrastructure. Although consumers can manage and control the deployed applications, they do not have control over the underlying cloud infrastructure. Examples of PaaS platforms include Microsoft Azure and Google App Engine.

3.2.3 Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) is the foundational layer of cloud computing that provides essential computing resources such as servers, storage and networking on an on-demand basis through service APIs. In this model, consumers are not aware of the underlying physical infrastructure but are given control over certain components, including operating systems, hosted applications, storage resources and limited networking features such as firewalls. IaaS services are generally billed according to resource usage, reflecting the amount of allocated and consumed resources. Amazon EC2 is a well-known example of IaaS.

Cloud Computing Deployment Models

Broadly, the cloud computing deployment models are categorized into four types:

3.3.1 Private Cloud

A private cloud refers to an internal cloud infrastructure that is exclusively owned and operated by a single organization or company. In this deployment model, the organization maintains complete control over all aspects of the cloud environment, including the applications being executed, the location of deployment and the users or organizations permitted to access it. Private clouds are generally built by virtualising an organization's existing infrastructure, which improves resource utilization and operational efficiency. The primary advantage of a private cloud is that it offers the benefits of virtualization while allowing the organization to retain full authority and control over its infrastructure.

3.3.2 Public Cloud

In a public cloud environment, cloud resources such as servers, storage, networks and other services are shared among multiple users, organizations, or customers. These services are made available to the public on a pay-as-you-use basis, allowing users to pay only for the resources they consume. Because public clouds are openly accessible and shared among many users, security and privacy remain major concerns in this deployment model [4].

3.3.3 Community Cloud

A community cloud is a cloud infrastructure shared by a group of organizations that have common objectives, policies, or security requirements. The infrastructure may be managed either collectively by the participating organizations or by a third-party provider. Community clouds are often used in situations where multiple organizations need to collaborate while maintaining shared security and operational standards, such as in national security applications [4].

3.3.4 Hybrid Cloud

A hybrid cloud combines two or more distinct cloud deployment models, such as private, public, or community clouds, which are integrated through standardized technologies [4]. This environment is typically managed by a central administrator and enables the portability of data and applications across different cloud platforms. By integrating multiple cloud models, the hybrid cloud provides greater flexibility, scalability and secure access control between users and cloud service providers [4].

Essential Characteristics of Cloud Computing

According to the National Institute of Standards and Technology [2], a cloud computing model is characterized by five essential features:

3.4.1 Network Access

Cloud resources and services can be accessed over a network through a variety of heterogeneous devices and platforms, including desktops, laptops, mobile phones and tablets.

3.4.2 Resource Pooling

Resource pooling is a fundamental characteristic of cloud computing in which resources such as networks, storage and computing power are shared among multiple users while maintaining location independence. Both physical and virtual resources are dynamically assigned and reassigned according to the changing needs of users.

3.4.3 On-Demand Service

Cloud computing enables users to access and utilize services whenever and wherever required, based on their specific demands and requirements.

3.4.4 Pay-as-You-Go Model

Cloud Service Providers (CSPs) continuously monitor and measure the usage of cloud resources and services by individual users. Users are then charged according to their actual consumption, ensuring transparency in service utilization and billing.

3.4.5 Scalability

Cloud computing offers scalability by allowing resources and services to be expanded or reduced in response to fluctuating user demands. Users can increase or decrease their resource usage at any time as needed.

Advantages and Disadvantages of Cloud Computing

Cloud technology provides numerous advantages, including extensive data storage capacity, high processing speed, unlimited backup facilities, scalability, cost-effectiveness and flexible access to services anytime and from anywhere. However, despite these benefits, several challenges continue to hinder the widespread adoption and success of cloud computing. These challenges include security and privacy concerns, service downtime, limited user control, data loss or leakage, internet connectivity problems, authentication issues and threats to data confidentiality and integrity. This study offers a comprehensive understanding of the major security threats associated with cloud computing as well as the possible solutions to address them.

Literature Review

This section presents a review of the existing literature related to cloud framework. The reviewed studies provide insight into the current state of knowledge, help identify gaps in existing research and offer guidance for future work in the related domain.

Kirti Walia and Kamaljit Singh Saini [8] presented a study titled “Security Issues of Cloud Computing”, in which they discussed cloud architecture along with various security controls associated with cloud environments.

P. Hima Bindu and T. Bhaskar Reddy [9] conducted a study titled “An Exploration of Security Issues for Cloud Computing”. Their work surveyed cloud architectural components, service deployment models, cloud security concepts and security requirements.

Khalil Al-Shqeerat and Husam Ahmad Al Hamad [10] published “A Taxonomy of Virtualization Security Issues in Cloud Computing Environments”, where they identified major virtualization-related security issues, threats in virtual environments and possible solutions.

Lubna Alhenaki, Alaa Alwatban, Bashaer Alamri and Noof Alarifi [11] authored “A Survey on the Security of Cloud Computing”, which reviewed major security attacks affecting cloud computing and discussed possible countermeasures and solutions for comparative analysis.

Priyanshu Srivastava and Rizwan Khan [12] wrote “A Review Paper on Cloud Computing”, focusing on the different types, components, approaches and advantages of cloud computing.

R. K. Bathla and Suseendran G. [13] presented "Research Analysis of Big Data and Cloud Computing with Emerging Impact of Testing", which discussed different forms of testing applicable to cloud-based applications and software systems.

Divya Kapil, Sonu Kumar, Parshant Tyagi and Vinay Prasad Tamta [14] authored "Cloud Computing: Overview and Research Issues", emphasizing virtualization as a core technology of cloud computing and highlighting associated research challenges.

Suyel Namasudra, Pinki Roy and Balamurugan Balusamy [15] published "Cloud Computing: Fundamentals and Research Issues", which provided a detailed discussion and categorization of various cloud computing research issues.

Isaac Odun-Ayo, Olasupo Ajayi, Boladele Akanle and Ravin Ahuja [16] presented "An Overview of Data Storage in Cloud Computing", focusing on cloud storage trends and associated issues.

Saneh Lata Yadav and Asha Sohal published [17] "Review Paper on Big Data Analytics in Cloud Computing", which examined the flow of big data within cloud environments and discussed related challenges.

Ashish Singh and Kakali Chatterjee [18] conducted a survey titled "Cloud Security Issues and Challenges", highlighting important security concerns and challenges in cloud computing.

Gary Garrison, Sanghyun Kim and Robin L. Wakefield [19] published "Success Factors for Deploying Cloud Computing", which discussed research models, methodologies, hypotheses and the critical factors influencing cloud computing deployment.

In 2014, Chaoqun Yu, Lin Yang, Yuan Liu and Xiangyang Luo [20] authored "Research on Data Security Issues of Cloud Computing", focusing on advancements in technologies related to cloud data security.

Ni Zhang, Di Liu and Yun-Yong Zhang [21] presented "A Research on Cloud Computing Security", which explored cloud security issues along with possible solutions.

In 2012, Han Qi and Abdullah Gani [22] presented the study "Research on Mobile Cloud Computing: Review, Trend and Perspectives". The study described Mobile Cloud Computing (MCC) as an extension and advancement of both mobile computing and cloud computing, inheriting important features such as high mobility and scalability.

Shyam Patidar, Dheeraj Rane and Pritesh Jain [23] authored "A Survey Paper on Cloud Computing". Their work discussed the architecture and major components of cloud computing while also highlighting its opportunities and challenges.

Ting-ting Yu and Ying-Guo Zhu [24] published "Research on Cloud Computing and Security". The study focused on cloud environment architecture along with the risks and countermeasures associated with cloud computing security.

Yubo Tan and Xinlei Wang [25] presented "Research of Cloud Computing Data Security Technology". Their research emphasized data security and encryption techniques in cloud computing, including a security mechanism based on full homomorphic encryption.

Santosh Kumar and R. H. Goudar [26] authored "Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey". The study compared different cloud computing platforms and discussed various challenges related to the adoption of cloud computing technologies.

Pardeep Sharma, Sandeep K. Sood and Sumeet Kaur [27] published "Security Issues in Cloud Computing". Their work provided a brief discussion on the major security issues in cloud computing and the possible solutions to address them.

Cloud Security

Key Security Issues in Cloud Computing

Virtualization and cloud computing are advanced technologies that provide flexible and scalable computing resources. However, many organizations remain cautious about adopting cloud technology due to concerns related to data and network security. Some major security concerns in cloud computing are as follows:

5.1.1 Authentication

Authentication ensures that only authorized users can access cloud resources using valid login credentials. Cloud environments commonly use Single Sign-On (SSO) mechanisms, allowing users to access multiple services with a single username and password. However, password theft and hacking remain major security threats.

5.1.2 Integrity

Integrity ensures that cloud data remains accurate, complete and unaltered by unauthorized users. Regular backup mechanisms are essential to protect data from loss or corruption and to ensure recovery during system failures or security incidents.

5.1.3 Availability

Availability refers to uninterrupted access to cloud resources, even during malicious attacks or system failures. For mission-critical applications, organizations require business continuity and redundancy plans to maintain reliable service availability.

5.1.4 Confidentiality

Confidentiality ensures that sensitive information is protected from unauthorized access. Data confidentiality may be compromised through physical breaches, social engineering attacks, or insecure communication channels lacking encryption.

5.1.5 Accountability

Accountability involves defining responsibilities and service obligations between cloud providers and users. The absence of clear policies and service agreements in cloud environments can make it difficult to identify responsibility for service failures or security violations.

Threats in Cloud Technology

The following threats are prominent in the cloud computing framework:

1. WS-Security

Web Services Security (WS-Security) is associated with protecting the confidentiality and integrity of data exchanged through web services.

2. Phishing Attack

In a phishing attack, attackers deceive users through fake websites, spoofed emails, or manipulated DNS services to steal login credentials and sensitive information, thereby compromising confidentiality.

3. Wrapping Attack

A wrapping attack exploits vulnerabilities in XML Signature mechanisms used for authentication and integrity verification within cloud services.

4. Injection Attack

This attack involves inserting malicious code, services, or virtual machines into the cloud environment, which can disrupt operations and affect service availability.

5. IP Spoofing

IP spoofing refers to the illegal use of another user's identity or authentication details, such as usernames and passwords, to gain unauthorized access to confidential information.

6. Tampering

Tampering involves unauthorized modification of data during transmission or storage, thereby affecting the integrity and reliability of information.

7. Repudiation

Repudiation occurs when users perform unauthorized or illegal actions in systems lacking proper tracking and auditing mechanisms, making accountability difficult.

8. Information Disclosure

Information disclosure refers to unauthorized access to another user's cloud data, resulting in the loss of data confidentiality and privacy.

9. Denial of Service (DoS) Attack

A Denial of Service attack makes cloud services or web servers unavailable to legitimate users by overwhelming resources or exploiting system vulnerabilities.

10. Man-in-the-Middle Attack

In this attack, an adversary secretly intercepts and alters communication between two parties, compromising data integrity and availability.

11. Lack of Trust

With the growing number of Cloud Service Providers (CSPs), users often face challenges in identifying reliable and trustworthy cloud providers.

12. Client Monitoring and Security

Cloud Service Providers must continuously monitor users, their access rights and service usage to maintain security and prevent unauthorized activities.

13. Weak Service Level Agreements (SLAs)

Inadequate or unclear SLAs between CSPs and users can lead to unreliable services, poor security measures, vendor lock-in, hidden costs and data availability concerns.

14. TCP Hijacking

TCP hijacking occurs when an attacker impersonates a trusted client by replacing its IP address, allowing unauthorized access and compromising confidentiality and integrity.

15. Password Guessing

Password guessing attacks involve attempting to crack user passwords to gain unauthorized access, making them one of the most common threats in cloud environments.

16. Data Loss or Leakage

Data loss or leakage occurs when sensitive cloud data is mishandled, exposed, or illegally shared by unauthorized parties, resulting in privacy and security violations.

17. Computer Network Attack

Computer network attacks aim to disrupt, damage, or destroy cloud networks and the data stored within them, affecting overall system functionality and security.

18. TCP Hijacking

This attack involves the attacker taking over an active communication session by impersonating a trusted system, thereby threatening data confidentiality and integrity.

19. Data Loss or Leakage

Improper handling or unethical storage practices by service providers can result in unauthorized disclosure or duplication of users' sensitive cloud data.

Mitigation Techniques

The following techniques deal with the security concerns in cloud framework:

1. Identity-Based Authentication (IBA)

In Identity-Based Authentication, users within a domain are assigned specific identities and a global master key is used to authenticate them, ensuring secure and private access to cloud resources.

2. RSA Algorithm

The RSA (Rivest–Shamir–Adleman) algorithm uses digital signatures and encryption techniques to provide secure communication and protect data from unauthorized access.

3. Dynamic Intrusion Detection System

This system is designed to detect and prevent suspicious or malicious activities in cloud environments, thereby enhancing overall cloud security.

4. Multi-Tenancy Based Access Control Model (MTACM)

MTACM integrates authentication, authorization and access control mechanisms into cloud systems to ensure secure sharing of resources among multiple users.

5. TLS Handshake Protocol

The Transport Layer Security (TLS) handshake protocol secures communication between cloud users and service providers by reducing ambiguities and ensuring secure data transactions.

6. Public Key-Based Homomorphic Authenticator with Random Masking

This method supports privacy-preserving public cloud auditing by protecting sensitive data while enabling secure verification processes.

7. Third Party Auditor (TPA)

A Third Party Auditor provides independent security auditing services to ensure the safety and integrity of cloud storage systems and services.

8. Probabilistic Sampling Technique

This technique enhances secure data storage, computation and privacy protection within cloud computing environments.

9. Diffie–Hellman Key Exchange

This cryptographic protocol allows secure sharing of secret symmetric keys between cloud users and service providers for protected communication.

10. Private Face Recognition

Private face recognition systems use facial authentication techniques and transmit encrypted authentication results to maintain user privacy and security.

11. Message Authentication Codes (MACs)

MACs are used to verify the integrity and authenticity of data by comparing the received data with precomputed authentication values.

12. Data Coloring and Software Watermarking Techniques

These techniques help distinguish user data and restrict unauthorized access, thereby protecting sensitive information from cloud providers or attackers.

13. Cloud Dependability Model

This model improves the reliability and security of heterogeneous cloud environments using advanced virtualization techniques.

14. Key Policy Attribute-Based Encryption (KP-ABE)

KP-ABE associates specific attributes with encrypted data and allows access only to users possessing the required attribute-based keys.

15. Role-Based Access Control (RBAC)

RBAC assigns permissions to specific roles rather than individual users, simplifying access management and improving security within cloud systems.

16. Identity Management

Identity management systems authenticate users and services based on predefined credentials and characteristics to ensure secure access to cloud resources.

17. Service Level Agreement (SLA)

An SLA is a formal agreement between cloud users and service providers that clearly defines services, responsibilities, security measures and dispute-resolution mechanisms to ensure transparency and reliability.

6. Applications of Cloud Computing

Cloud computing has transformed various business operations and significantly changed the way organizations manage and utilize technology. Its applications continue to expand with the advancement of cloud technologies, benefiting organizations of all sizes by improving efficiency, scalability and cost-effectiveness. Some major applications of cloud computing are discussed below:

1. Chatbots

Cloud computing provides extensive computational power and large-scale storage capabilities, enabling organizations to store and process massive amounts of user data. This allows businesses to develop intelligent chatbots capable of delivering highly personalized and contextual interactions based on user behavior and preferences. Cloud-based chatbots enhance customer engagement and improve user experience through real-time communication and automated support services.

2. Data Backup and Recovery

Traditional data backup systems were often time-consuming, costly and difficult to manage due to hardware maintenance and storage limitations. Cloud computing has simplified the backup and restoration process by offering automated, scalable and reliable storage solutions. Organizations can schedule regular backups, store large volumes of data securely and quickly restore information without concerns about hardware failures or storage shortages.

3. Communication Services

Cloud computing has greatly improved organizational communication by enabling network-based access to messaging and collaboration tools. Messages, files and other communication-related data are stored securely on the cloud rather than on individual devices. This allows employees to access information from any location, thereby enhancing collaboration, flexibility and remote working capabilities. Many modern communication and messaging applications are cloud-based.

4. Big Data Analytics

Cloud computing supports big data analytics by providing virtually unlimited storage capacity, advanced computational resources and access to modern analytical tools. Organizations can analyze massive datasets in real time to gain valuable insights, improve decision-making, identify risks and make accurate predictions. Cloud-based analytics solutions also reduce infrastructure costs and make advanced data processing more accessible and efficient.

5. Development and Testing Environments

The cloud enables organizations to create flexible and cost-effective environments for software development and testing. Unlike traditional systems that require physical infrastructure, cloud-based environments can be quickly created, modified and removed as needed. This reduces operational costs, accelerates project development and allows testing teams to scale resources according to project requirements without significant financial investment.

6. Application Development

Cloud platforms provide an ideal environment for developing web, mobile and gaming applications by offering scalable resources and multi-platform support. Developers can build, test and deploy applications more efficiently while reducing infrastructure and maintenance costs. Cloud computing also improves application performance, scalability and user experience, resulting in faster and more reliable software development processes.

Overall, cloud computing has become an essential technology that enhances productivity, streamlines business operations, improves data management and supports innovation across multiple domains.

7. Observations

1. Rapid advancements in cloud computing have led to its widespread adoption across various sectors and its usage is expected to continue increasing due to the numerous benefits it offers. Features such as scalability, flexibility, cost-effectiveness, remote accessibility and high computational power have made cloud computing an essential technology in the modern digital era.

2. Cloud computing encompasses a well-defined architecture that includes different service models and deployment models. The major service models include Software as a Service (SaaS), Platform as a Service (PaaS)and Infrastructure as a Service (IaaS), while deployment models consist of public, private, hybrid and community clouds, each designed to meet specific organizational and user requirements.

3. Existing research in the field of cloud computing provides valuable insights into the development, applications, challenges and advancements associated with cloud technologies. Previous studies have contributed significantly toward understanding cloud architecture, security mechanisms, resource management and service optimization.

4. Security concerns continue to be one of the major obstacles in the adoption and implementation of cloud computing technologies. Issues related to data privacy, unauthorized access, data breaches, malware attacks, insecure interfaces and service failures create significant challenges for both cloud service providers and users.

5. Various threats are prevalent in cloud computing environments and can adversely affect the confidentiality, integrity and availability of cloud resources and data. These threats include phishing attacks, ransomware, denial-of-service (DoS) attacks, malicious insiders, account hijacking, virtualization vulnerabilities and data leakage.

6. Different security mechanisms and tools are employed to address the security concerns of Cloud Service Providers (CSPs) and Data Owners (DOs). These include encryption methods, authentication protocols, firewalls, intrusion detection systems, access control techniques and monitoring tools that help strengthen cloud security and protect sensitive information.

7. The application of cloud computing in diverse domains such as healthcare, education, banking, business, research, e-commerce and government services clearly demonstrates the enormous potential and advantages of cloud technology. Cloud computing has significantly improved efficiency, collaboration, storage management and service delivery across these sectors.

8. Increasing complexity and large-scale usage of cloud networks are expected to intensify security concerns in the future. Consequently, there is substantial scope for further research aimed at analyzing existing security mechanisms, identifying their limitations and developing more robust, reliable and efficient cloud security solutions.

Conclusion

Cloud computing has significantly transformed the traditional approach to computing by shifting the emphasis from conventional hardware and software systems to advanced networks and cloud-based applications. It has revolutionized the manner in which IT services are delivered, accessed and utilized by both individuals and organizations. However, security remains one of the most critical factors in cloud computing, as the success and reliability of cloud services largely depend on the protection of data, resources and network infrastructure from various cyber threats and unauthorized access. To effectively leverage the advantages of cloud technology and maintain a competitive edge, it is essential to understand the concept of cloud computing, its architecture and its security framework, including security requirements, challenges and the various threats associated with cloud environments. A comprehensive understanding of these aspects further facilitates research in the crucial area of cloud security, particularly issues related to data protection, privacy, authentication and cloud network security. Although achieving complete end-to-end security remains challenging due to the complexity and dynamic nature of cloud networks, there exists substantial scope for future research focused on enhancing existing security techniques and developing more robust, reliable and efficient security solutions for cloud computing environments.

References

[1] Divya Kapil, Sonu Kumar, Parshant Tyagi, Mr. Vinay Prasad Tamta, “Cloud Computing: Overview and Research Issues”, pp. 439-443, 2018
[2] Mell, P. and Grance, T. (2018). The NIST Definition of Cloud Computing. [online] National Institute of Standards and Technology | NIST. Available at: https://www.nist.gov/ [Accessed 15 Nov. 2018].
[3] Suyel Namasudra, Pinki Roy, Balamurugan Balusamy, “Cloud Computing: Fundamentals and Research Issues”, Proceedings of- Second International Conference on Recent Trends and Challenges in Computational Models, 2017
[4] Priyanshu, Srivartava, Rizwan Khan, “A Review Paper on Cloud Computing”, International Journals of Advanced Research in Computer Science and Software Engineering, Volume-8, Issue-6, 2018
[5] Herhalt, J., Cochrane, K., “Exploring the Cloud: A Global Study of Government’s Adoption of Cloud”, IEEE, 2012
[6] J. Staten, et al., “Is Cloud Computing ready for the enterprise?” Forrester, 2008.
[7] Buyya, C.S. Yeo, and S. Venugopal, “Market-oriented Cloud Computing: vision, hype, and reality for delivering IT services as computing utilities,” Proc. of the 10th IEEE International Conference on High Performance Computing and Communications, Washington, DC, USA, pp. 5-13, 2008.
[8] Kirti Walia and Kamaljit Singh Saini, “Security Issues of Cloud Computing,”, Internal Journal of Science and Technology, Vol 29, 10s ,2020.

[9] Almutairy, Nadiah & Al-Shqeerat, Khalil & AlHamad, Husam, "A Taxonomy of Virtualization Security Issues in Cloud Computing Environment", Indian Journal of Science and Technology. 12. 19. 10.17485/ijst/2019/v12i3/139557, 2019
[10] Alhenaki, Lubna & Alwatban, Alaa & Alamri, Bashaer & Alarifi, Noof. ,"A Survey on the Security of Cloud Computing", 1-7. 10.1109/CAIS.2019.8769497, 2019
[11] Srivastava, Priyanshu & Khan, Rizwan, "A Review Paper on Cloud Computing. International Journal of Advanced Research in Computer Science and Software Engineering", 2018, 8. 17. 10.23956/ijarcsse.v8i6.711.
[12] R. K. Bathla and R. K. Bathla and Suseendran G., "Research Analysis of Big Data and Cloud Computing with Emerging Impact of Testing," , 2018.
[13] Kapil, Divya & Tyagi, Parshant & Kumar, Sonu & Tamta, Vinay. (2017). Cloud Computing: Overview and Research Issues, 71-76. 10.1109/ ICGI.2017.18.
[14] Suyel Namasudra, Pinki Roy and Balamurugan Balusamy, "Cloud Computing: Fundamentals and Research Issues," "Scalable Computing: Practice and Experience", vol. 18, no. 4, pp. 401–414, 2017.
[15] Isaac Odun-Ayo, Olasupo Ajayi, Boladele Akanle and Ravin Ahuja, "An Overview of Data Storage in Cloud Computing," "Journal of Physics: Conference Series", vol. 933, no. 1, 2017.
[16] Saneh Lata Yadav and Asha Sohal, "Review Paper on Big Data Analytics in Cloud Computing,", International Journal of Computer Sciences and Engineering, vol. 5, no. 6, pp. 177–180, 2017.
[17] Ashish Singh and Kakali Chatterjee, "Cloud Security Issues and Challenges: A Survey," "Journal of Network and Computer Applications", vol. 79, pp. 88–115, 2017
[18] Gary Garrison, Sanghyun Kim and Robin L. Wakefield, "Success Factors for Deploying Cloud Computing," "Communications of the ACM", vol. 58, no. 11, pp. 62–68, 2015.
[19] Chaoqun Yu, Lin Yang, Yuan Liu and Xiangyang Luo, "Research on Data Security Issues of Cloud Computing," in "Proceedings of the International Conference on Cyberspace Technology", pp. 1–5, 2014.
[20] Ni Zhang, Di Liu and Yun-Yong Zhang, "A Research on Cloud Computing Security," International Journal of Smart Home, vol. 7, no. 5, pp. 239–244, 2013.
[21] Han Qi and Abdullah Gani, "Research on Mobile Cloud Computing: Review, Trend and Perspectives," in "2012 Second International Conference on Digital Information and Communication Technology and Its Applications (DICTAP)", IEEE, pp. 195–202, 2012.
[22] Shyam Patidar, Dheeraj Rane and Pritesh Jain, "A Survey Paper on Cloud Computing," ,Proceedings of the International Journal of Computer Science and Information Technologies, vol. 3, no. 1, pp. 3942–3945, 2012.
[23] Ting-ting Yu and Ying-Guo Zhu, "Research on Cloud Computing and Security," "Advanced Materials Research", vols. 433–440, pp. 6326–6329, 2012.
[24] Yubo Tan and Xinlei Wang, "Research of Cloud Computing Data Security Technology," "International Journal of Digital Content Technology and its Applications", vol. 6, no. 20, pp. 385–390, 2012.
[25] Santosh Kumar and R. H. Goudar, "Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey," "International Journal of Future Computer and Communication", vol. 1, no. 4, pp. 356–360, 2012.
[26] Pardeep Sharma, Sandeep K. Sood and Sumeet Kaur, "Security Issues in Cloud Computing," ,2011 World Congress on Information and Communication Technologies (WICT), IEEE, pp. 36–41, 2011.