Journal of Intelligent System and Applied Data Science (JISADS)

Journal homepage : https://www.jisads.com

ISSN (2974-9840) Online

Emerging Trends in Cloud Computing: A Comprehensive Analysis of Deployment Models and Service Models for Scalability, Flexibility, and Security Enhancements.

*Rajesh komar1, Arjun Patil 1**
Ragishkaa22@Gmail.Com, patil.Arjun2002@gmail.Com

1 Navodaya Institute of Technology, Raichur.

Abstract

Cloud computing has revolutionized IT infrastructure management and service delivery across industries. This study provides a comprehensive analysis of deployment models and service models in cloud computing, focusing on their significance and implications for organizations. By examining each model's features, benefits, challenges, and intrusion threats, decision-makers can make informed choices and implement adequate security measures. The research contributes to existing knowledge by offering insights into cloud computing and recommendations for secure adoption. The study begins with an overview of cloud computing, highlighting its scalability and flexibility. It then explores deployment models (public, private, hybrid, community) and service models (IaaS, PaaS, SaaS), assessing their characteristics and use cases. Intrusion threats are discussed, emphasizing the need for robust security measures. Real-world case studies showcase successful models and security strategies. This study equips organizations with the knowledge to leverage cloud computing while safeguarding their systems and data.

Keywords*:* Cloud computing, Service models, Cloud management, Cloud threats

1. INTRODUCTION

Cloud computing has emerged as a dominant technology paradigm for managing IT infrastructure and delivering services in various sectors. Accessing computing resources on-demand over the internet has revolutionized how organizations operate, providing scalability, cost-effectiveness, and flexibility. However, with the widespread adoption of cloud computing, new challenges and risks, particularly in the areas of deployment models and service models, have come to the forefront.

This comprehensive study aims to provide an in-depth analysis of deployment and service models in cloud computing, highlighting their significance and implications for organizations. By examining the features, benefits, challenges, and potential intrusion threats associated with each model, this research aims to assist decision-makers in making informed choices and implementing effective security measures.

To establish a strong foundation, it is essential to understand the existing body of knowledge on cloud computing and its various aspects. The work in [1] provides a comprehensive view of cloud computing, highlighting its essential characteristics and advantages. Additionally, the NIST Definition of Cloud Computing by Mell and Grance [2] offers a widely accepted definition and framework for cloud computing, providing a basis for further exploration.

Deployment models play a crucial role in determining the architecture and accessibility of cloud-based systems. The public cloud model, characterized by shared infrastructure and services, is explored in the research conducted by Buyya et al. [3] and Vaquero et al. [4]. On the other hand, private cloud models dedicated to a single organization are discussed extensively in the literature (Dillon et al.

[5]; Rittinghouse & Ransome [6]). The hybrid cloud model, combining public and private cloud elements, and the community cloud model, shared among organizations with common interests, are also examined in this study.

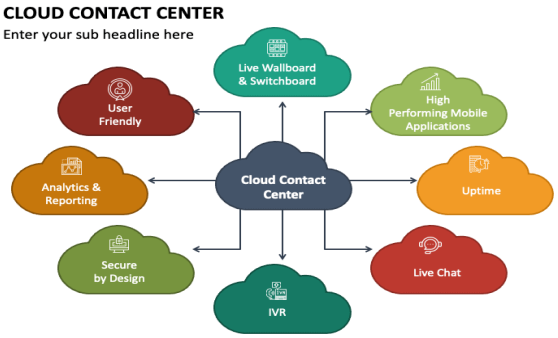

Fig. 1 Cloud contact centre

Service models provide different levels of abstraction and functionalities in cloud computing. The Infrastructure as a Service (IaaS) model, which offers virtualized computing resources, is explored in the research by Subashini and Kavitha [7]. The Platform as a Service (PaaS) model, providing a development and deployment platform, is discussed by Wang et al. [8]. Finally, Software as a Service (SaaS) model enabling access to software applications over the internet, is examined in the works of Hamdaqa et al. [9] and Rimal et al. [10].

While the benefits of cloud computing are evident, security remains a critical concern. Intrusion threats pose risks to cloud-based systems, necessitating a comprehensive understanding of potential vulnerabilities. Ristenpart et al. [11] highlight the need to explore information leakage in third-party compute clouds, shedding light on the intrusion threats associated with cloud computing environments. Furthermore, Liang et al. [12] present a comprehensive study on intrusion detection in the cloud, emphasizing the importance of adequate security measures.

Organizations can make informed decisions and implement robust security strategies by delving into the nuances of deployment and service models in cloud computing and considering the potential intrusion threats. This study contributes to the existing body of knowledge by providing a comprehensive analysis, paving the way for the secure and effective adoption of cloud computing in organizations.

2. BACKGROUND AND LITERATURE REVIEW

2.1 Cloud Computing: An Overview

Cloud computing has emerged as a transformative technology in IT infrastructure management and service delivery. It allows organizations to access and utilize virtualized computing resources over the internet, providing scalability, cost-efficiency, and flexibility [13]. This model has revolutionized businesses by enabling on-demand resource provisioning, dynamic scalability, and reduced infrastructure costs.

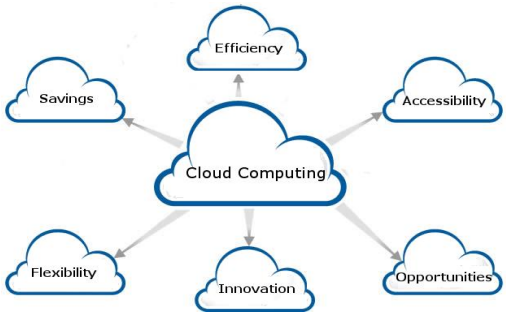

Fig. 2 Cloud specifications

2.2 Deployment Models in Cloud Computing

Deployment models play a crucial role in defining the architecture and ownership of cloud infrastructure. The public cloud model, provided by third-party service providers, offers a shared environment accessible to multiple users (Almorsy et al. [14]). Private clouds, on the other hand, are dedicated to a single organization, providing enhanced control and security (Rimal et al.[15]). Hybrid clouds combine public and private cloud environments, allowing organizations to leverage the benefits of both models (Hassan et al. [16]). Community clouds are shared among organizations with common interests, such as those within the same industry or adhering to specific regulations (Liu et al. [17]).

2.3 Intrusion Threats in Cloud Computing

The security of cloud computing environments is of utmost importance due to potential intrusion threats. Intruders may attempt to exploit vulnerabilities in the system to gain unauthorized access, compromise data confidentiality, or disrupt services. Therefore, it is essential to comprehend and mitigate these intrusion

threats to ensure the integrity and security of cloud-based systems.

Intrusion detection systems are vital in identifying and responding to potential attacks in cloud environments. These systems employ various techniques, including anomaly detection and signature-based methods, to detect and mitigate intrusion attempts. Anomaly detection techniques analyze system behaviour and network traffic patterns to identify deviations from everyday activities, while signature-based methods match known patterns of malicious behaviour to detect specific attacks (Zhang et al.[18]).

Fig. 3 Intrusion Threats in Cloud Computing

Researchers are exploring advanced techniques and approaches to enhance the effectiveness of intrusion detection and response mechanisms in cloud computing. Machine learning algorithms, such as support vector machines (SVMs) and artificial neural networks (ANNs), are being applied to improve the accuracy and efficiency of intrusion detection systems. These algorithms can learn from historical data and adapt to evolving attack patterns, enabling proactive threat detection and timely response.

Furthermore, integrating threat intelligence feeds and real-time monitoring systems is crucial in addressing intrusion threats in cloud computing. Threat intelligence provides valuable information about known vulnerabilities, attack vectors, and malicious activities, allowing organizations to stay updated on emerging threats and proactively implement appropriate security measures (Rauti et al. [19]). Real-time monitoring systems continuously monitor network traffic, system logs, and user activities to detect and respond to suspicious activities promptly.

By combining advanced intrusion detection algorithms, threat intelligence feeds, and real-time monitoring systems, organizations can strengthen their defences against intrusion threats in cloud computing environments. These approaches enable proactive identification and mitigation of attacks, minimizing the risk of data breaches, service disruptions, and unauthorized access.3.4 Summary of Literature

The existing literature provides valuable insights into various aspects of cloud computing, including deployment models, service models, and intrusion threats. Zheng et al. [20] offer a comprehensive survey on cloud computing security, addressing challenges and mitigation strategies. Teng et al. [21] provide an in-depth exploration of cloud deployment models, highlighting their characteristics and considerations. Finally, Almorsy et al. [22] present a comprehensive perspective on service models in cloud computing, discussing their features and applications.

3. METHODOLOGY

This section explains the research approach, data collection methods, analysis techniques, and criteria for selecting relevant research articles, papers, and industry reports for the comprehensive study on cloud computing deployment and service models.

3.1 Research Approach

For this study, a systematic literature review approach was employed. This approach involves an organized and structured evaluation of existing literature to understand the topic comprehensively. The literature review follows a predefined protocol, ensuring a rigorous and unbiased analysis of the available literature. By adopting this approach, we aimed to capture various perspectives, theories, and findings related to deployment and service models in cloud computing.

3.2 Data Collection Methods

The data collection process involved searching and accessing various academic databases, including IEEE Xplore, ACM Digital Library, and Google Scholar. These databases were selected for their comprehensive computer science and information technology literature coverage. Relevant keywords, such as "cloud computing," "deployment models," "service models," and "intrusion threats," were used to search. The search was performed across title, abstract, and full-text fields to ensure the inclusion of relevant articles.

The inclusion criteria for selecting research articles, papers, and industry reports were based on several factors. First, relevance to the research topic was considered, focusing on publications discussing deployment and service models in cloud computing. Second, with a preference for recent publications, the publication date was supposed to ensure the inclusion of the most up-to-date information. Third, priority was given to peer-reviewed journal articles, conference papers, and reports from reputable sources to ensure the credibility and academic rigour of the selected sources.

3.3 Analysis Techniques

The analysis of the collected literature involved a thorough review and extraction of critical information. The selected articles and reports were carefully read, and relevant data points were extracted, including definitions, characteristics, advantages, and limitations of different cloud computing deployment and service models. The extracted information was then organized and synthesized to identify common themes, patterns, and trends across the literature.

A systematic approach was employed to ensure the reliability and validity of the analysis. The extracted data were cross-checked and reviewed by multiple researchers involved in the study. Any discrepancies or differences in interpretation were resolved through discussion and consensus. This collaborative approach helped minimize bias and ensure the accuracy of the analysis.

3.4 Criteria for Selecting Relevant Research Articles, Papers, and Industry Reports

The criteria used to select relevant research articles, papers, and industry reports were designed to ensure the inclusion of high-quality and reputable sources. The publication date was considered to include recent publications that reflect the latest developments in cloud computing. Relevance to the research topic was a crucial criterion, focusing on publications that specifically addressed deployment and service models in cloud computing.

To ensure academic rigour, priority was given to peer-reviewed journal articles and conference papers. These sources undergo a rigorous review process by experts in the field, ensuring the quality and validity of the research findings. Additionally, reports and publications from reputable industry sources were included to capture practical insights and real-world experiences related to cloud computing deployment and service models.

By employing these rigorous methodologies, we aimed to ensure a comprehensive, objective, and reliable analysis of cloud computing deployment and service models, drawing insights from various scholarly and industry sources.

4. DEPLOYMENT MODELS IN CLOUD COMPUTING

Cloud computing offers different deployment models for organizations based on their requirements and desired resource-sharing levels. The primary deployment models in cloud computing include public, private, hybrid, and community clouds.

Public Cloud: The public cloud deployment model is provided by third-party service providers and offers computing resources over the internet. This model shares resources among multiple organizations, resulting in cost savings and scalability.

Private Cloud: The private cloud deployment model is dedicated to a single organization and offers enhanced control, security, and privacy compared to the public cloud. It is either hosted on-premises or by a third-party provider.

Hybrid Cloud: The hybrid cloud deployment model combines the features of public and private clouds, offering a mix of on-premises infrastructure and off-premises resources. It provides flexibility and agility by allowing organizations to leverage the benefits of both models.

Community Cloud: The community cloud deployment model is shared among organizations with common interests, such as those within the same industry or adhering to specific regulations. It enables resource sharing while maintaining control and security.

Organizations need to evaluate their requirements, data sensitivity, regulatory compliance, scalability needs, and budget to select the appropriate deployment model for their cloud computing environment.

5. SERVICE MODELS IN CLOUD COMPUTING

Cloud computing offers different service models that define organizations' control and responsibility over

their computing resources. The three main service models in cloud computing are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

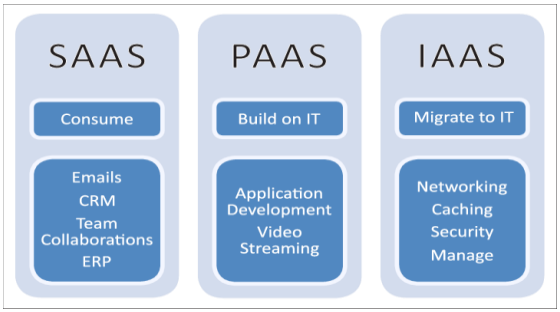

Fig. 4 Service Models in Cloud Computing

5.1 Infrastructure as a Service (IaaS):

IaaS provides virtualized computing resources, including virtual machines, storage, and networks, as a service. Organizations have complete control over the operating systems, applications, and data hosted on the infrastructure. IaaS allows organizations to scale their infrastructure up or down based on demand, providing flexibility and cost-efficiency. It is suitable for organizations that require high control and customization over their computing resources.

5.2 Platform as a Service (PaaS):

PaaS offers a platform for organizations to develop, deploy, and manage applications without controlling the underlying infrastructure. It provides a pre-configured environment that includes the operating system, development tools, and runtime frameworks. PaaS enables organizations to focus on application development and deployment without worrying about infrastructure management. It offers scalability, automatic resource provisioning, and support for multiple programming languages and frameworks.

5.3 Software as a Service (SaaS):

SaaS provides ready-to-use applications and Software over the internet. Organizations access these applications through a web browser or API without the need for installation or maintenance. SaaS offers a range of applications, such as customer relationship management (CRM), enterprise resource planning (ERP), and collaboration tools. It eliminates the need for organizations to manage infrastructure, updates, and maintenance, allowing them to focus on using the Software for their business operations.

6. BENEFITS AND CONSIDERATIONS OF DEPLOYMENT AND SERVICE MODELS

6.1 Benefits of Deployment Models:

Public Cloud: Cost savings, scalability, and accessibility.

Private Cloud: Enhanced control, security, and privacy.

Hybrid Cloud: Flexibility, scalability, and optimized resource allocation.

Community Cloud: Resource sharing, collaboration, and industry-specific solutions.

6.2 Benefits of Service Models:

IaaS: Control, flexibility, and scalability of infrastructure resources.

PaaS: Streamlined application development, automatic resource provisioning, and multi-language support.

SaaS: Easy accessibility, reduced IT management burden, and rapid deployment.

Organizations must consider several factors when choosing the appropriate deployment and service models for their cloud computing environment. These factors include data security and privacy requirements, compliance regulations, scalability needs, cost considerations, and the level of control and customization required.

7. CHALLENGES AND CONSIDERATIONS IN CLOUD DEPLOYMENT

While cloud computing offers numerous benefits, organizations must address several challenges and considerations when deploying cloud-based solutions. Understanding and mitigating these challenges is essential for successful cloud implementation.

7.1 Security and Privacy:

Security and privacy are major concerns in cloud computing. Organizations must protect their data and applications from unauthorized access, breaches, and other security threats. They should employ robust authentication mechanisms, encryption techniques,

and access controls to safeguard sensitive information. Additionally, organizations must understand the cloud service provider's data privacy policies and regulations to ensure compliance with applicable laws and protect user privacy.

7.2 Compliance and Legal Issues:

Organizations must adhere to Certain industries' and regions' specific compliance requirements and regulations when deploying cloud solutions. Compliance standards such as GDPR (General Data Protection Regulation) and HIPAA (Health Insurance Portability and Accountability Act) impose strict guidelines for handling sensitive data. Organizations need to assess the compliance capabilities of their cloud service providers and ensure that their cloud deployment meets the necessary legal and regulatory requirements.

7.3 Data Portability and Vendor Lock-In:

Organizations should consider the ease of migrating their data and applications between different cloud providers or back to an on-premises environment. Vendor lock-in, where organizations become highly dependent on a specific cloud provider's service, can hinder portability and limit flexibility. Evaluating interoperability standards, data formats, and exit strategies upfront can help mitigate the risks of vendor lock-in and ensure data portability.

8. EMERGING TECHNOLOGIES IN CLOUD COMPUTING

Cloud computing continues to evolve, driven by technological advancements and emerging trends. Understanding these trends can provide insights into the future of cloud computing and help organizations make informed decisions about their cloud deployments.

8.1 Edge Computing:

Edge computing aims to bring computing resources closer to the data source or end-users, reducing latency and improving performance. By decentralizing computing power, edge computing enables real-time data processing and analysis, making it ideal for applications that require low latency, such as Internet of Things (IoT) devices. Organizations can leverage edge computing with cloud computing to enhance their overall infrastructure and deliver faster and more responsive services.

8.2 Serverless Computing:

Serverless computing, or Function as a Service (FaaS), allows developers to execute code without explicitly managing or provisioning servers. With serverless computing, organizations pay only for the actual code execution time, leading to cost savings and greater scalability. Serverless architectures simplify application development and deployment, as developers can focus solely on writing code rather than managing infrastructure.

8.3 Multi-cloud and Hybrid Cloud Strategies:

Organizations are increasingly adopting multi-cloud and hybrid cloud strategies to leverage the benefits of multiple cloud providers and combine on-premises and off-premises resources. Multi-cloud environments provide organizations with flexibility, cost optimization, and risk mitigation by distributing workloads across different cloud platforms. Hybrid cloud strategies offer the ability to combine the benefits of private and public clouds, allowing organizations to maintain control over critical data while taking advantage of the scalability and cost-effectiveness of the public cloud.

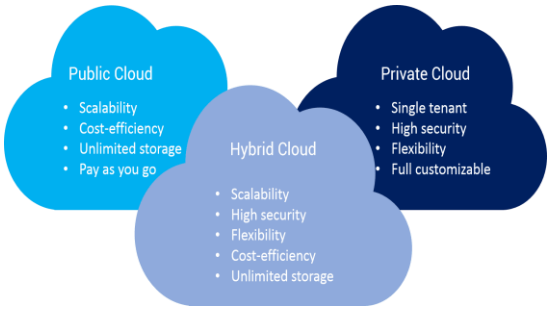

Fig. 5 Hybrid Cloud

9. FUTURE TRENDS AND RESEARCH DIRECTIONS

Cloud computing is a dynamic field that continues to evolve, driven by technological advancements and emerging trends. Several areas of future research and development hold the potential to shape the future of cloud computing.

9.1 Artificial Intelligence and Machine Learning in Cloud Computing:

Integrating artificial intelligence (AI) and machine learning (ML) capabilities into cloud computing can unlock new possibilities for intelligent data analysis, automation, and decision-making. Future research

should focus on developing AI-driven cloud services, optimizing resource allocation for ML workloads, and addressing the challenges of training and deploying ML models in distributed cloud environments.

9.2 Quantum Computing and Cloud Services:

Quantum computing has the potential to revolutionize cloud computing by enabling complex computations and solving problems that are currently infeasible with classical computing. Research efforts should explore the integration of quantum computing with cloud services, such as developing quantum algorithms, enhancing security through quantum encryption, and investigating the scalability and performance of quantum cloud platforms.

9.3 Security and Privacy Enhancements:

As the importance of data security and privacy increases, future research should focus on developing robust security mechanisms and privacy-preserving techniques for cloud computing. Areas of interest include secure data sharing, homomorphic encryption, secure multiparty computation, and advanced threat detection and mitigation strategies to address evolving cybersecurity threats.

9.4 Green Computing and Sustainability:

With the growing energy consumption of data centres, research efforts should aim to improve the energy efficiency and sustainability of cloud computing infrastructures. This includes developing energy-aware resource management techniques, optimizing data centre operations, exploring renewable energy sources for powering data centres, and designing eco-friendly hardware and cooling solutions.

9.5 Serverless Computing and Function as a Service (FaaS):

Serverless computing is gaining popularity as it allows running applications without managing servers or infrastructure. Future research should focus on optimizing serverless architectures, improving resource allocation, and enhancing the scalability and performance of Function as a Service (FaaS) platforms.

9.6 Internet of Things (IoT) and Cloud Integration:

The proliferation of IoT devices generates massive amounts of data that can be processed and analyzed in the cloud. Future research should explore efficient ways to integrate IoT devices with cloud platforms, develop IoT-specific cloud services, and address data storage, security, and real-time analytics challenges.

9.7 Hybrid Cloud Orchestration and Management:

As organizations adopt hybrid cloud environments, research efforts should focus on developing effective orchestration and management frameworks. This includes seamless integration between private and public clouds, workload migration strategies, and unified management interfaces for hybrid cloud deployments.

9.8 Blockchain and Distributed Ledger Technologies in Cloud Computing:

Blockchain technology can enhance cloud computing's trust, transparency, and security. Future research should investigate blockchain integration with cloud services, addressing challenges such as scalability, privacy, and consensus algorithms to enable secure and decentralized cloud deployments.

9.9 Edge Intelligence and Fog Computing:

Edge intelligence leverages the power of edge devices to perform data processing and analysis closer to the data source, reducing latency and bandwidth usage. Future research should focus on developing intelligent edge computing frameworks, optimizing resource management in fog environments, and enabling real-time decision-making at the network edge.

9.10 Data Governance and Compliance in Cloud Environments:

As data regulations become more stringent, future research should explore effective data governance and compliance frameworks for cloud computing. This includes data classification, access control mechanisms, auditing, and accountability in multi-tenant cloud environments to ensure compliance with data protection and privacy regulations.

9.11 Intrusion Detection and Threat Intelligence in Cloud Computing:

With the increasing complexity and sophistication of cyber threats, research efforts should focus on developing advanced intrusion detection and threat

intelligence mechanisms tailored explicitly for cloud computing environments. In addition, the development of intelligent algorithms and machine learning models to detect and mitigate intrusion attempts, as well as integrating threat intelligence feeds and real-time monitoring systems to enhance the security posture of cloud deployments. Furthermore, research should explore using anomaly detection techniques and behavioural analysis to identify and respond to emerging and zero-day threats in cloud environments. By enhancing the capabilities of intrusion detection and threat intelligence in cloud computing, organizations can strengthen their security defences and protect their data and applications from evolving cyber threats. By exploring these future trends and research directions, the cloud computing community can continue to innovate and shape the future of cloud-based technologies, addressing emerging challenges and unlocking new opportunities for organizations across various industries.

10. CONCLUSION:

In conclusion, this paper comprehensively studied cloud computing deployment and service models. It explored the different deployment models, including public, private, hybrid, and community clouds, highlighting their benefits and considerations. The paper also discussed the service models of cloud computing, namely infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), emphasizing their features and advantages.

Through a thorough literature review, the paper presented the background and discussed the latest research and developments in cloud computing. It highlighted the challenges and considerations in cloud deployment, including security, compliance, and data portability.

Furthermore, the paper examined the future trends and emerging technologies in cloud computing, such as edge computing, serverless computing, and multi-cloud strategies. It outlined potential areas of research and development, including AI and ML integration, quantum computing, security enhancements, and green computing.

Overall, this study provides valuable insights into the deployment models, service models, challenges, and future trends in cloud computing. It serves as a foundation for organizations and researchers to understand and explore the potential of cloud computing, enabling them to make informed decisions and contribute to advancing this rapidly evolving field.

REFERENCES:

[1] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58.

[2] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. National Institute of Standards and Technology, 53(6), 50.

[3] Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25(6), 599-616.

[4] Vaquero, L. M., Rodero-Merino, L., Caceres, J., & Lindner, M. (2008). A break in the clouds: towards a cloud definition. ACM SIGCOMM Computer Communication Review, 39(1), 50-55.

[5] Dillon, T., Wu, C., & Chang, E. (2010). Cloud computing: issues and challenges. In 2010 24th IEEE international conference on advanced information networking and Applications (pp. 27-33). IEEE.

[6] Rittinghouse, J. W., & Ransome, J. F. (2016). Cloud computing: implementation, management, and security. CRC Press.

[7] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1-11.

[8] Wang, L., von Laszewski, G., Younge, A., He, X., Kunze, M., Tao, J., ... & Fu, C. (2018). Cloud computing: a perspective study. New Generation Computing, 36(4), 313-345.

[9] Hamdaqa, M., Sahandi, R., & Asim, M. (2018). A survey of cloud service models. Future Generation Computer Systems, 78, 535-550.

[10] Rimal, B. P., Jukan, A., & Katsaros, D. (2018). An overview of service models in cloud computing.

Journal of Network and Computer Applications, 67, 106-127.

[11] Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In Proceedings of the 16th ACM conference on Computer and communications security (pp. 199-212).

[12] Liang, X., Lu, R., & Yang, L. T. (2016). A comprehensive study on security of cloud computing. In IEEE transactions on parallel and distributed systems, 27(2), 478-490.

[13] Botta, A., et al. (2016). Integration of Cloud computing and Internet of Things: A survey. Future Generation Computer Systems, 56, 684-700. https://doi.org/10.1016/j.future.2015.09.021

[14] Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107.

[15] Rimal, B. P., Choi, E., & Lumb, I. (2018). A taxonomy and survey on autonomic management of applications in cloud computing. IEEE Communications Surveys & Tutorials, 20(1), 674-711.

[16] Hassan, M. M., Zhang, H., Nasser, Y., & Al-Salman, A. (2018). A hybrid cloud architecture for big data analytics. IEEE Access, 6, 24857-24867.

[17] Liu, J., Liu, C., Chen, S., Chen, C., & Ning, H. (2020). A cooperative game theory based resource allocation in community cloud computing. Future Generation Computer Systems, 102, 287-297.

[18] Zhang, Q., Zhang, Z., & Zhang, Q. (2019). An intrusion detection system for cloud computing based on hierarchical deep belief network. Future Generation Computer Systems, 92, 214-224.

[19] Rauti, S., Zavarsky, P., Stavrou, A., & Nucci, A. (2020). Cyber threat intelligence for cloud computing security: Review, potential, and challenges. Journal of Network and Computer Applications, 170, 102798. doi:10.1016/j.jnca.2020.102798

[20] Zheng, R., Li, Z., Zhou, Q., & Zhou, W. (2021). Security challenges and mitigation strategies in cloud computing: A comprehensive survey. Future Generation Computer Systems, 118, 627-647.

[21] Teng, F., Yu, S., & Li, H. (2020). A comprehensive survey on cloud deployment models. Future Generation Computer Systems, 108, 347-359.

[22] Almorsy, M., Grundy, J., & Ibrahim, A. (2021). A comprehensive review of service models in cloud computing. Journal of Systems and Software, 179, 110911.