International Journal of Applied Data Science
Volume1, Issue1, 2025

New Developments in Cloud Computing: A Thorough Examination of Service and Deployment Models for Security, Flexibility, and Scalability.

Jehau A.H Hammad[1]
[1]Department of Computer Information Systems Al-Quds Open University, Palestine

Article Info

Received: 30-04-2025 ***Revised:08-05-2025*** ***Accepted:19-05-2025*** ***Published:29-05-2025***

Abstract

Across many sectors, cloud computing has transformed service delivery and IT infrastructure management. With an emphasis on their importance and ramifications for businesses, this paper offers a thorough examination of cloud computing deployment and service models. Decision-makers may make well-informed decisions and put in place suitable security measures by looking at each model's characteristics, advantages, difficulties, and intrusion risks. By providing insights into cloud computing and suggestions for safe usage, the study advances current understanding. An introduction to cloud computing that emphasizes its scalability and flexibility opens the subject. After that, it examines and evaluates the features and applications of the service models (IaaS, PaaS, and SaaS) and deployment methods (public, private, hybrid, and community). The need of strong security measures is emphasized in the discussion of intrusion risks. Successful models and security techniques are shown via real-world case studies. This report gives businesses the information they need to use cloud computing while protecting their data and infrastructure.

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

1. INTRODUCTION

One of the most popular technological paradigms for managing IT infrastructure and providing services across a range of industries is cloud computing. On-demand access to computer resources over the internet has completely changed how businesses function by offering flexibility, scalability, and cost-effectiveness. But as cloud computing has been more widely used, new dangers and concerns have emerged, especially with regard to deployment and service models.
The goal of this extensive research is to provide a thorough examination of cloud computing deployment and service models, emphasizing their importance and organizational ramifications. This study attempts to help decision-makers make wise decisions and put in place efficient security measures by looking at the characteristics, advantages, difficulties, and possible intrusion risks connected to each model.Understanding the collection of information currently available on cloud computing and its many facets is crucial to building a solid foundation. The paper in [1] offers a thorough analysis of cloud computing, emphasizing its key features and benefits. Furthermore, a well recognized concept and framework for cloud computing are provided by Mell and Grance's NIST concept of Cloud Computing [2], which serves as a foundation for further research.

The design and usability of cloud-based systems are largely determined by deployment strategies. The shared infrastructure and services that define the public cloud concept include examined in the studies carried out by Vaquero et al. [4] and Buyya et al. [3]. However, there is a lot of work on private cloud models that are exclusive to one company (Dillon et al. [5]; Rittinghouse & Ransome [6]). This research also looks at the community cloud model, which is shared by companies with similar goals, and the hybrid cloud model, which combines public and private cloud components.

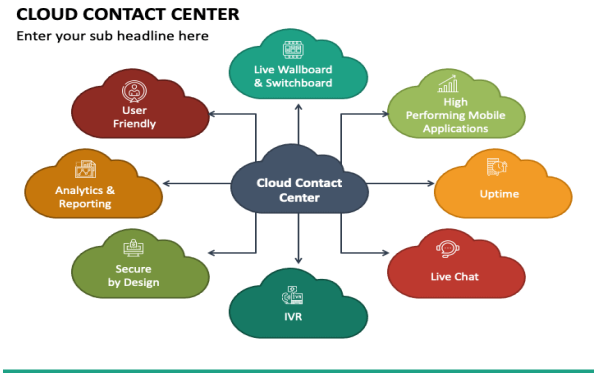


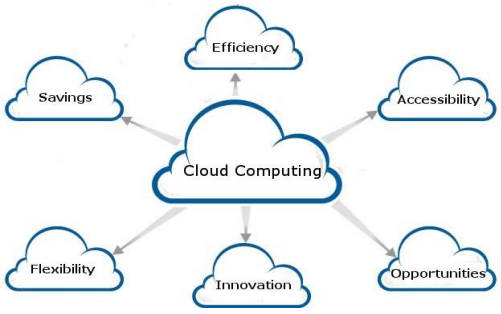
Fig. 1 Cloud contact centre

In cloud computing, service models provide varying degrees of abstraction and functionality. Subashini and Kavitha's study examines the Infrastructure as a Service (IaaS) concept, which provides virtualized computing resources [7]. Wang et al. [8] address the Platform as a Service (PaaS) paradigm, which offers a platform for development and deployment. Lastly, the studies of Hamdaqa et al. [9] and Rimal et al. [10] analyze the Software as a Service (SaaS) paradigm, which makes software programs accessible online.Even though cloud computing has many advantages, security is still a major worry. Cloud-based systems are at danger from intrusion threats, thus a thorough grasp of possible weaknesses is necessary. In order to shed light on the infiltration dangers related to cloud computing environments, Ristenpart et al. [11] emphasize the need of investigating information leakage in third-party compute clouds. Additionally, a thorough research on cloud intrusion detection is presented by Liang et al. [12], highlighting the need of appropriate security measures.
By exploring the subtleties of cloud computing deployment and service models and taking into account the possible risks, organizations can make well-informed choices and put strong security measures into place. dangers of intrusion. By offering a thorough analysis, this research adds to the body of information already in existence and opens the door for enterprises to safely and successfully use cloud computing.

3. BACKGROUND AND LITERATURE REVIEW

3.1 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

3.2 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]).

3.3 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.

4. 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.

4.1 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.

4.2 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.

4.3 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.

4.4 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.

5. 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.

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).

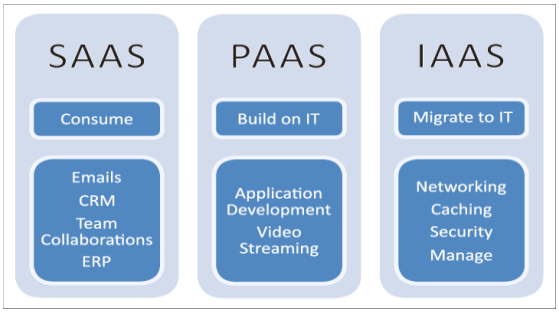


Fig. 4 Service Models in Cloud Computing

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.

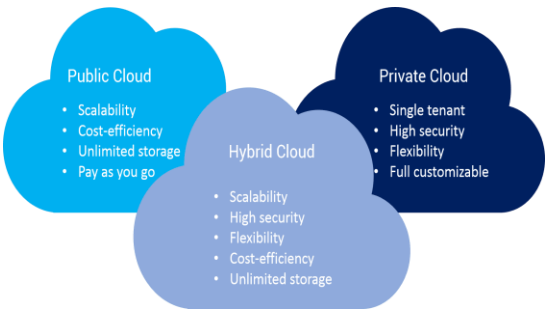


Fig. 5 Hybrid Cloud

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:

11. In summary, the deployment and service models of cloud computing were thoroughly examined in this research. It examined the various deployment models—public, private, hybrid, and community clouds—highlighting the advantages and factors to take into account. The cloud computing service models—Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)—were also covered in the paper, with an emphasis on their benefits. The study provided background information and analyzed the most recent advancements in cloud computing via a comprehensive literature analysis. It emphasized the difficulties and factors to be taken into account while using cloud computing, such as data portability, security, and compliance. Additionally, the study looked at new developments in cloud computing, including serverless computing, edge computing, and multi-cloud tactics. It included many possible research and development topics, such as green computing, quantum computing, security improvements, and the integration of AI and ML. All things considered, this research offers insightful information on cloud computing deployment patterns, service models, obstacles, and upcoming trends. It provides a framework for scholars and businesses to comprehend and investigate the possibilities of cloud computing, empowering them to make well-informed choices and further this quickly developing subject.

REFERENCES:

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

[2] Grance, T., and Mell, P. (2011). Cloud computing according to NIST. 53(6), 50; National Institute of Standards and Technology. [3] Buyya, R., Yeo, C. S., Broberg, J., Venugopal, S., & Brandic, I. (2009). Vision, hype, and reality for providing computing as the fifth utility: cloud computing and new IT platforms. Computer Systems of the Future, 25(6), 599-616.

[4] Lindner, M., Caceres, J., Rodero-Merino, L., and Vaquero, L. M. (2008). A cloud break: moving in the direction of a cloud definition. 39(1), 50-55; ACM SIGCOMM Computer Communication Review. [5] Chang, E., Wu, C., and Dillon, T. (2010). Cloud computing: problems and difficulties. 24th IEEE International Conference on Advanced Information Networking and Applications, 2010 (pp. 27–33). IEEE. [6] Ransome, J. F., and J. W. Rittinghouse (2016). Cloud computing: setup, administration, and safety. CRC Publishing. [7] Kavitha, V., and S. Subashini (2011). An analysis of security concerns in cloud computing service delivery architectures. Network and Computer Applications Journal, 34(1), 1–11. [8] Wang, L., von Laszewski, G., Younge, A., He, X., Kunze, M., Tao, J., ... & Fu, C. (2018). A research from a standpoint on cloud computing. 36(4), 313-345; New Generation Computing. [9] Asim, M., Hamdaqa, M., and Sahandi, R. (2018). An overview of cloud service models. Computer Systems of the Future, 78, 535-550. [10] Rimal, B. P., Katsaros, D., and Jukan, A. (2018). An outline of cloud computing service models. Network and Computer Applications Journal, 67, 106-127.

[2] [11] Savage, S., Shacham, H., Tromer, E., and Rensenpart, T. (2009). Investigating information leaks in third-party compute clouds: "Hey, you, get off my cloud." 199–212 in the Proceedings of the 16th ACM Conference on Computer and Communications Security.

[12] Yang, L. T., Liang, X., and Lu, R. (2016). a thorough analysis of cloud computing security. IEEE Transactions on Distributed and Parallel Systems, 27(2), 478-490.

[3] [13] A. Botta and colleagues (2016). A survey on the integration of cloud computing with the Internet of Things. Computer Systems of the Future, 56, 684-700. ttps://doi.org/10.1016/j.future.2015.09.021

[14] Grundy, J., Müller, I., and Almorsy, M. (2016). An examination of the security issue with cloud computing. arXiv preprint arXiv:1609.01107.

[4] [15] Lumb, I., Choi, E., and Rimal, B. P. (2018). A classification and overview of cloud computing applications' autonomous management. 674–711 in IEEE Communications Surveys & Tutorials, 20(1).

[5] [16] Hassan, M. M., Al-Salman, A., Zhang, H., and Nasser, Y. (2018). Big data analytics using a hybrid cloud architecture. IEEE Access, 6, 24857-24867.

[6] [17] Liu, J., Liu, C., Chen, S., Chen, C., & Ning, H. (2020). Resource allocation in community cloud computing based on cooperative game theory. Computer Systems of the Future, 102, 287-297.

[7] [18] Zhang, Q., Zhang, Z., and Zhang, Q. (2019). A hierarchical deep belief network-based intrusion detection solution for cloud computing. Computer Systems of the Future, 92, 214–224.

[19] In 2020, Rauti, S., Stavrou, A., Zavarsky, P., and Nucci, A. Review, possibilities, and problems of cyber threat intelligence for cloud computing security. Network and Computer Applications Journal, 170, 102798. 10.1016/j.jnca.2020.102798

[8] [20] Zheng, R., Zhou, Q., Zhou, W., & Li, Z. (2021). A thorough examination of cloud computing security issues and solutions. Computer Systems of the Future, 118, 627-647.

[21] Teng, F., Li, H., and Yu, S. (2020). An extensive analysis of cloud deployment methods. Computer Systems of the Future, 108, 347-359. [22] Ibrahim, A., Grundy, J., and Almarsy, M. (2021). An extensive analysis of cloud computing service models. Systems and Software Journal, 179, 11