International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/



(REVIEW ARTICLE)

Check for updates

CLOUD COMPUTING SECURITY MODELS GUARANTEE: A SYSTEMATIC REVIEW

George Elechi Christopher [1,*], Frank Ekene Ozioko [2] and Nnali Gabriel Nwachi [1]

[1] Computer Science Department, Akanu Ibiam Federal Polytechnic, Unwana. Ebonyi, Nigeria.
[2] Computer Science Department, Enugu State University of Science and Technology, Nigeria.

ORCID Details
George Elechi Christopher: https://orcid.org/0009-0007-1081-869x
Frank Ekene Ozioko: https://orcid.org/0000-0001-7092-6261

International Journal of Science and Research Archive, 2026, 21(02), 235–244

Publication history: Received on 27 September 2026; revised on 05 November 2026; accepted on 07 November 2026

Article DOI: https://doi.org/10.30574/ijsra.2026.21.2.1981

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0

ABSTRACT

Security in mobile and cloud computing is critical due to the high volume of sensitive data, remote access, and evolving cyber threats. Both domains require layered defenses, proactive monitoring, and regulatory compliance to ensure confidentiality, integrity, and availability. Cloud Computing Security: Cloud security involves protecting cloud infrastructure, applications, and data from threats like data breaches, DDoS attacks, insider threats, and misconfigurations. It uses the internet network for data distribution and operates on a shared responsibility model—the cloud provider secures the infrastructure, while customers secure their data, applications, and configurations. The back-end of the cloud network gives users access to resources such as Infrastructure as a Service (IaaS), Software as a Service (SaaS), Desktop as a Service (DaaS), Platform as a Service (PaaS), etc. It uses several security models, and yet it encounters serious data breaches, particularly in public cloud computing. Owing to this, the authors researched various cloud computing security models to ascertain the best model for the cloud computing system. The Systematic literature review methodology adopted the Kitchenham method. The literature was searched across leading academic databases. To ascertain the best quality, various cloud computing security models were analysed using a thematic analysis approach for identification, analysis, and reporting patterns for collated data. However, the finding shows that the RSA security model is not the only asymmetric security model. Meanwhile, it is the most concise with a simple arithmetic method, and the easiest to code. So, the review indicated RSA as the best cloud computing security model, but it needed an upgrade to accommodate primary key regularly updating to avoid data redundancy.

Keywords: Cloud Security Models; Asymmetric Algorithm; Kitchenham Method; Thematic Analysis; Network Security; RSA Model;

1 INTRODUCTION

Initially, computers were internally networked to enable internal data communication, and later, the technology gave birth to LAN and further to the global network, which is the Internet. In the same line, the virtualisation of the internet gave birth to cloud computing. So, cloud computing is a moving trend that satisfies users' IT services like infrastructure, software, platforms, and related computing services. However, the charges are minimal, and users pay for the service as

they used [1]. Also, a cloud is an IT infrastructure designed to enable distant access to services and scalable resources. It is designed for the customers to benefit from secure, adaptable, and scalable services. However, the internet service is the transport medium for cloud computing [1].

Cloud and network security are the setup rules, configuration and protocol to safeguard the integrity, confidentiality and accessibility of computer networks and data [3]. According to [4], Privacy is the right of an individual to control or influence what information can be collected and stored and by whom and to whom that information may be disclosed. In Europe, privacy is viewed as a human right, whereas in the United States, it has generally meant preventing harm to people in any circumstance. Thus, cloud computing network models lack user control. That is, the users and even the service providers may not ascertain the security capability of the system because they are not in control nor the owners of the infrastructure. The deployment requires STEM (Science, Technology, Engineering and Mathematics) experts. Also, adhering to all of the norms and regulations in various parts of the world is difficult. Although cloud computing encompasses many service-level agreements (SLA) with international standard internet protocols. Yet, user data security is not assured because of wireless transmission media [5].

Meanwhile, three basic security models serve as the foundation of the security model. These are: Bell-Lapadula, Biba model and Clerk-Wilson model. After these, the Brewer and Nash model and the Harrison, Ruzzo, and Ullman model emerge. So, the exploration of cloud technology to meet the global needs led to more network security innovations. These are: DES, RSA, Diffie-Hellman, Rail-fence and Playfair cypher model. However, to really assess the highest quality among the models, most of the network security models will be surveyed and analysed properly to ascertain the result.

1.1 Background and Motivation

The Scalability and multitenant network nature of a cloud made it a favourable internet business. This settles user service instantly anywhere you go, and you pay as you use. Likewise, every happening and busy business attracts thieves, which is the reason cloud computing is tampering with and requires adequate security. Meanwhile, there are many cloud security models. Yet, none is efficient in curbing cloud data breaches. This has led to the Zero Trust Cloud Security model. However, this model requires expensive infrastructure and STEM experts to achieve the system. In fact, the public, hybrid and multi-cloud computing are vulnerable to data breaches because of their distributive channels. However, asymmetric security algorithms use primary and secondary keys, such as the RSA security model, which is a popular security algorithm that enables an asymmetric pattern of keys for data security.

1.2 Research Objectives:

- Appraise cloud computing security model to ascertain need.
- Surveying the network models to gather information
- The gathered data will be critically analysed in (CLR) and a thematic analysis approach.
- Conduct a Comparative study of the results to ascertain the most efficient for cloud computing.

2 REVIEW OF THE RELATED LITERATURE

This research work focused on cloud network security models' challenges. The author deems it necessary to explore data and analyse it to forecast information that will be beneficial for interested cloud users and providers, to avoid wasting precious time surfing the internet for information that may not be accurate. Because of this, the companies and the resource utilisation were reviewed for appropriate results [6]. Moreover, cloud computing started as far back as 1961 with John McCarthy. This great computer scientist tagged it under utility computing. Likewise, that of the telephone and electricity system is a public utility. So, a computer utility can be organised as a public utility for consumers. Moreover, infrastructure, internet, virtualisation, utility computing, distributed computing, and software are the basic criteria for cloud computing [2]. However, reviewing the existing literature, the research fails to consider current trends and fails to treat the major cloud computing challenges, which are of vital concern to cloud users. However, this work has to be reviewed because it lacks coverage of hacking the distributed system and the security of user data. This may be an oversight because of the author's personal area of interest. So, the literature was reviewed to accommodate the research update and increment.

2.1 An Overview of Current Techniques in Securing Cloud Computing Environments

Because the cloud is highly scalable and cost-efficient has contributed positively to the organisation's pattern of managing data and applications. Nevertheless, the widespread adoption of cloud services poses significant security challenges in the face of emerging threats, complexities of shared responsibility, and compliance (Wagas, 2024). The research considers current trends in cloud security, from adopting Zero Trust architecture to integrating artificial intelligence and machine learning for advanced threat detection. The study discusses the essential techniques, such as encryption, access controls, and cloud-related standards, which were considered to address vulnerabilities and shield multi-tenant environments. Three tasks were focused on: a multi-layered approach to security, proper responsibility demarcation, and technological

advancement. However, the author pinpoints further research areas, especially in adversarial attacks and defining robust security for hybrid and multi-cloud configurations. Also, to improve collaboration among stakeholders, along with investment in privacy-preserving technologies [7]. In line with the Zero Trust Security Model, [8]. The implementation of this model to achieve the user's aim may pose a challenge because of manpower, infrastructure and experienced expert coders. In line with this, [9] forecasted the cloud computing security in 2026. States that:

Table 1: Metric and value. Adopted from https://www.codebridge.tech/articles/cloud-computing-security-expert-insigh

Metric	Value
Average cloud breach cost	$4.5 million
Percentage of incidents due to misconfiguration	30 percent
Increase in API-based attacks (2024–2025)	45 percent year-over-year

"AI monitoring isn't magic Everyone's talking about AI-powered security monitoring, and yes, it can help spot weird behavior in your systems. But here's the thing – it's not plug-and-play. You'll spend weeks training it on your specific logs and adjusting thresholds to cut down on false alarms. "Don't expect it to work perfectly out of the box." Moreover, [10] review that multi-cloud environments bring immense flexibility, but they also introduce complex security challenges. The Table 2.1: Metric and value study, explores through a real-world inspired of a tech company navigating multi-cloud security in 2025–2026 and see how organizations are trying to address these challenges. Also, this Table 2.1 shows the current result of cloud data breaches.



Figure 1: Adopted from https://medium.com/@thinuridulsini/cloud-security-challenges-in-a-multi-cloud-world-2026-41de572dec44

AWS runs a multi-cloud setup; their customer application is on AWS, data analytics on Google Cloud, and backups on Azure. They embraced multi-cloud for resilience and flexibility. Meanwhile, each cloud has its own security model, Identity and Access Management (IAM) system, logging format, and quirks. However, juggling multiple tools can dilute focus and create gaps. The survey found a strong desire for a single unified security dashboard, with a majority of organisations agreeing it would be "moderately to extremely helpful" to manage all clouds together [10]. Hybrid and multi-cloud environments require more sophisticated security and improved collaboration among stakeholders. Also, invest in privacy-preserving technology. However, this area of study requires further research on cloud data security [5].

In fact, [11] review the cloud security model to identify critical security issues, implement technical solutions, and investigate challenges. The study uses a systematic literature review methodology, adopting the Kitchenham method. The data used was adopted from a literature search across leading academic databases. The findings of the review strongly recommend further study on the security of a multi-cloud environment. Figure 2.1 shows the different types of cloud threats and confirmed cloud data breaches. However, inferring from literature from 2024 to early 2026, cloud security models are shifting from perimeter-based defences to proactive, identity-centric, and AI-driven frameworks [12]. Table 2.2 was used to tabulate categories of currently cited literature.

Table 2: Categories of Cited Literature

SN	Authors	Year	Technology/Method	Achievement	Deficiency
1	Rasha et al.	2023	Cloud architecture	Architecture for deployment	Deployed through the internet
2	Rashi et at. Rasha et al.	2021 2023	Data confidentiality and security	Four-Level-Cloud-Based Application	Support myriad diseases in the health cloud Only
3	Gorelik	2023	Taxonomy comprises cloud services and deployment models	Survey data collected from Amazon Web Services (AWS).	It will affect the demand for IaaS in future
4	Wagas Godwin and Rahman	2024 2024	Zero Trust Architecture	Zero Trust Cloud Security Model	High cost of Infrastructure and experts
5	Sentinel	2025	Cloud data issues	Review of cloud network model	Requires more research
6	Amit and Sajad	2025	Multiple Tenancy Model	Virtual partitions of every tenant's data	It slows down the physical server
7	Manuel	2023	Novel Trust Security Model (NTSM)	Service level agreement for the cloud provider and the user's requirements	Not popular in commercial cloud, and not open source
8	Zhihu.com Kinza	2025 2025	DES, Diffie-Hellman, Rail-Fence, Playfair cypher, and RSA models	Modern cloud network models	RSA is the common asymmetric cypher model
9	Jerry	2025	Cloud security model	Asymmetric algorithm	Key redundancy
10	Myroslav	2025	Forecasting tools	Forecast Cloud Security for 2026	Requires more security research
11	Wichramarachchi	2026	Multi-cloud Pup up Security Alat	Distributive Security	Different security platforms for each cloud

2.2 Research Gap

So, the exploration of cloud network security models to meet the global needs led to more network security innovations such as: DES, RSA, Diffie-Hellman, Rail-fence, Playfair cypher and zero trust model. The RSA is the common one that uses an asymmetric algorithm, which uses one key for encryption and the other key for decryption.

3 CLOUD COMPUTING AND THE INTERNET

The internet is the backbone of the cloud. Meanwhile, hybrid, public and multi-cloud computing use the internet channel for data communication. The hypervisor serves as a virtual machine

3. Cloud Computing and the Internet

The internet is the backbone of the cloud. Meanwhile, hybrid, public and multi-cloud computing use the internet channel for data communication. The hypervisor serves as a virtual machine

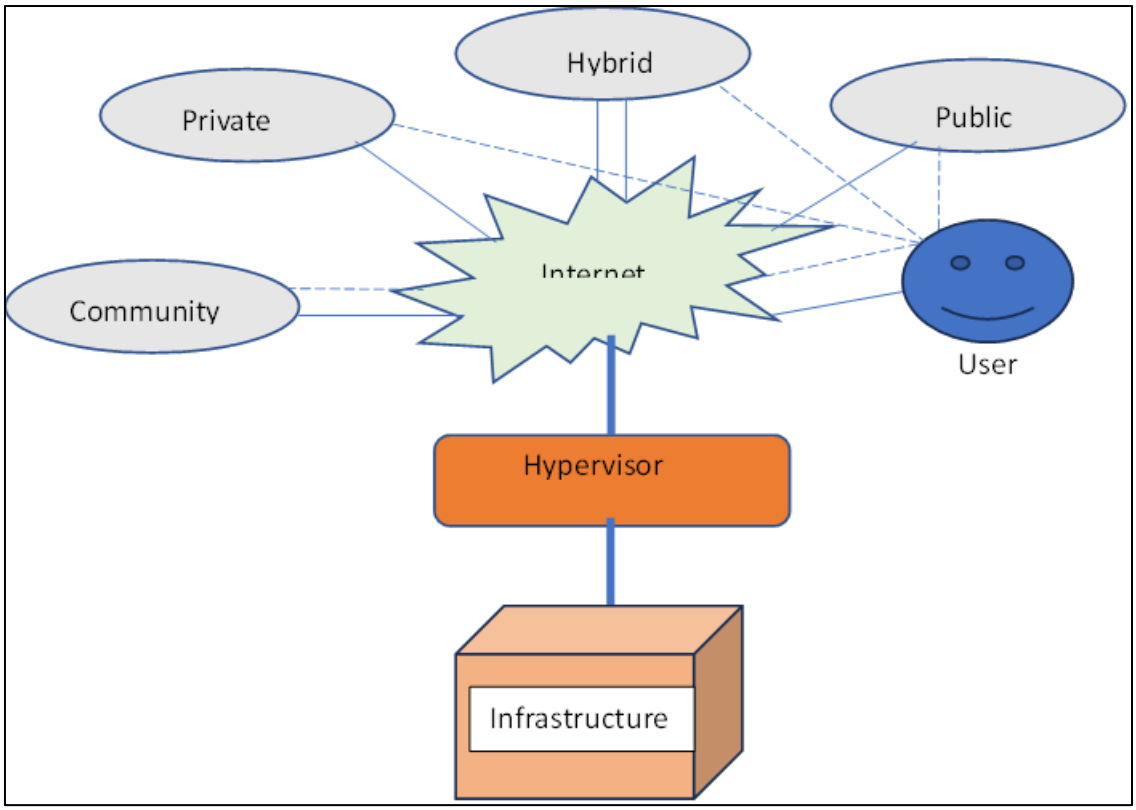


Figure 2: Cloud Architecture Model

Figure 3.1 shows the cloud architecture, and illustrate how hypervisor (VM) links the cloud infrastructure with the internet. A user will decide to engage in computing with any of these, depending on interest and cost of usage. However, multi-cloud, public, and hybrid are less expensive.

3.1 Clouds and their Available Services

There are many available clouds, these are owned by difference organisation and in some cases, jointly owned.

Table 3 below shows the details of the cloud organisation and the available services they provide for users. Also, these numerous services are attached and used for different purposes.

Table 3: Cloud Computing Services

SN	ORGANISATION	SERVICES	USES
1	Google Cloud Computing	Gmail Google Docs Google Analytics Google AdWords and AdSense Picasa	(a) Provides users with an email service of 25GB storage, less spam and mobile access. (b) User docs like: spread sheets, Word documents and PowerPoint presentations online. © Analytics is used to monitor the traffic coming onto a website. (d) Uses for advertising tools (e) Is a tool used to exhibit products and upload their images in the cloud.
2	Microsoft Cloud Computing	Windows Azure SQL Azure Windows Azure App Fabric	(a) A Windows environment for storing data and running applications in the cloud. (b) Relational database services in the cloud that use a special version of Microsoft SQL Server.

		Windows Azure Marketplace	© An infrastructure for applications that run in the cloud or inside an organisation. (d) It is an online market to buy and sell application software and data.
3	Amazon Web Services (AWS)	Amazon Elastic Compute Cloud (Amazon EC2) Amazon Simple Storage Services (Amazon S3) Amazon Virtual Private Cloud (Amazon VPC) Amazon CloudFront Amazon Route 53 Amazon Relational Database Services (Amazon RDS) Amazon Simple DB Amazon Simple Queue Service (Amazon SQS) Amazon SNS Amazon Elastic MapReduce	(a)Web service that provides configurable computing resources in the cloud. (b) Scalable, secure and reliable storage for the Internet that can be used to store and retrieve data of any size on the web. © It connects the company's existing IT infrastructure to the AWS cloud via a Virtual Private Network (VPN) (d)A web service for content delivery that transfers customers' data at high speed using a global network of edge locations (e) It is a scalable and highly available DNS service. (f) A web service that helps manage a relational database in the cloud (g) provides core database functions. (h) A scalable, reliable, hosted queue for storing messages. (i) It is a web service that helps manage and send notifications from the cloud. (j) Web service that enables customers to process a vast amount of data in the Cloud.
4	HP Cloud Compute	HP Cloud Object Storage HP Cloud Block Storage HP Cloud CDN HP Cloud Relational Databases for MySQL HP Cloud Identity Service	(a) An online massive storage capacity that allows customers to store large amounts of data, such as audio and video files. It enables scaling up and down on multi-club. (b) Allows customers to store data on HP Cloud resources for as long as they need and easily move it from one compute resource to another. © CDN refers to Content Delivery Networks, and it is a web service that delivers data from HP Cloud Object Storage to customers around the world at high speeds using a global network of servers from HP and Akamai technology. (d)A web service that provides on-demand access to relational structured databases. (e) provides a single method for managing HP cloud users' identities and authentication.

3.2 Analysis of Cloud Computing Deployment Systems

Cloud computing deployment systems are classified as public cloud, private cloud, community cloud and hybrid cloud.

- Public Cloud: In the public cloud, the infrastructure and other cloud services are made available to the general public over the Internet. The cloud is owned and managed by a CSP that offers services to consumers on a pay-per-use basis. Many popular cloud services are public, like Amazon EC2, Google App Engine and Salesforce.com.
- Private Cloud: the computing resources are operated exclusively by one organisation. It may be managed by the organisation itself or a CSP. Private clouds are considered to be more secure than public clouds since they may be running on designated infrastructure. The community clouds and hybrid clouds fall between public and private clouds.
- Community clouds: Community clouds are similar to private clouds, but the cloud infrastructure and computing resources are shared by several organisations that have the same mission, policy and security requirements. An example of a community cloud is an educational cloud used by universities and institutes around the world to provide education and research services.
- Hybrid Clouds: the infrastructure consists of a combination of two or more public, private or community

cloud components. The cloud components are bound together by standardised technology and managed as a single unit, yet each cloud remains a unique entity [6]. In line with this, Figure 3.2. shows different cloud deployment models.

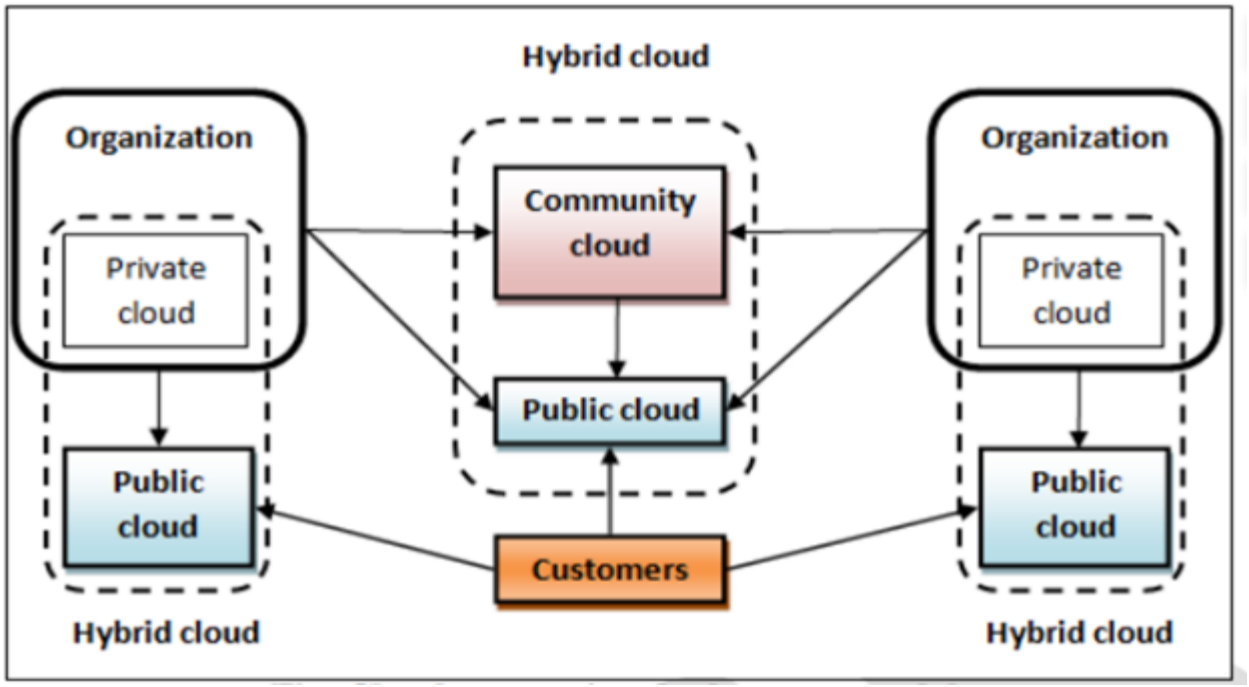


Figure 3: Cloud computing deployment model. Adopted from: International Journal of Engineering Research and General Science (2015).

4 METHODOLOGY

The research adopts a systematic literature review (SLR) approach to examine the existing cloud computing security model. Also, to identify an efficient method for enhancing system security. This methodology is structured in a way to enable a comprehensive, unbiased, and reproducible review process.

4.1 Research Design

This study is based on a qualitative review of secondary data obtained from scholarly educational databases, industry reports, articles and conference papers. The search is based on analysing, comparing, and synthesising various cloud security models proposed for the research.

4.2 Data Sources and Search Strategy

Related literature was collected from popular scholarly academic databases. These databases include:

- Google Scholar
- IEEE Xplore
- ACM Digital Library
- ScienceDirect
- SpringerLink
- WJARR

Search queries included these keywords:

- Cloud computing security models
- Cloud security frameworks
- Data protection in cloud computing
- Cloud security architecture
- Secure cloud system

Also, the Boolean operator (AND, OR) was used to fine-tune the search and improve result accuracy.

4.3 Inclusion and Exclusion Criteria

For the relevant quality assurance, the following were applied.

4.3.1 Inclusion criteria:

- An article focuses on a cloud security model or framework
- The studies published in peer-reviewed journals and conference papers
- Publication within the last 8 years to ensure the studies are currently relevant.
- Paper written in English, for authors to be comprehensible

4.3.2 Exclusion criteria:

- Authors excluded any studies that are not directly related to cloud security
- Duplicate publication
- Non-scholarly articles or opinion pieces
- Any publication lacking sufficient methodological detail

5 CLOUD DEPLOYMENT AND SECURITY LEVEL

Cloud deployments are the cloud delivery methods to the users. It involves Private, Public, Community and Hybrid. Table 3.2 shows: the scope of services of each deployment model, the owners, the types of organisation that manage it, the locations, and its security level (Babak, 2017).

Table 4: Comparison of Cloud Deployment and Security Level (www.ijergs.org).

Deployment Model	Scope of Services	Owner	Managed by	Security Level	Location
Private Cloud	Single organisation	Single organisation	Single organisation or CSP	Highly secure	Off or On-premises
Public Cloud	Public and a large industry group	CSP	CSP	Low	Off premise
Community Cloud	Organisation of the same mission, policy, and security requirements	Several organisation	Several organisations or CSP	High security	Off or On-premise
Hybrid Cloud	Public and organisation	Organisation and CSP	Organisation and CSP	Averagely secured	Off and On premise

5.1 Data Extraction and Analysis

However, selected articles were critically reviewed, and key information was extracted, which includes:

- Confidentiality, Integrity and Availability (CIA)
- Scalability
- Ease of implementation
- Resistance to security threats
- Cost efficiency

5.2 Synthesis of Findings

Based on the synthesis of findings, extracted data were synthesised using a thematic analysis approach, which is widely used in qualitative research methods for identifying, analysing and reporting patterns within collated data. The security model was divided into grouped these categories:

- Encryption-based models
- Identity and Access Management (IAM) models
- Framework of multi-layer security
- Deployment and adaptive security models
- Multi-cloud and single cloud security models

However, these categorisations enable to identify pattern, trends and gaps in existing research.

5.3 Validation of Result

To guarantee the efficiency and reliability of the finding, the finding was cross-checked across multiple sources. Consistent results across various studies were considered more reliable.

Those contradictory findings were critically analysed to understand the major differences. However, an asymmetric security algorithm is easy to implement and has a unique security pattern.

Limitation

This study is limited to secondary data and may not capture floating data and unpublished models. However, due to the evolution of modern technology, some of the models reviewed may soon be outdated. Also, findings depend on the methodology adopted for the research. So, an interested scholar may try another method.

6 CONCLUSION

In conclusion, the internet ubiquitously enacted cloud technology. Nowadays, cloud computing is very essential to individuals, organisations and communities because of its numerous advantages to users. Moreover, business advantages and the rapid growth of cloud services attract theft fore data breaches to hike fraud for their economic advantages. The review examines the quality of various cloud security models and synthesises their roles to ensure an efficient security model for the cloud system.

Furthermore, to have an efficient security cloud model, the study shows the cognisance tools: Cypher algorithm, encryption techniques, authentication mechanism, access control system, intrusion detection module, hybrid and multi-cloud security framework. The highly esteemed skills to integrate these sophisticated tools will surely guarantee cloud efficacy, reliability and confidentiality. Observation from the analysis shows that no single cloud model is efficient now for cloud security; though, asymmetric encryption techniques can be upgraded to handle constantly updating users' primary keys, which will rescue key redundancy. Also, integrating multiple security approaches using the STEM approach to implement an efficient security system.

However, most data breaches are caused by individual and organisational users. So, the organisation should train users on safe practices. Also, further research should focus on implementing a sophisticated, cost-efficient model for cloud computing to mitigate cloud data breaches.

In all, implementing a strong and capable cloud security model will guarantee an efficient, secure, CIA and trusted system for users and organisations in the entire globe.

STATEMENTS ON COMPLIANCE WITH ETHICAL STANDARDS

Acknowledgments

We sincerely appreciate many academic sites that are free and always available to surf like: Google Scholar; IEEE Xplore; ACM Digital Library; ScienceDirect; SpringerLink; WJARR, and others. Also, many cloud organisation gives open source to users which enable use to source for information. We commend Amason Web Service, Microsoft, Google etc for effective update. However, the IJSRA editor did a good job.

Disclosure of conflict of interest

The authors declare no conflicts of interest regarding this manuscript.

REFERENCES

[1] Tinankoria D, Babak BR. Cloud computing: a review of the concepts and deployment models. Int J Inf Technol Comput Sci. 2017. doi:10.5815/ijitcs.2017.06.07.

[2] Comer DE. The cloud computing book: the future of computing explained. Chapman and Hall/CRC; 2021.

[3] University of East London (UEL). Cloud computing manual. UEL-EN-7026; 2024.

[4] Buyya R, et al. Mastering cloud computing: foundations and applications programming. Newnes; 2013.

[5] Rasha T, Omar A, Omar T, Nicolae T. Design of an e-healthcare management system based on cloud and service-oriented architecture. IEEE; 2023.

[6] Aashna RM, Ashfaque, Prajakta PC. Exploring cloud computing services and applications. Int J Eng Res Gen Sci. 2015;3(1). ISSN: 2091-2730.

[7] Waqas A. Trends and challenges in securing cloud computing environments: an overview of current techniques. Premier Journal of Computer Science. 2024. doi:10.70389/PJCS.100004.

[8] Godwin N, Rahman AS. Implementing zero-trust security models in cloud computing environments. World J Adv Res Rev. 2024;24(3):1647-1660. doi:10.30574/wjarr.2024.24.3.3500.

[9] Myroslav B. Cloud computing security in 2026: expert insight [Internet]. Codebridge; 2025 [cited 2026 Mar 13]. Available from: https://www.codebridge.tech/articles/cloud-computing-security-expert-insigh

[10] Wickramarachchi T. Cloud security challenges in a multi-cloud world [Internet]. 2026. Available from: https://medium.com/@thinuridulsini/cloud-security-challenges-in-a-multi-cloud-world-2026-41de572dec44

[11] Darajat CD, Suhardi S, Budi R. Security issues in multi-cloud: a systematic literature review. IEEE Access. 2025. doi:10.1109/ACCESS.2025.3561352.

[12] Jerry C. DES/AES compared to RSA [Internet]. Quora; 2025 [cited 2026 Feb 2]. Available from: https://www.quora.com/

[13] Rashi K, Anchal G, Sparsh P, Yogesh K, Sanyam J. An improvised model for securing cloud-based systems. Computational Intelligence. 2021;933.

[14] Gorelik E. S.M. in engineering and management [thesis]. Cambridge (MA): Massachusetts Institute of Technology, Engineering Systems Division; 2025.

[15] Sentinel O. Cloud security [Internet]. 2025 [cited 2026 Feb 23]. Available from: https://www.googlescholar.net/

[16] Amit C, Sajad AZ. A review of security models in cloud computing and an innovative approach. Int J Comput Trends Technol. 2015;30(2):87-103. Available from: http://www.ijcttjournal.org

[17] Manuel P. A trust model of cloud computing based on quality of service. Ann Oper Res. 2015;233:281-292. doi:10.1007/s10479-013-1380-x.

[18] Zhihu.com. Introduction to the RSA model [Internet]. 2025 [cited 2026 Feb 14]. Available from: https://www.zhihu.com/topic/intro

[19] Kinza Y. What is the RSA algorithm? [Internet]. Tencent Cloud; 2025 [cited 2026 Feb 14]. Available from: https://www.tencentcloud.com/techpedia