RESEARCH ARTICLE OPENACCESS

With The Growing Adoption of Cloud Computing, Cybersecurity Strategies Must Shift Toward Zero Trust Architecture to Effectively Mitigate Modern Threats

Pratibha Singh[1], Naina Gupta[2], Nootan Ojha[3], Pratham Vashisth[4], Prof. Ashutosh Pradhan[5]

Master of Computer Application
RD Engineering College,
Ghaziabad
India

ABSTRACT
The rise in cybersecurity breaches, data privacy issues, phishing emails across the globe created the demand for cybersecurity protection in cloud-computing platforms such as IaaS, PaaS and SaaS. Cloud Computing Technology is widely used across industries to optimise the real-time data integration, storage, outsourcing IT product/services and reduced the need for strong IT infrastructure for software development. The study proposed the integration of the Zero Trust Architecture model across cloud computing platforms to improve cyber-resilience

Keywords - AZero Trust Architecture, Cloud Computing, Cyber-resilience, privacy, cybersecurity breaches.

I. INTRODUCTION

The concept of cloud computing can be defined as the technique of delivering computing resources such as servers and storage, which originated from the idea proposed by an American computer-oriented scientist and psychologist, J.C.R. Licklider. Licklider's idea of "Intergalactic Computer Network"impacted ARPANET (Network Agency of Advanced Research Projects) development by introducing the cloud computing feature [1]. Cloud computing plays a crucial role in improving the influence of cybersecurity strategies in the prospect of mitigation of cyber threats. Cloud computing offers scalable resources, resulting in real-time detection of cyber threats, alongwith assurance about instant response to cyber attacks.

The key benefits acquired by the active collaboration of cloud computing techniques with cybersecurity strategies involve the integration of Zero Trust Architecture for the appropriate addressing of cybersecurity threats. This model effectively relies on the principle associated with “never trust and always verify,” which highlights no trust for any user or device irrespective of their network access and location. The approach is significant for cloud environments due to its positive impact on reducing threats by leveraging reliability, specifically for internal users[2]. ZTA is important for companies having a hybrid workforce, as its data is accessed by employees from various locations

II. CLOUD COMPUTING

In this section, we will provide a brief overview of the cloud computing technique through the introduction of its concept along with its operational function and main framework of its research

A. Brief introduction to Cloud Computing

The cloud computing technique ensures access for users to resources on demand. The variable models of cloud computing are divided into two broad categories, which are the Deployment model and the Service model. The deployment models of the cloud computing technique involve public, hybrid, cloud computing and private models. Public models include IT infrastructure, such as networking resources. As per Khando et al. [3], Private models provide a computing environment developed specifically for a single organisation[3]. Hybrid models combine both private and public networks for the creation of a flexible infrastructure. Community cloud involves the sharing of a common interest among several organisations.

The service models are Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS). The Infrastructure as a Service (IaaS) is a cloud-computing that facilitates access to computing resources, including networks, servers and internal storage on the service user’s demand. The diagram demonstrates the basic architectural view of IaaS using Azure Virtual Machines. The figure highlights that individual virtual machines have access to a single network card with a distinct public IP. The end user access request is transmitted to the Public load balancer through a firewall. The virtual machine used by the software owner is uploaded into the storage system. Based on the user request, a distinct virtual machine linked to a computer is deployed for the end user.

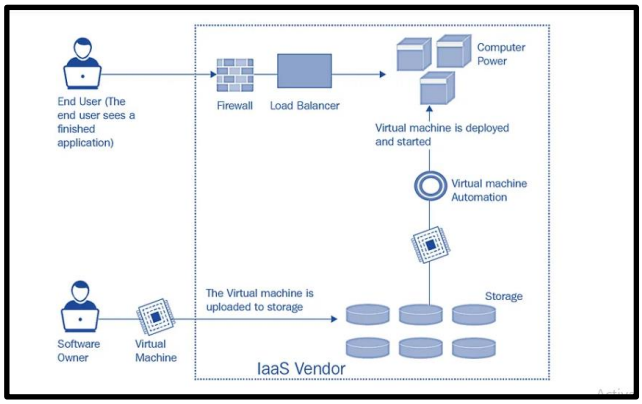

Figure 1: Network Architecture of Infrastructure-as-a-Service vendor platform

Source: [4]

The Software as a Service (SaaS) involves accessibility to software applications by users through the internet [5]. The image below illustrates the architecture of SaaS in real time, for example, the coding segment, cloud-based database and organizational servers are integrated into a single application. The end user can easily get access to the application (latest software version) through the internet and can use the software using a subscription model.

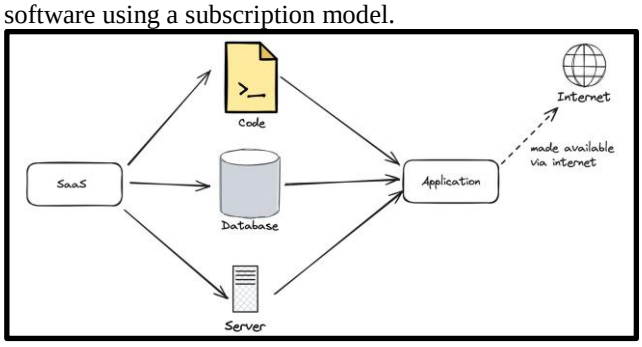

Figure 2: Architecture of Software-as-a-Service model

Source: [5]

Platform-as-a-service is a cloud-computing model that leverages third parties to offer business applications, hardware and software components to the end users on demand [6]. The image below illustrates that developers integrated the network access, hardware components, data backup facilities, data security, application hosting and database. Moreover, the third-party developers also offer an Integrated Development Environment, an Operating System and Software on a subscription basis to run individual applications.

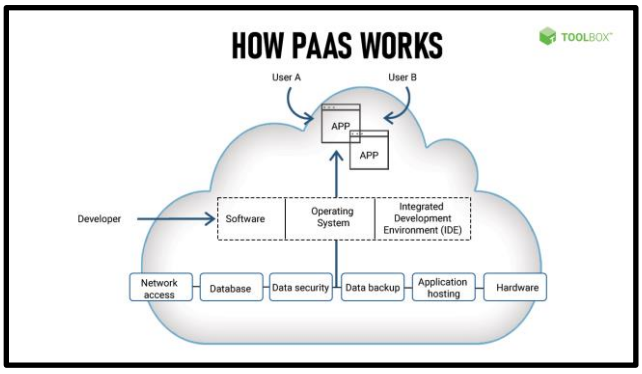

Figure 3: System Architecture for Platform-as-a-Service model

Source: [6]

B. ***Operational functions of Cloud Computing (CC)***

In [7], the author explained that the operational function of the CC model is to offer data programs, hardware and software components and an integrated development environment to the end-users on demand. This reduced the reliance of end users on local storage services and computer hard drives. Thus, in comparison to on-premise or local servers, cloud computing services are more inclined towards the cost-effectiveness side. Alongside that, resource management, backup and recovery and automatic also comes under the core operational function of cloud computing. In [8], the authors evidenced and distributed nature of Cloud Computing contributed to scale and share the computing capabilities with multiple end users.

C. ***Basic research framework of Cloud Computing***

According to the basic functioning of Cloud Computing, in [9], segments cloud computing in 2 aspects, the frontend and another is backend. In the front-end operations, a Graphical User Interface (GUI) is used to create a consistent interaction with the cloud. The key components of backend operations include, “security”, “management”, “cloud runtime”, “management”, “application” and “service”. The front-end and back-end components of the Cloud Computing research framework are connected via the Internet.

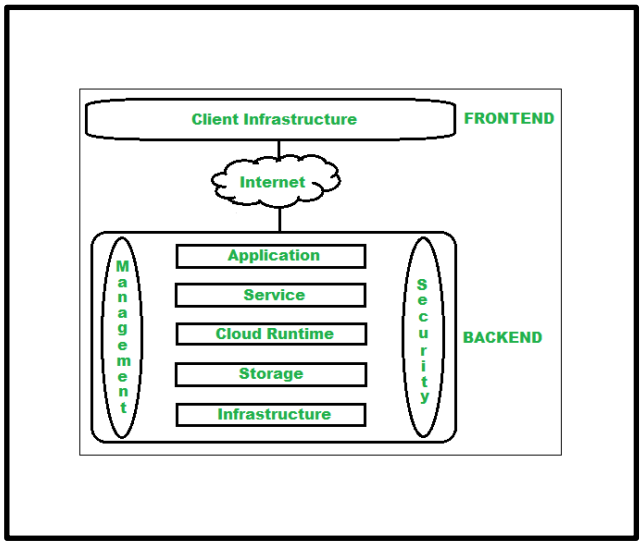

Figure 4: Basic Research Framework for Cloud Computing

Source: [9]

The proposed research framework of Cloud Computing also refers to the existing literature. For example, Binary Terms [10] proposed a research framework that highlights the core functioning of the frontend and backend components of Cloud Computing

.

III. RECENT CHALLENGES AND THREATS WITHIN CYBERSECURITY

A. Malware attacks

Malware attacks might occur in either frontend or backend processes of Cloud computing, for example, web application attacks are commonly seen in the front end side. Whereas, server-driven malware occurs from the back-end process of Cloud Computing. Here are some examples,

Denial of Service: The authorised end-users access to the server is lost, the attack can be planned from a single source as well as from distributed systems [11].

Logic Bomb: The code developed by a programmer enters into a specific application or event to carry out the destruction works.

B. Challenges of social engineering and phishing attacks

The frequent occurrence of phishing attempts and social engineering activities might hinder the usage of cloud computing platforms. Some of the consequences of social engineering and phishing attempts are stated below:

Financial Harm: Clicking on the phishing emails might lead to unauthorised access to financial account credentials.

Breach of individual privacy: Stolen of personally identifiable information through social engineering activities and phishing emails might lead to an individual privacy breach [12].

C. Advanced Persistent Threats and challenges

In [13], the author mentioned that the traditional Intrusion Detection System is prone to wrong identification of attacks, low accuracy and high false-positive rates towards Advanced Persistent Threats. APTs are referred to the targeted cyberattacks that aim to steal online information or data over time. Some of the negative consequences of APTs in cloud computing are explained below:

Increased operational cost: As per IBM Security, the average cost of recovering information from APT attacks increased to $4.35 million in 2023 [13].

Financial loss: From the perspective of a large organisation, a single APT attack can cost up to $6.93 million [13].

D. Ethical challenges

Turilli and Floridi [14] in their research evidenced that cloud computing adoption in the IT infrastructure can be challenged by a few ethical issues, which include, fairness and accountability. Describing each ethical challenge below:

Fairness: The prevalence of digital divide might trigger unfair distribution of computational resources during cloud computing [14]. Still in the 20th century, the prevalence of digital divide is considered high, as the internet access in urban areas was 82% whereas in rural regions it was 46% [15]

.

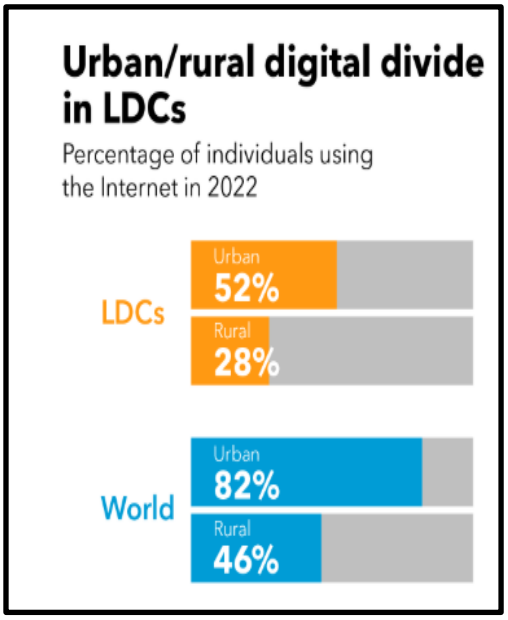

Figure 5: Digital Divide prevalence in the world in 2022

Source: [15]

Accountability: Cloud Computing platforms are prone to user anonymity, this might include the developed, end users and software procuring organisation. Thus, low accountability among the service users in cloud computing might amplify their privacy risks.

IV. APPLICATION SCENARIOS OF CLOUD COMPUTING TO MITIGATE CYBERSECURITY THREATS

A. Incident Response

Cloud Computing Technology enabled the users to quickly report the nature of cybersecurity attacks, for example, whether it is DDoS or logic bomb, or phishing emails. The integration of Cloud Technology enabled the users to quickly gain awareness of the attack, assessing the surface area of

attack, containing the attacks with firmware and minimising the harm through a distributed architecture. Some use cases of Cloud computing in Incident Response are:

Alibaba: The company applied Cloud computing technology, "Alibaba Cloud" to report, communicate and handle data breaches and security incidents [16].

Microsoft: The technology company also had a cloud computing platform, "Microsoft Cloud" in place to handle incident response and tackle network vulnerabilities effectively [17].

B. Threat Detection

Cloud-computing Technology can also be used in the areas of threat detection and threat intelligence. The technology plays a pivotal role in real-time detection of digital threats and network security vulnerabilities in SaaS, PaaS, or IaaS platforms. The use case of Cloud-based Threat Detection are provided below:

Amazon GuardDuty: The retail giant, Amazon, incorporated ML algorithms into its cloud service platform, "Amazon Web Services", to procure Amazon GuardDuty. The application offers end-to-end visibility and is explicitly used for Intelligent Threat Detection [18].

IV. CYBERSECURITY STRATEGIES WITHIN ZERO TRUST ARCHITECTURE

In [19], the author evidenced 5 core principles of Zero Trust Architecture in terms of strengthening the perimeter-based defense mechanisms in cloud space. The Zero Trust Core Principles include "establish identity", "assume presence of a hostile actor", "zero trust is a paradigm", "Risk-based adaptive approach", and "limited access" [19]. The perceived benefits of zero trust architecture are flexibility, enablement and resilience. Thus, maximizing cybersecurity with the Zero Trust Architecture model using the following stages:

1. Risk Prioritisation in digital landscape: Identifying the vulnerable surface and threat landscape in the cyber environment using ML/AI algorithms.
2. Enterprise-wide Policy to gause cyber assets sensitivity: Reporting the threat landscape and assets vulnerability using cloud-based Threat Detection services (Amazon GuardDuty).
3. Granular perimeter enforcement along with microsegmentation of cyber assets: Assuming the operating cyber networks is hostile, this helps in removing the trust perception in cybersecurity and cloud computing. This fulfills one of the principles of Zero Trust Approach.
4. Applying the Zero Trust Network on IaaS Cloud Computing platforms: Leveraging the Zero Trust Network (ZTN) into the IaaS architectural model might reduce the vulnerability of facing cyber threats in the frontend and backend components of Cloud computing.
5. Updating the cloud server access provisions with multi-factor authentication: As proposed in [20], multi-factor authentication will help to minimize the disclosure of cloud servers to unauthorised access.

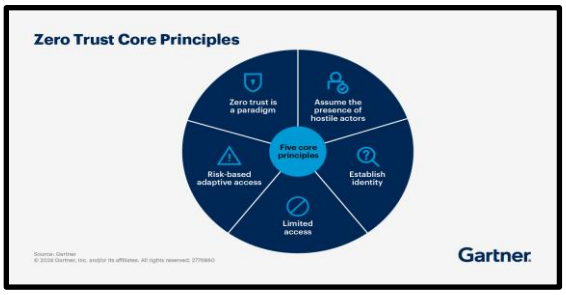

Figure 6: Principles of Zero Trust Network
Source: [19]

VI. Trends on future developments in Cloud computing and Zero trust cybersecurity frameworks

1) Identity Governance in Zero Trust Network

In [21], the author explained the future possibilities of implementing an Identity Governance policy in the cloud computing functional areas. The proposed future development can be achieved through enterprise resource access optimization, for example, only enabling partial access to cloud servers and online databases. This will also help to counter the access privileges in enterprise resources used for cloud computing.

2) Cloud-to-cloud Enterprise with Zero Trust Network integration

Zero Trust Network Approach is an ongoing trend in the field of cybersecurity and reputed technology brands and regulators such as Microsoft and the National CyberSecurity Centre also promote the usage of Zero Trust Architecture design to counter cyber vulnerabilities. Hence, there is a future possibility to enhance the perimeter security of Cloud-to-Cloud or MultiCloud Enterprise Network through Zero Trust Architecture deployment [21].

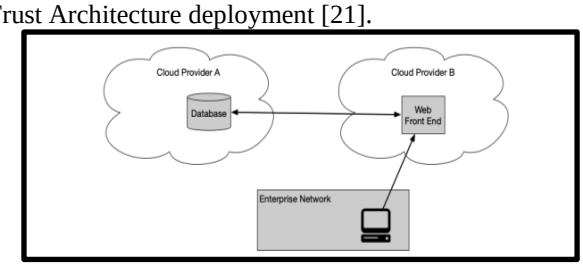

Figure 7: Multi-Cloud Enterprise using Zero Trust Architecture
Source: [21]

V. CONCLUSION

The increasing usage of the internet, smartphones and e-commerce positively influences the adoption rates of cloud computing technology. On the other hand, social engineering activities, phishing attempts and DDoS attacks acted as barriers to cloud computing integration. Thus, the findings of the research proposed the usage of the Zero Trust Architecture model to improve the cybersecurity controls in cloud-computing platforms.

REFERENCES

[1] S. Susnjara and I. Smalley, "Cloud Computing," accessed Apr. 25, 2025 [Online] Ibm.com. Available at: https://www.ibm.com/think/topics/cloud-computing.

[2] W. Yeoh, M. Liu, M. Shore, and F. Jiang, "Zero trust cybersecurity: Critical success factors and A maturity assessment framework," Computers & Security, vol. 133, p. 103412, Oct. 2023, doi: https://doi.org/10.1016/j.cose.2023.103412.

[3] K. Khando, S. Gao, S. M. Islam, and A. Salman, "Enhancing Employees Information Security Awareness in Private and Public organisations: a Systematic Literature Review," Computers & Security, vol. 106, no. 1, p. 102267, 2021, doi: https://doi.org/10.1016/j.cose.2021.102267.

[4] S. Mirkhanov, "What is Infrastructure as a Service (IaaS)," Navixy, Oct. 29, 2020. https://medium.com/navixy/what-is-infrastructure-as-a-service-iaas-25c15268ad05

[5] A. K. Batra, "Fundamentals of SaaS Architecture - Amit Kumar Batra - Medium," Medium, Dec. 24, 2023. https://medium.com/@amit2067/fundamentals-of-saas-architecture-c824f82b888b (accessed Apr. 25, 2025).

[6] V. Kanade, "What Is Platform as a Service (PaaS)? Definition, Examples, Components, and Best Practices," Spiceworks, Feb. 18, 2022. https://www.spiceworks.com/tech/cloud/articles/what-is-platform-as-a-service/

[7] R. Islam et al., "The Future of Cloud Computing: Benefits and Challenges," International Journal of Communications, Network and System Sciences, vol. 16, no. 4, pp. 53–65, Apr. 2023, doi: https://doi.org/10.4236/ijcns.2023.164004.

[8] H. U. Khan, F. Ali, and S. Nazir, "Systematic analysis of software development in cloud computing perceptions," Journal of Software: Evolution and Process, Jun. 2022, doi: https://doi.org/10.1002/smr.2485.

[9] S. Jena, "Architecture of Cloud Computing," GeeksforGeeks, Mar. 10, 2021. https://www.geeksforgeeks.org/architecture-of-cloud-computing/

[10] Binary Terms, "What is Cloud Architecture: Layers and Types," Binary Terms, Nov. 16, 2022. https://binaryterms.com/cloud-architecture.html

[11] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments," Energy Reports, vol. 7, no. 7, pp. 8176–8186, Nov. 2021, doi: https://doi.org/10.1016/j.egyr.2021.08.126.

[12] M. Schmitt and I. Flechais, "Digital deception: generative artificial intelligence in social engineering and phishing," Artificial Intelligence Review, vol. 57, no. 12, Oct. 2024, doi: https://doi.org/10.1007/s10462-024-10973-2.

[13] N. H. A. Mutalib, A. Q. M. Sabri, A. W. A. Wahab, E. R. M. F. Abdullah, and N. AlDahoul, "Explainable deep learning approach for advanced persistent threats (APTs) detection in cybersecurity: a review," Artificial Intelligence Review, vol. 57, no. 11, Sep. 2024, doi: https://doi.org/10.1007/s10462-024-10890-4.

[14] M. Turilli and L. Floridi, "Cloud Computing and its Ethical Challenges," SSRN Electronic Journal, 2021, doi: https://doi.org/10.2139/ssrn.3850031.

[15] LibreTexts, "11.3: The Digital Divide," Workforce LibreTexts, Aug. 09, 2022. https://workforce.libretexts.org/Courses/Evergreen_Valley_College/Information_Systems_for_Business_2e/11%3A_Information_Systems_Globalization_and_Inequality/11.03%3A_The_Digital_Divide

[16] A. Nallathambi, "Alibaba Cloud in Cybersecurity," Alibaba Cloud Community, Aug. 24, 2023. https://www.alibabacloud.com/blog/alibaba-cloud-in-cybersecurity_600315

[17] Microsoft, "Security incident management overview - Microsoft Service Assurance," learn.microsoft.com, 2025. https://learn.microsoft.com/en-us/compliance/assurance/assurance-incident-management

[18] AWS, "Amazon GuardDuty – Intelligent Threat Detection - AWS," Amazon Web Services, Inc., 2024. https://aws.amazon.com/guardduty/

[19] Gartner, "Zero Trust Architecture: Strategies and Benefits | Gartner," Gartner, 2024. https://www.gartner.com/en/cybersecurity/topics/zero-trust-architecture

[20] EY, "How organizations can maximize security efforts with Zero Trust Architecture," Ey.com, 2025. https://www.ey.com/en_in/insights/cybersecurity/how-organizations-can-maximize-security-efforts-with-zero-trust-architecture

[21] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," NIST Special Publication 800-207, Aug. 2020, doi: https://doi.org/10.6028/nist.sp.800-207.