Iraqi Journal of Information and Communications Technology(**IJICT**)
Vol. 8, Issue 1, April 2025

www.ijict.edu.iq

ISSN: 2222-758X
e-ISSN: 2789-7362

A REVIEW ON ANALYZING CLOUD COMPUTING AND NETWORK CYBER SECURITY THREATS: ISSUES AND CHALLENGES WITH SOLUTIONS

Shah Mohammad [1], **Ahthasham Sajid** [2], **Urwa Sajjad Ahmed Abbasi** [3], **Hamza Razzaq** [4], **Shipra Yadav** [5], **Shahnaz Khademizadeh** [6]

[1] Department of Computer Science, Faculty of ICT, Baluchistan University of Information Technology, Engineering and Management Sciences, Quetta, Baluchistan, Pakistan

[2,4] Department of Cyber Security and Data Science, Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan

[3] School of Politics and International Relations, Faculty of Social Science, Quaid-e-Azam University, Islamabad, Pakistan

[5] Department of Computer Science and Engineering, Marwadi University, Rajkot Gujrat India

[6] Knowledge & Information Science Shahid Chamran University of Ahvaz, Ahvaz, Iran

bluesky7688@gmail.com[1], ahthasham.sajid@riphah.edu.pk[2], Urwa.sajjad1999@gmail.com[3], hamza.razzaq@riphah.edu.pk[4], shipra.yadav@marwadieducation.edu.in[5], sh_khademizadeh@yahoo.com[6]

Corresponding Author: **Ahthasham Sajid**

Received:01/06/2024; Revised:28/10/2024; Accepted:28/12/2024

DOI:**10.31987/ijict.8.1.288**

***Abstract*- Cloud computing is defined as the practice of storing, managing, and processing data on a network of remote servers hosted on the internet rather than a local server or a personal computer. Cloud computing is among the newest technologies in era of Information Technology (IT). Most firms employ cloud computing to save money on server, storage, and maintenance infrastructure purchases. Addressing the several problems related to cloud computing in depth is therefore rather crucial. A big problem for industries is security. In this paper, we investigate some major advantages of cloud computing and significant features of cloud model. The report also covers security concerns, drawbacks of the current method, and possible solutions related to cloud computing.**

keywords: **Cyber Defense, DDoS Attacks, MITM Exploits, DNS Poisoning, IP Spoofing, Rootkits, Botnets, Zero-Day Attacks, APT Attacks.**

I. Introduction

Cloud computing, which reduces costs and increases efficiency, became popular in 2009 because firms could lease storage and CPU power [1]. It removes physical hardware and staff administration through virtualization and remote sessions, enabling scalability, cheaper hardware costs, and better flexibility. Cloud computing's inception, benefits, security threats, literature review, comparative analysis, and future work are examined in this paper.

A. *Cloud Computing Architectures*

Cloud computing service models may be categorized into three main classifications. Depending on the precise demands and requirements of a business and the allocation of firm resources in the cloud, one of these service models, or a mix of the three, might be employed [2].

1) Software as a Service (SaaS): It is the primary cloud computing approach for small enterprises, providing software that can be accessed through web browsers instead of being installed locally as shown in Fig. 1. Users have a restricted

level of authority over the program and configuration settings, such as web-based apps and coding with limited access [3].

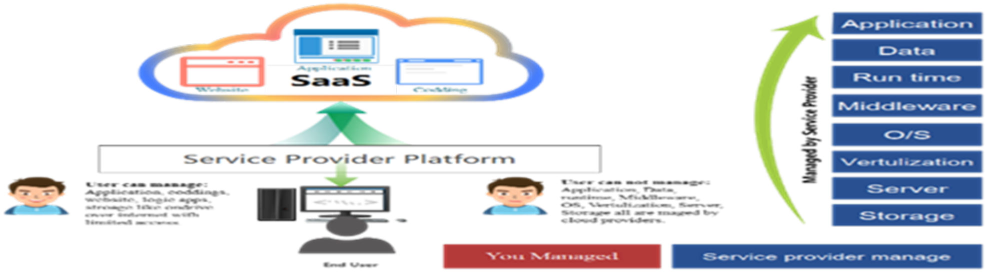
Application
SaaS
Website
Coding
Service Provider Platform
User can manage:
Application, coddings, website, logic apps, stroage like ondrive over internet with limited access.
End User
User can not manage:
Application, Data, runtime, Middleware, OS, Vertulization, Server, Storage all are maged by cloud providers.
Managed by Service Provider
Application
Data
Run time
Middleware
O/S
Vertulization
Server
Storage
You Managed
Service provider manage

Figure 1: Software as a Service (SaaS).

2) Infrastructure as a Service (IaaS): It leases computing resources and storage from an external supplier who handles CPUs, memory, and storage as shown in Fig. 2. Virtual machines, storage, and Azure load balancers are IaaS [4].

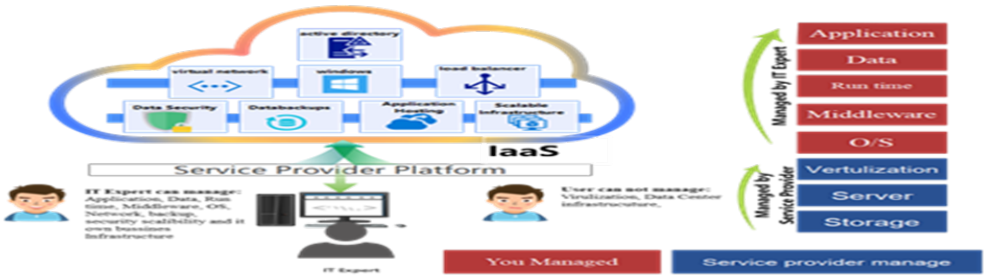

Figure 2: Infrastructure as Service provide resources to manage infrastructure network.

3) Platform as a Service (PaaS): It gives developers full control over program development with secure and scalable resources. It allows technological component and infrastructural customization [5]. Fig. 3 shows the Platform as Service Provider for App Development, and Coding with API.

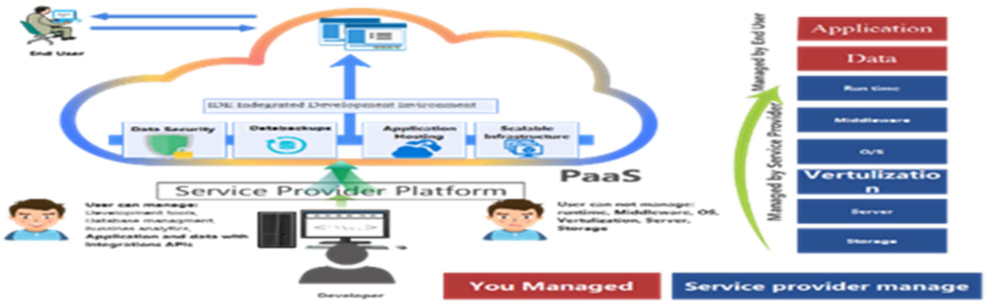
End User
IDE Indegrated Development Environment
Data Security
Databackups
Application Hosting
Scalable Infrastructure
PaaS
Service Provider Platform
User can manage:
Development tools, Database managment, Business analytics, Application and data with integrations APIs
Developer
User can not manage:
runtime, Middleware, OS, Vertulization, Server, Storage
Managed by End User
Managed by Service Provider
Application
Data
Run time
Middleware
O/S
Vertulizatio n
Server
Storage
You Managed
Service provider manage

Figure 3: Platform as Service provider for App development and coding with API.

B. *Cloud Computing Services - Explanation of Management Responsibilities*

As shown in Fig. 4, network administrators administer on-premises infrastructure, IaaS offers internet-based resources, PaaS manages web pages and code, while SaaS, suited for small enterprises, prioritizes speed and administration [4].

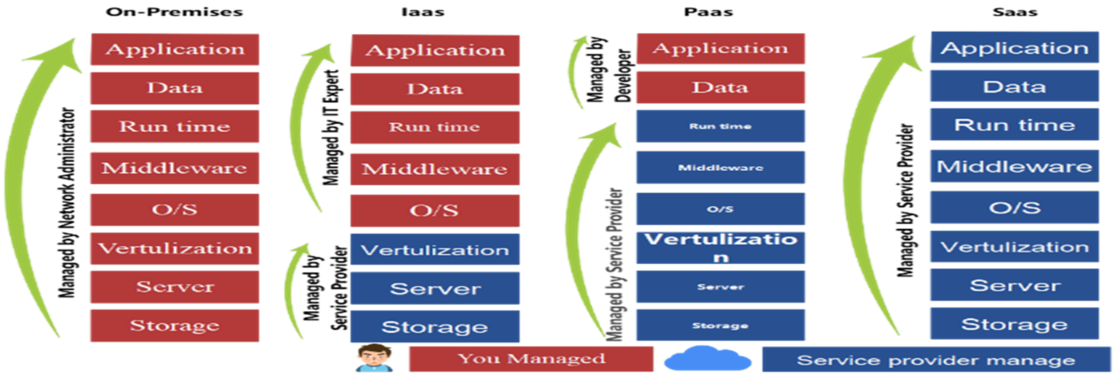

Figure 4: Comparison of on-premises, IaaS, PaaS, and SaaS: key differences and insights.

C. *Benefits of Cloud Computing*

Cloud computing benefits include lower IT expenditures by removing expensive systems and equipment [6]. It allows enterprises to scale operations and storage without costly upgrades. Cloud backups preserve and enable business continuity [7]. Smooth communication and file sharing across locations boost collaboration efficiency, while flexible work practices offer data access from anywhere [8]. The service's automatic updates keep systems up to date [9].

The most significant contributions of this study "Analyzing Cloud Computing and Network Cyber Security Threats: Issues and Challenges with Solutions" are as follows:

1) Identification of Principal Cybersecurity risks: The document delineates significant risks in cloud computing, encompassing Distributed Denial of Service (DDoS) assaults, data breaches, and advanced persistent threats, offering a thorough examination of the most urgent concerns in the field.
2) Evaluation of Security Protocols: It assesses current security protocols and finds deficiencies, providing a comprehensive grasp of the shortcomings in present protective measures.
3) Proposed Mitigation Strategies: The research recommends pragmatic solutions include encryption, firewalls, and multifactor authentication, specifically designed to successfully address the identified concerns.
4) Emphasis on Emerging Technologies: It highlights the significance of Artificial Intelligence (AI) and machine learning in improving threat detection and response, facilitating the development of more sophisticated and adaptable cloud security frameworks.

II. Research Methodology

This study utilizes a thorough qualitative research methodology to examine the difficulties and solutions associated with cloud computing and network cybersecurity. Considering the dynamic and complex nature of cybersecurity threats in cloud systems, a qualitative methodology facilitates a comprehensive understanding of the fundamental challenges and the formulation of successful responses. The research seeks to connect theoretical knowledge with practical applications in addressing cybersecurity risks by emphasizing real-world scenarios, expert views, and current case studies.

To fulfill the primary aims of the study, data is collected through a comprehensive examination of current literature, encompassing peer-reviewed journals, technical papers, and industry publications. This establishes a solid basis for recognizing the most common security issues, including data breaches, illegal access, and Advanced Persistent Threats (APTs), which are becoming more frequent in cloud systems. Moreover, interviews with cybersecurity professionals and cloud computing specialists offer direct insights into the changing threat landscape, new vulnerabilities, and possible responses [10].

The research uses a case-study methodology to illustrate actual instances of cybersecurity vulnerabilities in cloud computing settings. These situations are meticulously examined to reveal trends, evaluate the efficacy of executed solutions, and discern best practices applicable to analogous settings. Furthermore, the study incorporates a comparative assessment of current cybersecurity frameworks and technologies to determine their relevance, efficacy, and scalability in tackling the stated concerns [11].

This approach is pertinent due to its direct correlation with the study issue, since it specifically examines the intricate relationship between cloud computing and cybersecurity. The research intends to produce actionable insights by concentrating on qualitative data and expert perspectives, therefore improving the comprehension of current situations and fostering the creation of novel solutions. This method guarantees that the results are anchored in practical significance while tackling the theoretical deficiencies in the domain, so furthering the discussion on cloud computing and network cybersecurity [12].

Nowadays cloud computing becoming more prominent technology for every student, teacher, developer and businessman's. Where cloud provides many facilities to us but it has some challenges as well. Consequently, this study will provide the most prevalent obstacles that arise while dealing with cloud computing; let us examine them individually [13].

1) Data Security and Privacy: Comprehensive earlier studies have shown the significant hazards related to data security in cloud computing, including data loss, illegal access, and identity theft. Research has continually shown the necessity for strong user identification systems, efficient identity management, data encryption standards, and rigorous access restrictions to protect sensitive information. Research demonstrates that although cloud service providers guarantee a fundamental degree of security, organizations must adopt additional steps to reduce the risk of breaches that might harm their brand and financial viability [14].

2) Cost Management: The current research has investigated the financial difficulties linked to the "Pay as You Go" pricing model utilized by cloud service providers. This technique can conceal expenses associated with unutilized server IP addresses, storage resources, or instances that remain active during weekends or idle intervals. Research indicates that firms frequently undervalue these concealed expenses, resulting in considerable financial inefficiencies and unforeseen costs [15].

3) Multi-Cloud Environments: The intricacies of managing multi-cloud solutions, as emphasized in prior literature, are an increasing worry for IT teams. Businesses are increasingly utilizing hybrid cloud set-ups to exploit the distinct benefits of platforms like AWS, Azure, and Google Cloud. Nonetheless, previous research indicates that overseeing the integration and optimization of these varied systems has significant obstacles, such as operational inefficiencies and increased security concerns [15].

4) Interoperability and Flexibility: The complexity and duration of cloud service provider migrations have been highlighted in previous studies, especially because of the requirement for application stack redesign, data transfer supervision, and the implementation of new security measures. These studies highlight that such migrations frequently lead to operational interruptions and diminished flexibility, constraining firms' capacity to swiftly adjust to changing business requirements [16].

5) High Dependence on Network: Prior research has emphasized the essential role of high-speed networks in enabling effective data transmission between consumers and cloud servers. Research also underscores the difficulties arising from constrained network capacity and recurrent service disruptions, which disproportionately impact smaller firms. Ensuring sufficient network capacity continues to impose a considerable financial and operational strain on these organizations, as evidenced by previous research [17]. This part consolidates previous research, offering a fundamental comprehension of the primary issues and corresponding solutions in cloud computing security. These findings are crucial for guiding future developments in the sector.

III. Results and Discussions

When transitioning to cloud computing, it is essential to evaluate the security of the infrastructure, with a specific focus on the twelve most significant cyber vulnerabilities that may occur [18]. Cloud services may be accessed online by those who have the necessary credentials, which presents additional security obstacles. Comprehending the consequences of these risks is a crucial aspect of assessing cloud security dangers [19].

1) Poor Access Management: Cloud computing access management is crucial because hackers might use stolen keys to access data. Multi-factor authentication, which requires a password and a temporary key from a personal device, improves security. This protects accounts by informing users and locking accounts after breaches [20].
2) Data Breach and Data Leak: Data breaches can disclose sensitive data publicly or on the dark web due to unauthorized access and extraction. An all-encompassing cloud security approach that addresses user behavior is needed to prevent such attacks. This prevents data leaks [21].
3) Multi-factor Authentication: In order to proceed, the user is required to furnish not just evidence of their identification, but also their access credentials [22]. For example, entering a password and thereafter receiving a mobile phone notification containing a transient, randomly generated string of numbers that can only be used once. It has become one of the current cloud security standards [23].
4) Encrypting Data at Rest: Data-at-rest refers to stored data that is not currently in use on different devices. This technique encompasses several components such as logs, databases, datasets, and other related elements [24]. A

perimeter firewall regulates the flow of data between a private and public network, whereas an inside firewall oversees and identifies irregularities in approved network traffic [25].

5) Data Loss: In addition to the negative consequences of a data breach, there exists a more severe cloud security risk: the potential for irreversible loss, akin to tears dissipating in the rain. Data loss is a challenging cloud security issue that is both unpredictable and hard to control. Now, let us examine three of the primary factors that frequently lead to data loss [26], [27].
6) Strategies to Prevent Data Loss - Backups: Maintain frequent backups and automate the process with data loss prevention software, determining backup eligibility. Cloud APIs for data transit and analytics pose security risks, hence multi-factor authentication and encryption are necessary [28]. To prevent API problems, undertake penetration testing, system security audits, SSL/TLS data transfer encryption, and multi-factor authentication.
7) Misconfigured Cloud Storage: When cloud computers are set up incorrectly, whether they are used for storage or computing, they can be hacked. Most of the time, people make the following mistakes when configured: The server's cloud security settings are set to the defaults, and data and access are managed normally. Someone who isn't supposed to be there gets accidental access to private data because of bad access control [29].
8) Denial-of-service (DoS) attack: Disabling users' access to programs or disturbing their work makes DoS assaults a security concern [30]. Modern intrusion detection systems that detect anomalous traffic and alert users depending on their behavior can avoid DoS assaults [31]. Cloud breaches may be detected and addressed using this method.
9) Botnet attacks: Exploiting botnets of hacked devices, hackers spread malware via emails, links, and unlawful websites. Botnets steal personal data, disseminate spam, and launch DDoS assaults. The type of botnet assault matters more than the number of active bots [32].
10) Types of Botnet Attacks: Even so, the amount of active bots in a cloud infrastructure does not always determine the relative strength of a botnet attack. Somewhat, the nature of the attack has a far greater impact on its success.
    - Brute Force Attack: When username and password are unknown, hackers try different password (see Fig. 5) repeatedly while guessing, name, date of birth, nationality and etc. publicly revealed personal information for password attempts [33].

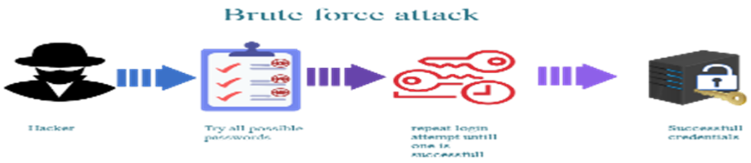
Brute force attack
Hacker
Try all possible passwords
repeat login attempt untill one is successfull
Successfull credentials

Figure 5: Brute force attack.

- Distributed Denial of Service (DDoS) attack: Particular target networks are overloaded with a lot of activity with the goal of completely crashing the system as shown in Fig. 6.

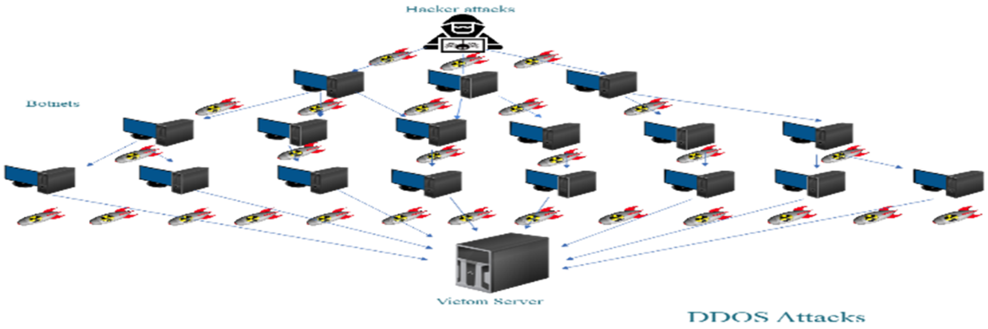

Figure 6: DDoS attack.

- Spam and Phishing: Individuals are cheated into sharing personal information and login credentials by suspicious emails and messages, gain attackers access to the computer system in question [34]. Fig. 7 shows stealing the login information of user.

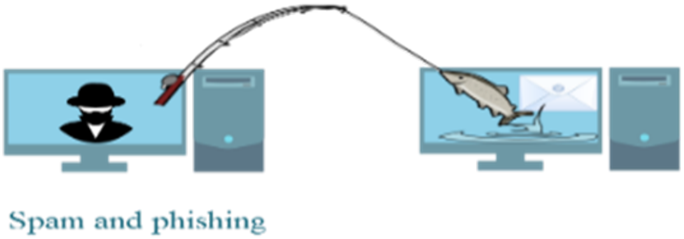

Figure 7: Stealing the login information of user.

- Device Bricking: Botnet assaults can incapacitate targeted devices by infecting them with viruses that hide the attack. Restrict access from unfamiliar networks, implement cybersecurity best practices, and employ Sangfor Botnet Detection to prevent such attacks. Update software, change passwords, encrypt devices, and educate personnel. If a breach happens, contact IT for OS and antivirus upgrades [8].

11) Man in the Middle (MitM) Attack: This involves hackers intercepting two parties' communication to eavesdrop or change data (see Fig. 8). This attack intercepts or decrypts data before it reaches its target [34].

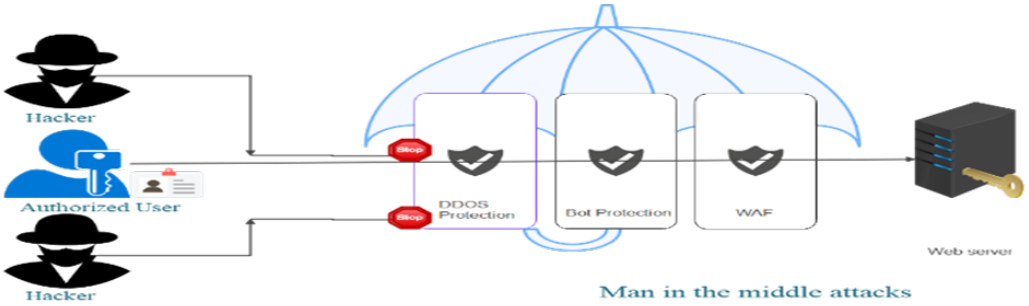

Figure 8: MitM attacks communication listening between source and destinations.

12) Preventing MitM Attacks:

- VPN: For secure connections, use a VPN Connection between the client and the server. VPN protects your data transfer from MitM attacks. VPN prevents unauthorized traffic bypass.
- Firewall: By allowing only authorized traffic, the firewall can block MitM attacks. To prevent MitM attacks, firewalls filter visitors from unsecured sources.
- Two-factor Authentication: It is a two-step security procedure. Other than the username and password, this authentication requires extra forms of identification. Two-factor authentication protects privacy protection and prevents various types of middle attacks [21].
- Network Monitoring: To analyze traffic, use monitoring of network and intrusion prevention system tools. When an MitM invasion occurs, intrusion detection tools raise an alert [27].
- SSL/TLS: Always communicate using SSL/TLS protocols. These protocols ensure data confidentiality and integrity in communication while protecting against MitM attacks [30].
- HTTPS: SSL & TLS allows for secure communications in HTTPS. MitM attacks on HTTPS websites are hard for an attacker to carry out [34].
- Domain Name Server (DNS): Domain name system is a network protocol that allows IP addresses and domains to be identified. Encode your DNS requests with DNS over HTTPS to protect against DNS hijacking. To prevent malware-based middle attacks, the DNS resolver fulfils content filtering [11].

13) Domain Name Server (DNS) Spoofing: DNS faking, or DNS cache poisoning, sends visitors to bogus websites where hackers steal login credentials and personal data. Fake sites often install malware or botnets, giving attackers long-term access to victims' computers and data.

As in Fig. 9 below, the BUITMS user wants to access real website https://www.buitms.edu.pk/ but the user access fake website https://www.hackerone.com it looks same as real website, the communication between user and fake website is encrypted by hacker [25].

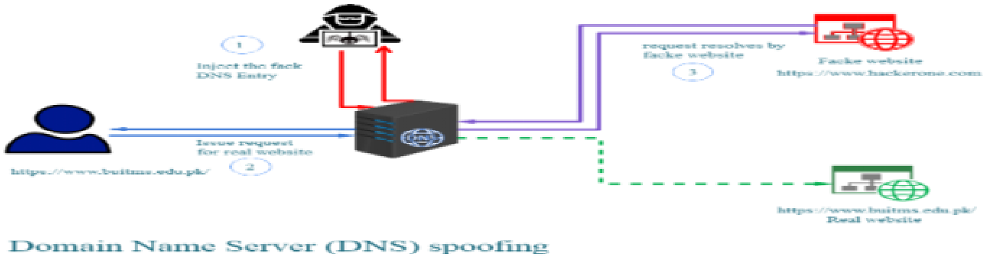

Figure 9: DNS spoofing attack.

14) Preventing DNS Spoofing Attacks:
    - Domain Name Server Security (DNSSEC): DNSSEC is a protocol that adds extra methods of verification to your DNS to make it more secure. The protocol generates a one-of-a-kind cryptographic signature that is stored along with your other DNS records, such as a records and CNAMEs. Your DNS resolver then uses this signature to verify a domain name reaction, making sure that the record has not been tampered with [8].
15) IP Spoofing: MitM and DoS attacks involve IP spoofing, which compromises network security [9]. Block undesirable IP addresses and foreign packets with ingress filtering and firewall settings to avoid such assaults. Stop TCP sequence prediction attacks by limiting connections to recognized MAC addresses and disabling IP source routing on all devices [12].
16) A Distributed Denial-of-Service Attack: DDoS attacks disturb legitimate users by flooding servers with botnet traffic [5]. Perform a full resource inventory, filter hardware and software, and design a detailed response strategy with roles and backups to prevent these assaults. Inform clients about performance difficulties and explore Azure, AWS, and Google Cloud DDoS protection.
17) Rootkit Attack: Rootkits allow concealed data theft and botnet assaults [10]. Rootkit removal generally requires specialist programs like Kaspersky's TDSS Killer, although deleting and reinstalling the OS may be necessary [35].

IV. Comparative Analysis of Security Threats of Cloud Computing

After giving a general overview of the risks to cloud security and the possible ways to protect it, this section will focus on comparing cloud security, data privacy, and identification problems [35]. Companies prefer cloud computing for its affordability, storage, and scalability, but data security and privacy issues remain. Information security and data loss are key concerns. This study examines twelve significant cloud security risks and their remedies, expanding on [3],[7], [16] limited research as shown in Table I.

TABLE I
Analysis of Cloud Security

REFERENCES	YEARS	OBJECTIVE	FOCUS OF WORK	LIMITATIONS
Neeti Mehra [3]	2018	• Explore cloud security issues and challenges. • Highlight secure login practices for the cloud. • Provide insights into common attack techniques used by hackers.	• Secure login to cloud. • How to avoid all techniques that provide loopholes for hackers. • Common attacks on cloud.	• There is no technical and proper solution for cyber-attacks. • Solutions to attacks are very common and widely known. • Lacks technical and innovative solutions.
Rajeev Kumar [7]	2020	• Investigate advances in cloud security solutions. • Explore the incorporation of artificial intelligence in identifying and alleviating cyber risks. • Analyse the scalability of cloud security frameworks.	• Storage access via Remote data integrity checking. • Enhancement of encryption of data. • Detailed AI-based solutions for threat detection.	• Very limited details mentioned in the paper related to accessing storage on cloud. • Techniques are still not fully mature and face many problems. • Shared access key with specific time period is not used.
Abdullah Aljumah [16]	2020	• Assess hazards and vulnerabilities in cloud data storage. • Propose encryption methodologies to augment data secrecy. • Emphasize user education to mitigate intrusions.	• Define various aspect of threats • Highlights encryption as a primary defense. • Emphasizes user awareness and training.	• Two factor authentication is not used. • Poor quality of graphics used. • Overemphasis on data storage, lacking broader network and infrastructure security insights.

V. CONCLUSION

This research emphasizes the significance of mitigating security vulnerabilities in cloud computing, encompassing network, cloud, and data security. The main emphasis is on guaranteeing the security of data even in the absence of the data owner. Ensuring appropriate management of cloud security concerns, such as encryption and data verification, is of utmost importance. Ensuring the safety of services, even during cloud failures, is crucial despite the complexity of cloud systems, which makes achieving end-to-end security tough. Placing trust in apps from untrustworthy sources continues to be a major worry, but effectively utilizing cloud services with the proper security measures, such as DDoS protection, network security groups, and recovery service vaults, can reduce the chances of being hacked. Complying with these cloud security requirements is crucial for safeguarding a company's brand and financial well-being.

VI. FUTURE WORK

Future initiatives must concentrate on deploying sophisticated, scalable, and adaptive security protocols to successfully tackle the difficulties of cloud computing and network cybersecurity. These actions encompass:

1) Enforce rigorous access limitations by permitting only authenticated and sanctioned networks to engage with cloud infrastructures. Employ sophisticated firewalls, Intrusion Detection Systems (IDS), and precisely configured Access Control Lists (ACLs) to oversee and manage both incoming and outgoing traffic. Enhanced Role-Based Access Control (RBAC) must be implemented to restrict user rights to the minimum required for job execution, hence safeguarding data security and integrity.
2) Consistently analyze network traffic using advanced analytics technologies to detect abnormalities and possible threats in real time. Implement enterprise-level antivirus and anti-malware solutions, and maintain timely updates of operating systems and applications to prevent vulnerabilities. When possible, implement fortified operating systems such as Linux

due to their intrinsic security benefits. Utilize advanced defensive technologies, including DDoS mitigation tools, and implement Multi-Factor Authentication (MFA) to secure cloud-based operations.

3) Implement a continuous cybersecurity education program for IT professionals and personnel to be proactive against emerging threats. Conduct frequent training on new cyber threats, including ransomware, social engineering, and phishing assaults, and furnish people with best practices for the implementation and maintenance of secure systems. This proactive strategy guarantees a knowledgeable and alert workforce ready to react promptly to risks.

Incorporation of AI and machine learning utilize AI-driven solutions to anticipate, identify, and mitigate security risks prior to inflicting substantial damage. Machine learning algorithms may examine extensive datasets to reveal concealed trends and possible weaknesses, offering proactive alarms and actionable insights. Formulate and implement extensive cybersecurity frameworks customized to the specific needs of cloud environments. These frameworks must incorporate blockchain for immutable data records, zero-trust models for rigorous verification at each access point, and quantum-resistant encryption approaches to address forthcoming cryptographic difficulties. Perform regular security audits and penetration testing to assess the effectiveness of deployed safeguards. These methods facilitate the identification of vulnerabilities in security architecture and provide actionable recommendations for subsequent improvements. The future work can guarantee a more secure, resilient, and adaptive cloud computing ecosystem that is capable of mitigating both current and emergent cyber threats by addressing these key areas.

FUNDING

None.

ACKNOWLEDGEMENT

The authors would like to thank the reviewers for their valuable contribution in the publication of this paper.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] H. BULENS, AZ-900, HENDRIK BULENS, 2019.
[2] K. D. Foote, "DATAVERSITY," DATAVERSITY, December 17, 2021. [Online]. Available: https://www.dataversity.net/brief-history-cloud-computing.
[3] N. Mehra, "Analyzing Cloud Computing Security," Issues and Challenges, p. 10, Springer Nature Singapore Pte Ltd. 2018.
[4] Oroos Arshi and Aryan Chaudhary, "Fortifying the Internet of Things: A Comprehensive Security Review", EAI Endorsed Trans IoT, vol. 9, no. 4, p. e1, Oct. 2023.
[5] D. K. Riaan Lowe, Exam Ref AZ-104 Microsoft, Birmingham: BIRMINGHAM-MUMBAI, 2022.
[6] Q. Government, "Queensland Government," Business Queensland, 16 11 1995. [Online]. Available: https://www.business.qld.gov.au/running-business/digital-business/online-risk-security/cloud-computing/how. [Accessed 16 11 2022].
[7] R. Kumar, "Security in Cloud," New Delhi, India, New Delhi, India, 2020.
[8] vanigupta, 20024. [Online]. Available: https://www.geeksforgeeks.org/. [Accessed 16 11 2022].
[9] S. Technologies, "SNAGFOR," Sangfor Technologies, 2019. [Online]. Available: https://www.sangfor.com/glossary/cybersecurity/what-is-botnet-attack. [Accessed 2022].
[10] S. Miles, Microsoft Azure, Livery Place: Livery Place, 2022.
[11] E. Vodovatova, "THE APP solution," THE APP solution, 11 11 2016. [Online]. Available: https://theappsolutions.com/blog/development/cloud-security-risks/. [Accessed 16 11 2022].
[12] Arshi, O. Chaudhary, A. (2024). Smart healthcare: Integration of AI and brain cells for advanced healthcare applications. Open Health, 5(1), 20230029. https://doi.org/10.1515/ohe-2023-0029
[13] K. Sriram, "Cloud Panel," Cloud Panel, [Online]. Available: https://www.cloudpanel.io/blog/what-is-man-in-the-middle-attack/. [Accessed 2022].
[14] r. b. B. D. M. Tomasz Andrzej Nidecki, "Invicti," Invicti, 2020. [Online]. Available: https://www.invicti.com/learn/mitm-ip-spoofing-ip-address-spoofing/. [Accessed 2022].
[15] Arshi, O., Mondal, S. Advancements in sensors and actuators technologies for smart cities: a comprehensive review. Smart Constr. Sustain. Cities 1, 18 (2023). https://doi.org/10.1007/s44268-023-00022-2

[16] A. Aljumah, "Cyber security threats," Saudi Arabia, Saudi Arabia, 2020.
[17] N. Davies, "Security Boulevard," Security Boulevard, 21 12 2020. [Online]. Available: https://securityboulevard.com/2020/12/6-significant-cloud-security-threats/. [Accessed 16 11 2022].
[18] O. Arshi, A. Chaudhary and R. Singh, "Navigating the Future of Healthcare: AI-Powered Solutions, Personalized Treatment Plans, and Emerging Trends in 2023," 2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI), Raipur, India, 2023, pp. 1-6, doi: 10.1109/ICAIIHI57871.2023.10489554.
[19] I. U. Khan, M. Y. Ayub, A. Abdollahi and A. Dutta, "A Hybrid Deep Learning Model-Based Intrusion Detection System for Emergency Planning Using IoT-Network," 2023 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM), Cosenza, Italy, 2023, pp. 1-5, doi: 10.1109/ICT-DM58371.2023.10286954.
[20] Ahmad, Waqas, Aamir Rasool, Abdul Rehman Javed, Thar Baker, and Zunera Jalil. 2022. "Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey" Electronics 11, no. 1: 16. https://doi.org/10.3390/electronics11010016
[21] Catteddu, Daniele. "Cloud Computing: benefits, risks and recommendations for information security." In Web Application Security: Iberic Web Application Security Conference, IBWAS 2009, Madrid, Spain, December 10-11, 2009. Revised Selected Papers, pp. 17-17. Springer Berlin Heidelberg, 2010.
[22] Ramachandra, Gururaj, Mohsin Iftikhar, and Farrukh Aslam Khan. "A comprehensive survey on security in cloud computing." Procedia Computer Science 110 (2017): 465-472.
[23] Ramgovind, Sumant, Mariki M. Eloff, and Elme Smith. "The management of security in cloud computing." In 2010 Information Security for South Africa, pp. 1-7. IEEE, 2010.
[24] Ali, Mazhar, Samee U. Khan, and Athanasios V. Vasilakos. "Security in cloud computing: Opportunities and challenges." Information sciences 305 (2015): 357-383.
[25] Kuyoro, Shade O., F. Ibikunle, and Oludele Awodele. "Cloud computing security issues and challenges." International Journal of Computer Networks (IJCN) 3, no. 5 (2011): 247-255.
[26] Ahmed, Monjur, and Mohammad Ashraf Hossain. "Cloud computing and security issues in the cloud." International Journal of Network Security Its Applications 6, no. 1 (2014): 25.
[27] Khalil, Issa M., Abdallah Khreishah, and Muhammad Azeem. "Cloud computing security: A survey." Computers 3, no. 1 (2014): 1-35.
[28] Winkler, Vic JR. Securing the Cloud: Cloud computer Security techniques and tactics. Elsevier, 2011.
[29] Sabahi, Farzad. "Cloud computing security threats and responses." In 2011 IEEE 3rd International Conference on Communication Software and Networks, pp. 245-249. IEEE, 2011.
[30] Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." Future Generation computer systems 28, no. 3 (2012): 583-592.
[31] Inukollu, Venkata Narasimha, Sailaja Arsi, and Srinivasa Rao Ravuri. "Security issues associated with big data in cloud computing." International Journal of Network Security Its Applications 6, no. 3 (2014): 45-56.
[32] Wu, Hanqian, Yi Ding, Chuck Winer, and Li Yao. "Network security for virtual machine in cloud computing." In 5th International conference on computer sciences and convergence information technology, pp. 18-21. IEEE, 2010.
[33] Subramanian, Nalini, and Andrews Jeyaraj. "Recent security challenges in cloud computing." Computers Electrical Engineering 71 (2018): 28-42.
[34] Sohal, Amandeep Singh, Rajinder Sandhu, Sandeep K. Sood, and Victor Chang. "A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments." Computers Security 74 (2018): 340-354.
[35] I. U. Khan, I. M. Qureshi, M. A. Aziz, T. A. Cheema and S. B. H. Shah, "Smart IoT Control-Based Nature Inspired Energy Efficient Routing Protocol for Flying Ad Hoc Network (FANET)," in IEEE Access, vol. 8, pp. 56371-56378, 2020, doi: 10.1109/ACCESS.2020.2981531.