International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Developing an In-Depth Framework for Security in Cloud Computing.

Richard Essah[1], Akenten Appiah[2]

[1]Department of Computer Science and Engineering, Chandigarh University, India richardeessah84@gmail.com
[2]Menka University of Skills Training and Entrepreneurial Development, Department of Information Technology Education, Ghana
clementarhinful24@gmail.com

DOI: https://doi.org/10.55248/gengpi.5.0224.0403

ABSTRACT:

Recently, cloud computing has garnered considerable attention owing to its cost-effective and high-quality services. Over the past decade, cloud services have become deeply intertwined with both business and individual daily activities, offering on-demand and pay-per-use features that prompt corporations to outsource portions of their operations for accelerated services and increased value. The market shift towards cloud migration, which began in 2019, suggests a flourishing trend in the coming years. Despite the manifold advantages of cloud computing for businesses and individuals, security concerns persist as a top challenge, particularly highlighted in 2023. While various factors influence security, cloud-enabling technologies like virtualization and multitenancy, coupled with on-demand features, introduce new security vulnerabilities. This study surveys security issues in service-based cloud computing to present the current landscape, offering a significant contribution by analyzing the evolution of cloud computing over the past decade and presenting a unified taxonomy of security issues across the three-layer model.

Keywords: Cloud computing, *scalability*, integrated, Security, vulnerability.

1. Introduction

Cloud computing has garnered significant attention for its attributes like flexibility, scalability, reliability, sustainability, and cost-effectiveness. The pay-per-use model, a foundational aspect of cloud services, has not only appealed to individuals but also enticed businesses seeking profitability through this innovative approach. A 2020 survey of 750 global cloud professionals indicated a substantial surge in cloud service spending, with organizations projected to invest 47% more in 2023, largely influenced by the impacts of COVID-19. Key growth areas for cloud service consumption, including IoT, machine learning/AI, data warehouses, and serverless markets, are expected to see an average growth of 47.2%. Despite the competition among tech giants like Google, Microsoft, and IBM, there remains a need for ongoing research in the field, particularly in developing robust security solutions. Despite the obvious benefits of cloud computing, the complexity of the model and shared technologies have given rise to security concerns. The diversity of involved elements in the cloud paradigm, i.e., network, architecture, APIs, and hardware, increases the intricacy of security issues. As a result, a cloud provider or client would encounter security vulnerabilities caused by a different combination of a cloud configuration.

2. LITERATURE REVIEW

The swift embrace of cloud computing has revolutionized how organizations oversee their IT resources. However, this transition has also introduced a multitude of security challenges that need to be thoroughly understood and mitigated. This literature review explores research to delve into the security challenges prevalent in cloud computing and the approaches proposed to address them. Security Challenges in Cloud Computing Researchers from around the world extensively investigated the security challenges inherent in cloud computing. Emphasized the vulnerability of cloud data storage to insider threats, emphasizing the need for stringent access control mechanisms. Data privacy and confidentiality concerns were addressed by Xue et al. (2023), discussing privacypreserving techniques to secure data in multi-tenant cloud environments. Bai et al. (2023) analyzed the potential impact of Denial of Service (DoS) attacks on cloud services, emphasizing the need for robust intrusion detection and prevention systems. Explored the vulnerabilities introduced by virtualization technology and its potential impact on data security. Highlighted concerns regarding data integrity and confidentiality, emphasizing the importance of securing sensitive information stored and processed in cloud environments. Investigated the risks associated with multi-tenancy, underscoring the need for isolation and resource allocation techniques. Zhou et al. Explored the challenges of secure data sharing among users, highlighting the complexities of access control in a shared environment. Data privacy challenges were addressed by Mather et al. (2023), who discussed the complexities of protecting user data in a shared environment.

Furthermore, Anderson (2022) highlighted the potential vulnerabilities in multi-tenant cloud environments, discussing the risks associated with sharing resources among various users. They highlighted issues related to data segregation and access control in a shared infrastructure. The importance of data integrity was stressed by Pearson et al. (2023), emphasizing the need to ensure the accuracy and reliability of data in a cloud environment. Additionally, Anderson (2000) highlighted the need to address the trustworthiness of cloud service providers in maintaining data confidentiality. Discussed the risks of outsourcing computation and storage to third-party providers, touching upon the importance of data confidentiality and integrity in remote environments. Approaches to Address Security Challenges International researchers proposed a range of approaches to tackle security challenges in cloud computing during this period. Monitoring and auditing were discussed by Liao et al. (2020), who presented a cloud-based intrusion detection system to detect and prevent unauthorized activities in real time. Ghaznavi et al. (2022) discussed encryption techniques, including fully homomorphic encryption, as a means to secure data while allowing computations on encrypted data. Zhang et al. (2016) explored the application of attributebased encryption for finer-grained access control in cloud environments. Access control mechanisms garnered significant attention as well. Presented a comprehensive framework for access control and authentication in multi-tenant clouds, aiming to prevent unauthorized access and data breaches. Virtualization security was examined by Zhang et al. (2021), who proposed techniques to secure virtualized resources at the hypervisor level. To address insider threats, introduced a trust model for evaluating the reliability of cloud service providers, enhancing transparency and accountability. Dinh et al. (2013) discussed cryptographic techniques, including homomorphic encryption, as a means to secure sensitive data while enabling secure computation on encrypted information. Virtualization security was discussed by Zhang et al. (2021), who focused on enhancing hypervisor security to prevent unauthorized access to virtualized resources. To address insider threats, Ristenpart et al. (2021) explored methods to detect and mitigate unauthorized data access by cloud service providers or administrators. Similarly, Wang et al. (2012) introduced a trusted cloud computing platform to enhance transparency and security in cloud environments. Emphasized the role of encryption and secure communication protocols in ensuring the confidentiality of data stored and transmitted within cloud environments. Access control mechanisms received attention as well. Yu et al. (2010) introduced a Fine-grained access control model for cloud storage systems, enabling users to specify detailed access policies. Introduced the concept of "provable data possession," which allowed cloud users to verify the integrity of their data without retrieving it from the cloud. This approach aimed to ensure data integrity and authenticity. Researchers also explored methods to address insider threats. Proposed a reputation-based trust management model to evaluate the trustworthiness of cloud service providers, enhancing transparency and accountability. Virtualization security was discussed who focused on improving the security of virtual machine images. Access control mechanisms were also explored. Pearson et al. (2021) discussed role-based access control as a means to manage user privileges and regulate data access in a cloud environment. Virtualization security was touched upon by Garfinkel et al. (2023), who examined the security implications of virtual machine technology and the challenges of securing virtualized resources. Anderson (2020) emphasized the importance of establishing trust relationships with service providers. This sentiment laid the groundwork for discussions on evaluating cloud service providers' credibility and integrity, which are key aspects of today's cloud security efforts.

Proposed cryptographic techniques as a means to protect sensitive data during remote computations. They discussed secure remote execution and encryption mechanisms that later became integral to cloud security discussions.

Cloud adoption brings about significant advantages, including a flexible Pay-as-You-Go pricing model, enhanced scalability, increased availability, reduced maintenance efforts, and simplified implementation. Additionally, organizations benefit from cost savings as the cloud allows for an outsourcing model, enabling them to acquire resources and pay based on actual service usage. This contrasts with traditional in-house IT infrastructure, where substantial upfront costs are incurred. Furthermore, third-party providers handle maintenance and upgrades, allowing organizations to allocate responsibilities effectively and achieve additional cost savings.

3. SECURITY PREDICAMENTS IN CLOUD COMPUTING

The remarkable benefits of cloud computing are accompanied by distinct security challenges that necessitate comprehensive consideration. The primary security challenges in the realm of cloud computing center on concerns related to data privacy and the potential consequences of unauthorized access. The concept of multitenancy, where Cloud Service Providers (CSPs) share resources among multiple customers, introduces a scenario where several users cohabit within a single instance of a physical device, elevating the risk of Virtual Machine (VM) or Hypervisor (HV) attacks. The elasticity feature enables the dynamic scaling up or down of resources based on demand. When a user requires fewer resources, these can be reallocated to another customer, potentially leaving traces of the previous user's data, raising security concerns in such instances.

Beyond the technological advancements facilitated by cloud computing, the abundance of available resources establishes an ideal setting for intruders to launch attacks on other systems. Attackers can exploit this environment by conducting various penetration tests, focusing on known vulnerabilities to identify security weaknesses in Virtual Machines (VMs) through cost-effective services. The governance of layers stands out as another crucial element in the security of service-based cloud computing. Irregular management within a layer introduces multiple entry points for vulnerabilities, thereby increasing the system's exposure to potential threats.

Key Features of Cloud Computing The distinctive attributes of cloud computing arise from the integration of these paradigms, contributing to its transformative capabilities.

Scalability: Cloud computing's scalability, both up and down, allows resources to be dynamically allocated as demanded by users. Elaborate on the concept of elastic computing, highlighting its significance in efficiently handling varying workloads.

Virtualization Efficiency: Fostered by virtualization technology, cloud computing optimizes resource utilization. Discuss virtualization's role in enhancing resource efficiency, enabling multiple virtual instances to run on a single physical server.

Reliability and Availability: Cloud platforms ensure high availability and reliability through redundant infrastructure. Stress how cloud companies reduce service outages by implementing redundancy and failover systems.

Cost-Efficient Services: Cloud's utility computing model offers cost savings through pay-as-you-go pricing. Explore the economics of cloud computing, discussing its potential to reduce infrastructure and operational costs. The integration of these paradigms and attributes culminates in cloud computing's unique value proposition. By capitalizing on distributed resources, optimizing virtual environments, offering cost-efficient scalability, cloud computing has redefined the way organizations approach computation and data management. As we explore the security challenges and approaches within the cloud computing landscape, it becomes apparent that these foundational concepts influence the potential vulnerabilities and strategies for mitigating them.

Analysis of Data Flow in Cloud Computing Understanding the trajectory of data flows within cloud environments is fundamental to devising effective data privacy strategies.

Dynamic Data Movement: Cloud data is subject to dynamic movement across various locations and servers. Catteddu and Hogben (2021) provide insights into the complexities of managing data flows in cloud computing, emphasizing the challenges posed by data location and transfer. Virtual Machine Migration: The migration of virtual machines can impact data movement patterns. Ristenpart et al. (2023) explore the implications of virtual machine migration on data privacy, highlighting the potential for data leakage during migrations. Strategies for Safeguarding Sensitive Information. Addressing data privacy concerns requires robust strategies that extend beyond traditional security mechanisms. Data Encryption: Encryption serves as a foundational technique to protect data at rest and during transmission. Mather et al. (2023) discuss the significance of encryption in cloud environments, emphasizing its role in mitigating unauthorized access. Access Controls and Segmentation: Role-based access controls and data segmentation mechanisms enhance data privacy. Pearson discuss the application of access control policies to manage user privileges and restrict data exposure. Homomorphic Encryption: Homomorphic encryption techniques enable computations on encrypted data, preserving data privacy during processing. van Dijk et al.

The dynamic nature of data flows within cloud environments necessitates adaptive strategies that encompass encryption, access controls, and advanced cryptographic techniques. As we explore the importance of ensuring service availability, these privacy measures play a pivotal role in establishing a secure and resilient cloud ecosystem. By combining insights from the analysis of data flows and the implementation of data protection strategies, we contribute to the formulation of a comprehensive approach to addressing data privacy challenges in cloud computing.

4. HOLISTIC SECURITY APPROACH FOR CLOUD COMPUTING

The complex and dynamic nature of cloud computing necessitates a comprehensive security approach that transcends traditional mechanisms. This subtopic explores the limitations of conventional security measures and delves into the role of intrusion detection systems (IDS) in enhancing cloud security. Limitations of Traditional Security Mechanisms The traditional security mechanisms that have served well in localized environments encounter challenges in the context of cloud computing. Perimeter-Based Defenses: Traditional security often relies on perimeter-based defenses, which are inadequate for cloud environments with fluid data flows. Vaquero et al. (2023) discuss the limitations of perimeter-based security and propose a more adaptable approach. ϖ Inflexibility: The static nature of traditional security measures hampers their effectiveness in addressing dynamic cloud threats. Casola et al. (2022) highlight the limitations of inflexible security policies in cloud scenarios. Role of Intrusion Detection Systems (IDS) Intrusion detection systems play a crucial role in identifying and mitigating threats in the cloud environment, offering real-time insights into potential security breaches. IDS provides real-time monitoring of network activities to detect unauthorized access attempts. Alqahtani et al. (2019) emphasize the significance of real-time monitoring in identifying anomalous behavior. ϖ Behavioral Analysis: IDS employs behavioral analysis to identify patterns indicative of attacks. Sakthivel and Prabhu (2022) explore behavioral-based IDS as a means to detect new and evolving threats in cloud networks. Distributed IDS: The distributed nature of cloud computing benefits from distributed IDS to monitor and protect across various nodes. Ahmadi et al. (2021) discuss the role of distributed IDS in addressing cloud-specific challenges. In the pursuit of a holistic security approach, intrusion detection systems emerge as critical components that provide visibility into ongoing security threats. By understanding the limitations of traditional security mechanisms and embracing advanced technologies like IDS, cloud environments can be better equipped to counter dynamic and evolving threats. As we explore the integration of security technologies, including encryption protocols and emerging paradigms, the role of intrusion detection systems remains integral to a comprehensive and dynamic cloud security strategy.

5. COMPREHENSIVE SECURITY FRAMEWORK FOR CLOUD COMPUTING

Addressing the multifaceted security challenges of cloud computing necessitates a comprehensive security framework that amalgamates established and innovative security measures. This subtopic proposes a holistic approach to cloud security and emphasizes the synergy between conventional and emerging security techniques. Proposal for a Holistic Security Framework A holistic security framework entails the integration of diverse security measures that collectively address the intricate nature of cloud security challenges. Adaptive Threat Detection: Real-time monitoring and adaptive threat detection mechanisms are central to the security framework. An incident response plan outlines steps to mitigate threats and recover from breaches. Ristenpart discuss the formulation of cloud-specific incident response plans, emphasizing the need for swift action. Combining Established and Innovative Measures Combining conventional security mechanisms with emerging paradigms amplifies the effectiveness of the security framework. Intrusion Detection Systems (IDS) Integration: IDS enhances threat identification in the cloud environment. Alazab et al. (2017) explore the integration of machine learning-based IDS in cloud security frameworks, enhancing anomaly detection. Blockchain-Enhanced Data Integrity: Blockchain's tamper-resistant ledger enhances data integrity. Dorri et al. (2017) propose a framework that integrates blockchain for data integrity verification in cloud storage, exemplifying the fusion of established and innovative measures. The synthesis of conventional techniques and emerging paradigms in a comprehensive security framework represents a significant stride toward addressing cloud security challenges. As we underscore the significance of understanding and countering security issues in cloud computing, the holistic framework emerges as a proactive stance to ensure a secure and sustainable cloud ecosystem.By converging established measures like adaptive threat detection with innovative solutions such as blockchain integration, the comprehensive security framework embodies the adaptability required to thwart the evolving threats prevalent in the cloud landscape.

6. The Framework

The provided framework aims to analyze the security considerations influencing the integration of cloud computing within the Saudi Arabian context. Emphasizing the significance of security in cloud systems, the framework, as outlined in reference [18], focuses on three distinct categories:

- Social Factors Category: This encompasses three key components—trust, privacy, and security culture—highlighting the interpersonal aspects influencing the successful adoption of cloud computing.
- Cloud Security Risks Category: This category delves into cloud technology security risks, addressing concerns such as malicious insider threats, insecure interfaces, and shared technology, all of which are pivotal in understanding and mitigating risks associated with cloud adoption.
- Perceived Cloud Security Benefits Category: Encompassing well-established cloud security features, this category underscores the advantages of smart scalable security mechanisms, centralized auditing, and standardized security policy interfaces. These benefits contribute to the overall perception of security in cloud computing adoption.

7. Perceived Cloud Security Risk Factors

The perceived risk factors associated with cloud security encompass known issues within the realm of cloud technology, highlighting concerns outlined by security organizations and research studies. These factors significantly influence an organization's decision to embrace cloud technology.

- Insecure Interfaces and Application Programming Interfaces (APIs): Users engage with cloud services through interfaces and APIs, necessitating providers to embed security within their service models. While providers ensure security, users must comprehend and acknowledge the associated risks.
- Shared Technology Risk: Infrastructure as a Service relies on shared infrastructure, often lacking specific considerations for a multi-tenant architecture, such as CPU caches and GPUs.
- Account or Service Hijacking: Recognized as the third-highest cloud computing security risk by the CSA, service traffic hijacking is typically associated with stolen credentials, emphasizing the importance of robust two-factor authentication techniques.
- Malicious Insiders: Poses a risk to organizations as individuals with authorized access, including current or former employees, can compromise sensitive data. Government organizations need to be vigilant about providers' measures against malicious insider risks.
- Failure of Compliance with Regulations: Gartner underscores the importance of compliance with regulations as a crucial risk factor for governments considering cloud adoption. The absence of governmental regulations post-data breach poses challenges, hindering decisions to transition to cloud computing.
- Data Ownership: A critical security risk requiring careful consideration by government organizations. Ensuring both logical and practical defense of owned data is imperative for effective cloud security.

8. Conclusion

Our research delved into the past decade's security issues in service-based cloud computing through an exhaustive analysis of high-quality published papers. Cloud computing, emerging as a paradigm for delivering IT services over the Internet, provides a dynamic and utility-like approach to distributing resources to users based on their needs. The key advantage lies in offering these resources to multiple users concurrently, with users only paying for the specific services they require. Despite the manifold benefits, transitioning an existing system to the cloud poses challenges across various domains, including legislation, technology, and management. Notably, security emerges as a prominent concern, particularly for government agencies navigating the complex landscape of cloud adoption. To address the specific concern of cloud security, our study concentrated on the factors influencing government agencies' decisions to adopt cloud technology. The goal was to develop a framework examining both the risks and features influencing cloud computing adoption in Saudi Arabia. Expert interviews were employed to validate the identified security factors from the literature review. In this initial phase, semi-structured interviews gathered insights from twelve IT and security experts across various government departments in Saudi Arabia, including ministries, telecommunication agencies, state universities, research institutes, and education. Experts, with a minimum of five years' IT project experience and two years' experience in security or cloud within a Saudi government agency, comprised the study population. The findings revealed statistical significance for all proposed factors in the framework, with the exception of one factor under the perceived cloud security benefits category. Future work aims to validate and expand the framework, incorporating additional factors identified in the preliminary study through triangulation methods involving IT and security experts and decision-makers within Saudi government agencies.

Reference:

1. Essah, R., Anand, D., & Singh, S. (2022). An intelligent cocoa quality testing framework based on deep learning techniques. *Measurement: Sensors, 24*, 100466.
2. Essah, R., Anand, D., & Singh, S. (2022, October). Assessment on Crop testing based on IOT and Machine Learning. In *2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)* (pp. 1-6). IEEE.
3. Essah, R., Anand, D., & Singh, S. (2023). Empirical Analysis of Existing Procurement and Crop Testing Process for Cocoa Beans in Ghana. In *Mobile Radio Communications and 5G Networks: Proceedings of Third MRCN 2022* (pp. 229-244). Singapore: Springer Nature Singapore.
4. Essah, R., Kaur, A., & Agbeko, M. (2022). A bibliometric review and future directions in Cloud Architecture and Security in Web of Science from 2008 to 2022. *Computer Integrated Manufacturing Systems*, *28*(12), 2184-2210.
5. Jain, S., & Essah, R. (2022, November). Movie recommendation using collaborative filtering to make accurate predictions. In *2022 International Conference on Advances in Computing, Communication and Materials (ICACCM)* (pp. 1-5). IEEE.
6. Essah, R., Tetteh, A., Baidoo, P. K., Duah, B., & Teye, E. Q. (2021). Information Processing in IoT Based Manufacturing Monitoring System. *International Journal of Research in Engineering, Science and Management*, *4*(8), 168-177.
7. Gyane, S. O. J., Essah, R., Senior, I. A. A., & Tetteh, A. (2021). Reliability and efficiency of computerized systems for admission into colleges of education affiliated with the university of cape coast. *Asian Journal of Research in Computer Science*, *12*(4), 84-96.
8. Essah, R., & Anand, D. (2021). Proposal on automatic cocoa quality testing and procurement in Ghana. *Asian Journal of Research in Computer Science*, *12*(4), 132-146.
9. Tetteh, A., Essah, R., Badhon, A. J., Asante, Y. A., & Patrick, A. B. (2021). A Statistical Study into Network Security Issues of IT Companies in Accra. *Asian Journal of Research in Computer Science*, *12*(3), 1-13.
10. Asante, Y. A., & Essah, R. (2021). Comparative analysis of OSPFv3/IS-IS and RIPng/IS-IS mixed protocols for real-time applications in ipv6 communication networks. *Asian Journal of Research in Computer Science*, *12*(4), 111-131.
11. Bhattacharjee, S. B., Gangwar, S., Kumar, M., Saini, K., Saini, R., Chauhan, S., ... & Goyal, N. (2024). Original Research Article An efficient framework for secure data transmission using blockchain in IoT environment. *Journal of Autonomous Intelligence*, *7*(2).
12. Essah, R. (2021). The Role of Cloud Computing Fashionable the Strategic Growth of Business Enterprises in India. *Asian Journal of Research in Computer Science*, *12*(1), 37-48.
13. Essah, R., Boam, J. K., Faustino, A., & Tetteh, A. Assessment of Crop Quality Using Machine Learning Techniques for Smart Farming.
14. Anveshini, D., & Shetty, S. P. (2016). Investigating the Impact of Simulation Time on Convergence Activity & Duration of EIGRP , OSPF Routing Protocols under Link Failure and Link Recovery in WAN Using OPNET Modeler. International Journal of Computer Science Trends and Technology (IJCST), 4(5), 38–42.
15. Asher, P. (2015). Comprehensive Analysis of Dynamic Routing Protocols in Computer Networks. International Journal of Computer Science and Information Technologies, 6(5), 4450–4455.
16. Chawda, K. and D. Gorana (2015). A survey of energy efficient routing protocol in MANET. Electronics and Communication Systems (ICECS), 2015 2nd International Conference on, IEEE.
17. Dangwal, K., & Kumar, V. (2014). Comparative Study of EIGRP AND RIP Using CISCO Packet Tracer. International Journal of Engineering Sciences & Emerging Technologies, 6(6), 475–480.
18. Deng, J., Wu, S., & Sun, K. (2014). Comparison of RIP , OSPF and EIGRP Routing Protocols based on OPNET. In Communication Networks (pp. 1–25).
19. Finardi, A. (2018). IoT Simulations with Cisco Packet Tracer. Helsinki Metropolia University of Applied Sciences.
20. Greenberg, A., Hjalmtysson, G., Maltz, D. A., Myers, A., Rexford, J., Xie, G., … Zhang, H. (2005). Public Review for A Clean Slate 4D Approach to Network Control and Management. ACM SIGCOMM Computer Communication Review, 35(5), 41–54.
21. Garg, P. and A. Gupta (2015). "Restoration Technique to Optimize Recovery Time for Efficient OSPF Network." Research Advances in the Integration of Big Data and Smart Computing: 64.
22. Gehlot Komal, NC Barwar (2014) Performance Evaluation of EIGRP and OSPF Routing Protocols in Real Time Applications. J. N. V. International Journal of Emerging

23. Hoang, T. D. (2015). "Deployment IPv6 over IPv4 network infrastructure."

24. Hanumanthappa, J., & Sridevi, M. D. H. (2010). Comparison between Performance Analysis of IPv6 in IPv4 Static Tunneling with Automatic 6 to 4 Tunneling in IPv4/IPv6 Transition Mechanism . Comparison and Contrast between Performance Analysis of IPv6 in IPv4 Static Tunneling with Automatic 6 to 4 Tunnel. Research Gate Publication, (June 2014), 1–13.

25. Jain, N., & Payal, A. (2020). Performance Evaluation of IPv6 Network for Real-Time Applications IS-ISv6 Routing Protocol on Riverbed Modeler. Procedia Computer Science: International Conference on Smart Sustainable Intelligent Computing and Applications under ICITETM2020, 173, 46–55. https://doi.org/10.1016/j.procs.2020.06.007

26. Jaiswal, R., Lokhande, S., Bakre, A., & Gutte, K. (2015). PERFORMANCE ANALYSIS OF IPv4 AND IPv6 INTERNET TRAFFIC. ICTACT Journal on Communication Technology, 6(4), 1–10. https://doi.org/10.21917/ijct.2015.0177

27. Lee, J., Bonnin, J., Member, S., & You, I. (2013). Comparative Handover Performance Analysis of IPv6 Mobility Management Protocols. IEEE Transactions on Industrial Electronics, 60(3), 1077–1088.

28. Maltz, D. A., Xie, G., Zhan, J., Zhang, H., & Greenberg, A. (2004). Routing Design in Operational Networks : A Look from the Inside. SIGCOMM, (9), 1–14.

29. Panford, J. K., & Kufuor, O. B. (2015). Comparative Analysis Of Convergence Times Between RIP And EIGRP Routing Protocols In A Network. Journal of Computer Science, 2(3), 1–11.

30. Pavani, M., Lakshmi, M. S., & Kumar, S. P. (2014). Dynamic Routing Protocols in TCP/IP. The International Journal Of Science & Technoledge, 2(5), 227–234.

31. Rakheja, P., Kaur, P., Gupta, A., & Sharma, A. (2012). Performance Analysis of RIP , OSPF , IGRP and EIGRP Routing Protocols in a Network. International Journal of Computer Applications, 48(18), 6–11.

32. Sandhu, P. S., Bhatia, K. S., & Kaur, H. (2013). Comparitive Study of Various Router Protocols. International Conference on Innovations in Engineering and Technology (ICIET'2013), 25–27. Retrieved from http://dx.doi.org/10.15242/IIE.E1213512

33. Sankar, D., & Lancaster, D. (2020). Routing Protocol Convergence Comparison using Simulation and Real Equipment. Advances in Communications, Computing, Networks and Security 10, 186–194.

34. Vetriselvan, V., Patil, P. R., & Mahendran, M. (2014). Survey on the RIP, OSPF, EIGRP Routing Protocols. (IJCSIT) International Journal of Computer Science and Information Technologies, 5(2), 1058–1065.

35. Vissicchio, S., Tilmans, O., Vanbever, L., & Rexford, J. (2015). Central Control Over Distributed Routing. SIGCOMM, 15, 43–56. Retrieved from http://dx.doi.org/10.1145/2785956.2787497

36. Xu, D., & Trajkovi, L. (2012). Performance Analysis of RIP, EIGRP, and OSPF using OPNET. Research Gate Publication, (5), 1–5. Retrieved from https://www.researchgate.net/publication/267385378