PROJECT 3

Literature Review and Design Solution

Group Members:

Okuhle Salelo 222384085

Yenziwe Biyela

Nokuthula Ndlovu

Abigail V Chauke

Nokuthula Ndlovu

Enhancing network of a Holdings company by implementing cybersecurity measures, to prevent unauthorized access and bandwidth misuse.

1. Introduction

In the age of digital transformation, Cloud computing, enabling businesses to expand operations and reduce costs, presents new cybersecurity threats due to distributed responsibility models. Multi-cloud setups, leveraging services from multiple providers, make security management more challenging due to insufficient policies, enhanced attack surfaces, and integration obstacles. Cyberattacks are rapidly evolving, using advanced techniques like AI and social engineering. With cloud-based data, the need for secure network design and real-time threat detection is increasing.

This literature review critiques previous research on cybersecurity in cloud and network ecosystems, focusing on risk prevent line with current cybersecurity measures and capable of addressing real-world threats nation, threat intelligence, and trust models. It identifies weaknesses, risks, and limitations in current frameworks, and suggests designing secure network structures using simulation programs like cisco packet tracer that comply with current cybersecurity measures and effectively combat real-world threats.

2. Thematic Review

2.1 Vulnerability Remediation and Management

Cloud computing raises data security risks due to distant servers and shared infrastructure, making sensitive information vulnerable. Businesses and individuals handling sensitive data should be cautious. Strong security measures like encryption, multi-factor authentication, and adherence to data protection laws are crucial to control these risks and maintain confidence in cloud systems. The universal thread is that vulnerabilities must be detected and remediated before they can be exploited. According to Khan and Anis (2022), organizations transitioning to cloud infrastructures usually are vulnerable to misconfigured servers, weak access controls, and open endpoints. Their solution is a mix of automated vulnerability scanners and manual penetration testing, which allows organizations to detect vulnerabilities beforehand. Secondly, the auto-remediation actions included enable systems to automatically respond to threats without requiring a human touch, hence limiting downtime and exposure.

2.2 AI and Machine Learning-Based Real-Time Threat Detection

One of the overarching themes is the use of artificial intelligence (AI) and machine learning (ML) for threat detection. Such technologies make it possible for systems to monitor activity in real-time, detect anomalies, and predict threats based on patterns that have been learned from experience. In the work of Khan and Anis, AI technologies caused a reduction of 40–45% in detection time, which speaks to their promise of enhancing system responsiveness and compensating for attacks. This is particularly a germane theme in dynamic cloud environments where threats evolve more quickly than traditional defences can react.

2.3 Trust and Privacy Preservation in Multi-Cloud Environments

Udeh (2025) introduces the theme of decentralized trust using blockchain technology. In multi-cloud situations where varying vendors may handle data accuracy, transparency, and user privacy matter. The proposed blockchain model uses smart contracts to secure data ownership and access rights while logging interactions on an immutable blockchain. It provides transparency, auditability, and regulation compliance, for example, under the GDPR. Technical security is not in focus solely here, but on establishing provable trust among users and service providers.

These papers explore the integration of AI, blockchain, and smart contracts into current systems to enhance security mechanisms, despite challenges like legacy systems, budget constraints, and skill gaps. Udeh's work highlights the lack of empirical validation in theoretical proposals like blockchain models, which are not tested in specific environments, and the absence of comprehensive benchmarks and test case deployments in Khan and Anis.

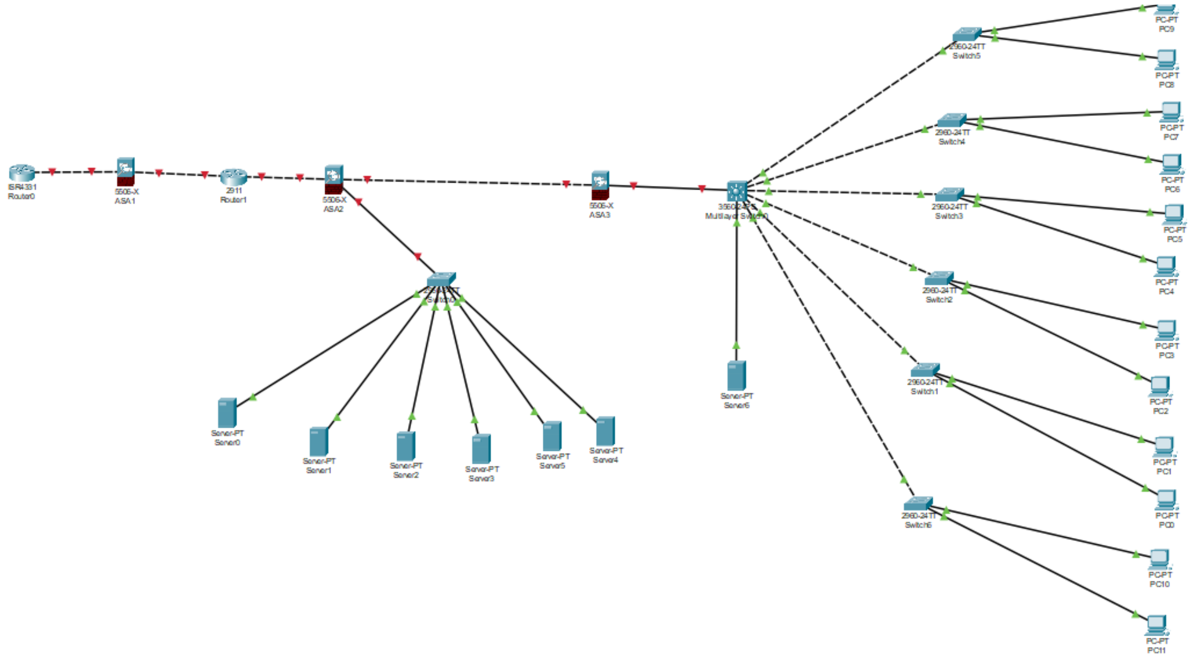
3. Summary and Design

The literature highlights challenges in safeguarding cloud and network environments due to increased exposure to threats, cyberattacks, sophisticated threats, and inadequate detection mechanisms. The absence of standardized security policies in multi-cloud systems, privacy and trust concerns, and limitations in technology adoption make it difficult to implement these technologies effectively. AI and blockchain offer potential but require significant resources, specialized personnel, and IT infrastructure recovery, making them difficult for most businesses to adopt.

Several design improvements can be incorporated into the Packet Tracer architecture considering all of these difficulties, this will include the implementation of a Layered Security, Demilitarized Zone (DMZ), Simulated Real-Time Monitoring, Blockchain-Inspired Rule Enforcement, Encryption and Secure Communication, Cloud Service Provider Simulation, and Role-Based Access Control. These measures aim to prevent attackers from accessing critical resources, isolate internal networks from external access, and ensure secure communication channels. The system also supports simulated user levels and limiting privileges, enhancing overall security.

According to the publications, measures made regarding Packet Tracer architecture can improve cloud security and network resilience. For instance the use of Syslog and SNMP for logging and alerting, integrating local networks for cloud segments, and segmenting networks using VLANs. One important resilience technique for cloud systems is availability, which is achieved by establishing redundant connections and failover procedures. Compliance considerations are also taken into account, utilizing security best practices such as access limitation, encryption, and in-depth logging that are recommended by models such as GDPR. The goal of these design decisions is to get ready for future scalability and multi-cloud scalability.

4. Design



5. References

Sharmila, R. & Sabitha, J., 2023 International Journal of Humanities & Social Science Studies (IJHSSS), 12(1), p.163.

Anastasiadis, C., Sarigiannidis, P., Lagkas, T., & Vlachos, D., 2022. Implementation Aspects of Smart Grids Cyber-Security Cross-Layered Framework for Critical Infrastructure Operation. Applied Sciences, 12(14), p.6868. https://doi.org/10.3390/app12146868

Alabady, S., 2009. Design and Implementation of a Network Security Model for Cooperative Network. International Arab Journal of e-Technology, 1(2), pp.26–36

Kadry, S., Khaled, S. & Hassan, W., 2008. Design and Implementation of System and Network Security for an Enterprise with Worldwide Branches. Journal of Applied Sciences Research, 4(10), pp.1361–1370

- Kshetri, N. “The global cybercrime industry: economic, institutional and strategic perspectives” , Springer, 2010.

- Dupont A. Time to attack cybercrime with a strong security policy. WWW page, October 2010.

- Fong, E., and Okun, V. “Web Application Scanners: Definitions and Functions”. In System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on (2007).

- M. A. Aladwani, “Thinking Big for Small Businesses. What the EU does for SMEs,” Int. J. Inf. Manag. 21, vol. 21, pp. 213–225, 2001, [Online]. Available: https://www.centralbank.ie/publications/Pages/SMEMarketReports.aspx%0Ahttps://ec.europa. eu/jrc/sites/jrcsh/files/annual_report_-_eu_smes_2015-16.pdf%0Ahttp://0-search.proquest.com.pugwash.lib.warwick.ac.uk/docview/237066570?accountid=14888.

- Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. Computers & Security, 45, 58–74. doi:10.1016/j.cose.2014.05.006

- Li, J. (2015). The research and application of multi-firewall technology in enterprise network security. International Journal of Security and Its Applications, 9(5), 153–162. doi:10.14257/ijsia.2015.9.5.16

- Maisey, M. (2014). Moving to analysis-led cyber-security. Network Security, 2014(5), 5–12. doi:10.1016/ S1353-4858(14)70049-2

[10:36 am, 14/05/2025] YS: Gordon, L.A., Loeb, M.P., Lucyshyn, W. & Zhou, L., 2015. Increasing cybersecurity investments in private sector firms. Journal of Cybersecurity, 1(1), https://doi.org/10.1093/cybsec/tyv011.
Karanja, M. & Smith, L., 2021. A Framework for Enhancing Cybersecurity in Small and Medium Enterprises (SMEs).

[10:41 am, 14/05/2025] YS: G. Culot, G. Nassimbeni, M. Podrecca and M. Sartor, "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda", TQM J, vol. 33, no. 7, pp. 76-105, Jan. 2021.