JOURNAL INNOVATIONS COMPUTER SCIENCE
E-ISSN: 2961-970X, P-ISSN: 2961-9718
Volume 4 Number 2, November 2025, pp 230-241.
DOI: https://doi.org/10.56347/jics.v4i2.318

Implementation of Defense In Depth and IAM Best Practices Based on Segmented VPC Architecture Using Amazon Web Services (AWS) for Small Business Network Security

Muhamad Umar Hassan Asrori [a*], Fadillah Said [b]
[a*,b] Informatics Engineering Study Program, Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, East Jakarta City, Special Capital Region of Jakarta, Indonesia.

ABSTRACT
This study presents the design, implementation, and validation of a cloud security architecture on Amazon Web Services (AWS) that integrates *Defense in Depth* strategies with *Identity and Access Management (IAM) Best Practices*, tailored for small and medium-sized enterprises (SMEs). Using the AWS Free Tier, an experimental cloud infrastructure was constructed to evaluate the effectiveness of multi-layered protection encompassing network segmentation, least-privilege access control, and real-time monitoring. The architecture employed a segmented Virtual Private Cloud (VPC) with public and private subnets, controlled by Security Groups (SGs) and Network Access Control Lists (NACLs), while IAM policies and Multi-Factor Authentication (MFA) enforced identity-level security. Centralized monitoring through CloudTrail and CloudWatch enabled anomaly detection and event logging with high accuracy. Test results showed that unauthorized access was effectively blocked, suspicious activities were detected promptly, and all administrative actions were recorded reliably. The findings indicate that combining layered network defenses and IAM governance significantly enhances the resilience, visibility, and security posture of SMEs adopting AWS environments. Beyond its technical effectiveness, the model offers scalability, auditability, and cost-efficiency—demonstrating that enterprise-grade protection can be achieved even within the resource constraints of SMEs. Future work is encouraged to integrate automation and advanced AWS tools such as GuardDuty and Config to strengthen real-world adaptability and compliance.

ARTICLE HISTORY
Received 27 July 2025
Accepted 30 October 2025
Published 30 November 2025

KEYWORDS
Cloud Security; AWS; Defense in Depth; IAM; SMEs.

1. Introduction

The acceleration of digital transformation has compelled small and medium-sized enterprises (SMEs) to adopt cloud computing as a core infrastructure strategy due to its flexibility, scalability, and cost efficiency (Check Point Research, 2023; Kominfo, 2023). Among the available platforms, Amazon Web Services (AWS) has emerged as a preferred choice for SMEs, offering extensive infrastructure and managed services capable of supporting business operations at varying scales (Amazon Web Services, 2023a). Despite these advantages, the rapid migration to the cloud has exposed new security challenges. Many SMEs still lack the expertise, budget, and structured policies necessary to safeguard cloud assets effectively, resulting in

CONTACT Muhamad Umar Hassan Asrori muh.umar.hassan.18@gmail.com Informatics Engineering Study Program, Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, East Jakarta City, Special Capital Region of Jakarta, Indonesia.

misconfigurations, weak access control, and inadequate monitoring practices (Reece *et al*., 2023; Darmawan & Nugroho, 2020). Recent reports show that cyberattacks targeting SMEs have increased by 38% globally, reflecting how insufficient cybersecurity governance continues to leave cloud environments vulnerable (Check Point Research, 2023).

The primary issue lies not in the adoption of cloud technology itself but in the absence of a layered and systematic defense strategy. Many organizations deploy AWS environments using default configurations without implementing a defense-in-depth architecture or adhering to Identity and Access Management (IAM) best practices (Susanti & Pratama, 2022; Sulaiman & Setiawan, 2021). The defense-in-depth principle emphasizes the deployment of multiple protective layers—network segmentation, strict access control, traffic inspection, and activity monitoring—to ensure that the compromise of one control does not endanger the entire system (Bhattacharyya & Nair, 2022; Shaw *et al*., 2022; Mukherjee, 2024). Complementary to this, IAM serves as the foundation of cloud security, defining who can access specific resources and under what conditions (Amazon Web Services, 2023b; Gudelli, 2022; Wulandari & Puspitasari, 2022). AWS recommends the least privilege principle, multifactor authentication (MFA), and continuous auditing through CloudTrail and CloudWatch to maintain access integrity (Amazon Web Services, 2023c, 2023d; Afriansyah & Huda, 2023). When implemented jointly, defense-in-depth and IAM frameworks reinforce each other by establishing both perimeter and identity-level security, forming a robust safeguard for multi-layered cloud environments (Anthony, 2018; Kanikathottu, 2024; NIST, 2022).

While prior studies have addressed individual aspects of cloud security—such as virtual private cloud (VPC) design (Aditya & Ramadhan, 2022) and IAM enforcement (Sulaiman & Setiawan, 2021; Wulandari & Puspitasari, 2022)—few have combined these approaches into a unified and cost-effective model suitable for SMEs. Most existing works focus either on theoretical frameworks without technical validation or on specific configurations that overlook access orchestration and monitoring integration (Saputra & Dwi, 2023; Susanti & Pratama, 2022). Consequently, there remains a practical gap in constructing an AWS-based network security model that integrates defense-in-depth principles and IAM best practices using free-tier or low-cost services. This study aims to address that gap by developing and validating a layered cloud security architecture on AWS that merges defense-in-depth mechanisms with IAM-based access governance. The design leverages VPC segmentation, role-based access control, real-time activity logging, and monitoring through AWS native tools—particularly CloudTrail and CloudWatch—to demonstrate measurable resilience against simulated attacks. By using an affordable and replicable configuration, this work intends to provide SMEs with a tested reference model that enhances network protection while maintaining cost efficiency. Ultimately, the research contributes a practical blueprint for secure AWS deployment and an empirical basis for advancing SME cloud security strategies grounded in both policy and technical implementation.

2. Methodology

This research employed an experimental approach to construct and simulate a representative cloud infrastructure for small and medium-sized enterprises (SMEs) on Amazon Web Services (AWS) using the AWS Free Tier. This approach was selected because it allows direct validation of the effectiveness of layered network security within

a controlled environment and adheres to the principles of systematic and transparent experimental design in software engineering (Kitchenham, 2007). The experimental framework focused on building a segmented, secure, and cost-efficient infrastructure, as illustrated in **Figure 1**, which presents the AWS network topology designed for this study. The topology consists of a Virtual Private Cloud (VPC) with a CIDR block of [10.0.0.0/16], divided into one public subnet (10.0.1.0/24) hosting the Application Load Balancer (ALB) and two private subnets (10.0.2.0/24 and 10.0.3.0/24) running EC2 instances for application processing. Routing was configured using an Internet Gateway (IGW) for external communication and a NAT Gateway for secure outbound traffic from private subnets. Each resource was tagged for operational management and cost transparency, while all data stored on Elastic Block Store (EBS) volumes was encrypted by default (Amazon Web Services, 2023a; Shields, 2022). The architectural design followed AWS best practices emphasizing segmentation and least-privilege configuration (Kanikathottu, 2024; Anthony, 2018).

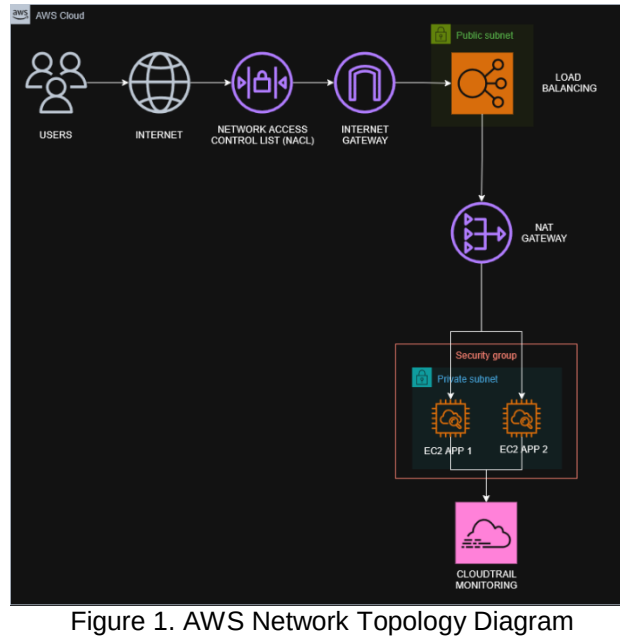

Figure 1. AWS Network Topology Diagram

The architecture includes a single VPC connected to an Internet Gateway and NAT Gateway. The ALB in the public subnet routes traffic to EC2 instances in private subnets. Security Groups (SGs) restrict inbound ports to 80/443, while Network Access Control Lists (NACLs) regulate subnet-level communication. CloudTrail and CloudWatch provide centralized logging and performance monitoring. Security controls were implemented using the Defense-in-Depth strategy, applying multiple security layers across network, host, and identity domains (Mukherjee, 2024; Bhattacharyya & Nair, 2022; Shaw *et al*., 2022). At the network layer, SGs and NACLs were configured with strict inbound and outbound policies to prevent unauthorized access and reduce the risk of lateral movement (Alavizadeh *et al*., 2020). For identity and access management, AWS Identity and Access Management (IAM) policies were established based on the NIST (2022) Cybersecurity Framework and AWS IAM best practices (Amazon Web Services, 2023b, 2023c). Three IAM users—*admin*, *developer*, and *monitoring*—were created with custom JSON policies applying the least-privilege principle, where each user was granted only the specific permissions required for their role (Sulaiman & Setiawan, 2021; Wulandari & Puspitasari, 2022). Multi-Factor Authentication (MFA) was enforced for all users to mitigate credential-based threats

(Machado, 2025), while IAM roles and policies were aligned with AWS DevSecOps pipeline security models (Tolt *et al*., 2023). Fine-grained role assignments and Infrastructure-as-Code (IaC) policy validation were applied to enhance automation security, reflecting recent empirical research on IaC security management (Verdet *et al*., 2023).

Monitoring and evaluation processes were conducted using AWS CloudTrail and CloudWatch to ensure every administrative and API activity was logged and analyzed (Afriansyah & Huda, 2023; Amazon Web Services, 2023d, 2023e). CloudTrail was configured to capture all API calls and store logs in an encrypted S3 bucket with public access blocked, while CloudWatch metrics and alarms were designed to detect anomalous login attempts—triggering notifications after five failed ConsoleLogin attempts within five minutes. Validation and testing were carried out through three scenarios: (1) Network and remote access testing, involving verification of public and private IP isolation and SSH denial from unauthorized IPs; (2) IAM management testing, simulating failed logins and unauthorized policy modifications to validate least-privilege enforcement; and (3) logging validation, ensuring all events were accurately recorded, including denial responses and administrative actions. Performance evaluation focused on three quantitative indicators: rejection rate (the percentage of unauthorized access attempts successfully blocked), detection time (the average duration between suspicious activity and alarm notification), and log accuracy (the completeness and reliability of event records). The system achieved high rejection and detection rates, validating the synchronization between IAM governance and layered network controls. These outcomes are consistent with prior findings emphasizing the role of integrated monitoring and automation in securing cloud-based SMEs (Sarimole & Firdaus, 2020; Reece *et al*., 2023; Saputra & Dwi, 2023). Moreover, the applied configuration aligns with AWS Security Best Practices (Amazon Web Services, 2023f), the *AWS Security Cookbook* (Kanikathottu, 2024), and broader cybersecurity frameworks encouraging defense layering and adaptive risk management (Susanti & Pratama, 2022; Kominfo, 2023). This methodological implementation demonstrates that by combining systematic configuration, identity-centric access control, continuous monitoring, and evidence-based evaluation, AWS Free Tier services can effectively deliver enterprise-grade security to SMEs while maintaining affordability and replicability, reinforcing both academic and applied perspectives in cloud security design (Shields, 2022; Darmawan & Nugroho, 2020; Gudelli, 2022).

3. Results and System Validation

The implementation of the cloud security system using the *Defense in Depth* approach combined with *Identity and Access Management (IAM) Best Practices* demonstrated success in establishing a robust, segmented, and auditable cloud infrastructure. The environment was designed using a single *Virtual Private Cloud* (VPC) with a CIDR block of 10.0.0.0/16, divided into one *Public Subnet* (10.0.1.0/24) hosting the *Application Load Balancer* (ALB) and one *Private Subnet* (10.0.2.0/24) containing EC2 instances functioning as the application server. The testing confirmed that each security layer operated as designed. The EC2 instance within the private subnet was fully isolated from direct internet access and could only be reached through the *Network Load Balancer* (NLB) positioned in the public subnet, ensuring that no public IP was exposed and minimizing the attack surface (Figure 2. EC2 Instance Isolation in the Private Subnet and Figure 3. Access to Private Instance via NLB).

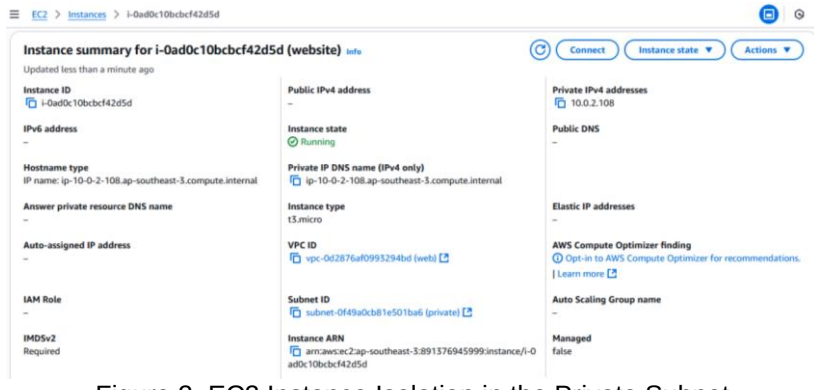

Figure 2. EC2 Instance Isolation in the Private Subnet

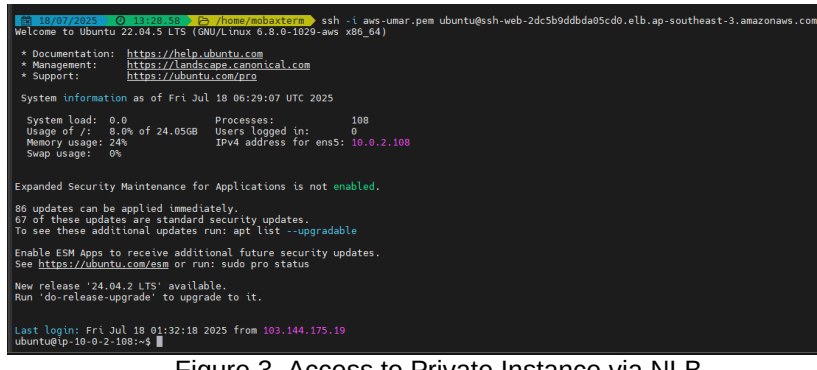

Figure 3. Access to Private Instance via NLB

Further validation showed that *Security Groups (SG)* and *Network Access Control Lists (NACL)* effectively blocked unauthorized connections between subnets, confirming that the network segmentation functioned optimally and that traffic filtering was enforced as intended (Figure 4. AWS Security Group Configuration and Figure 5. AWS Network Access Control List Configuration).

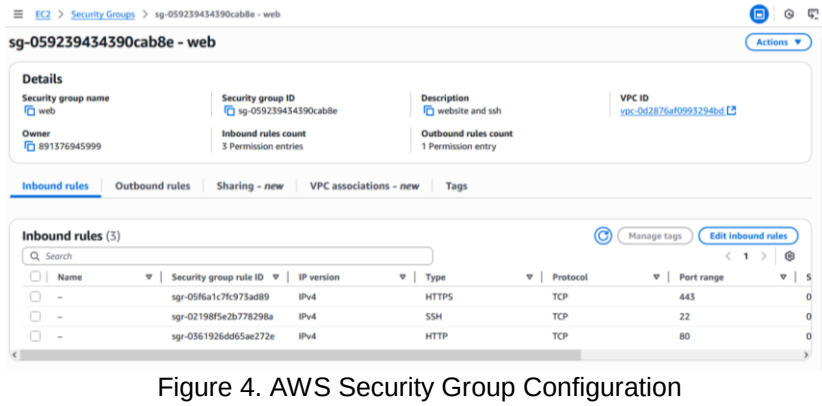

Figure 4. AWS Security Group Configuration

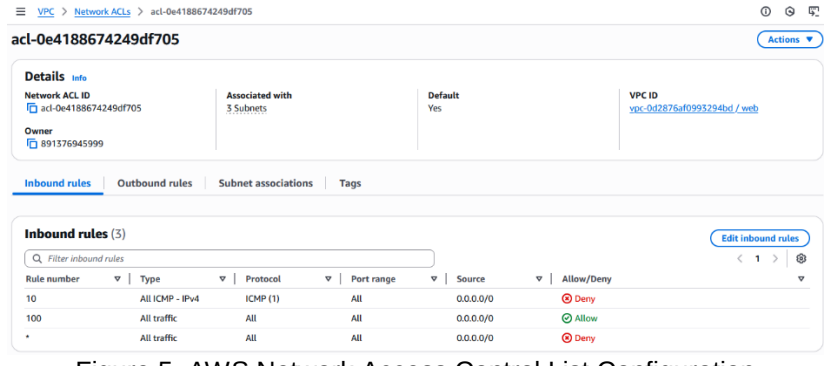

Figure 5. AWS Network Access Control List Configuration

Subsequent IAM testing demonstrated that the *least privilege* principle was implemented successfully. When a limited-permission IAM user attempted to stop or terminate an EC2 instance, access was automatically denied and recorded in *AWS CloudTrail* (Figure 6. Ping Test from Client and Figure 7. Access Denial for Monitoring User on EC2 Instance).

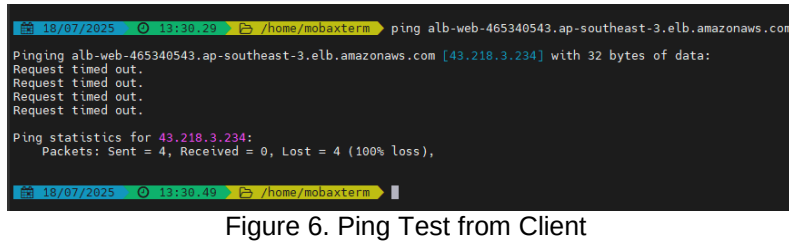

Figure 6. Ping Test from Client

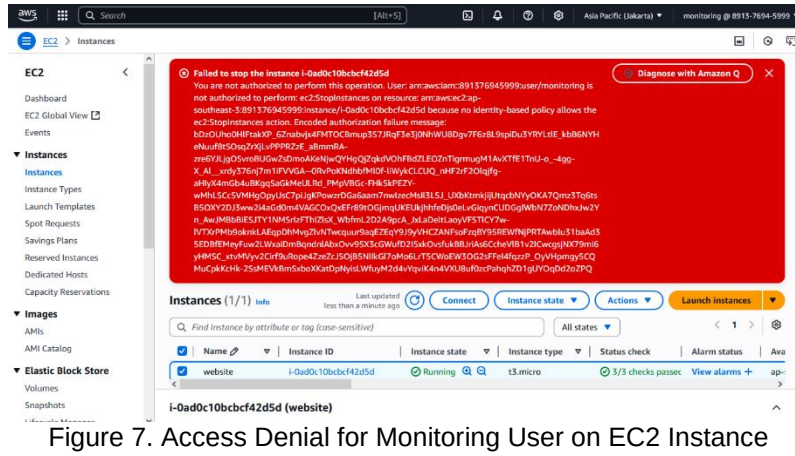

Figure 7. Access Denial for Monitoring User on EC2 Instance

The *logging* and *monitoring* mechanisms also performed effectively, with *Amazon CloudWatch* detecting failed login attempts and automatically generating alerts when more than five failures occurred within five minutes (Figure 8. Detection of Failed Login Attempts via CloudWatch).

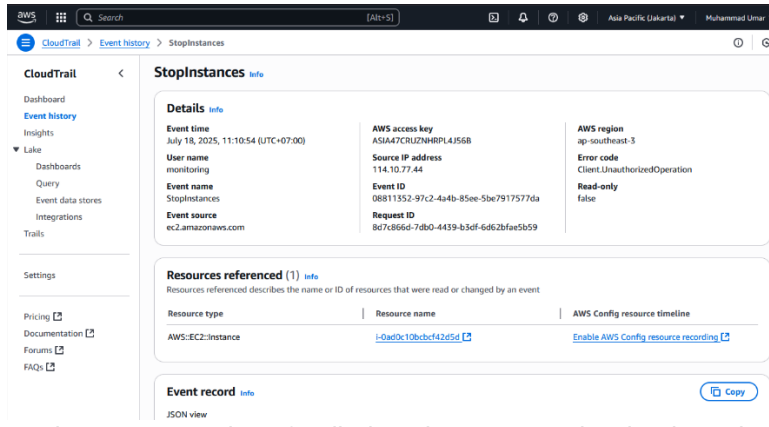

Figure 8. Detection of Failed Login Attempts via CloudWatch

The outcomes of all security tests are summarized in Table 1. Summary of Testing Scenarios and Validation Results, showing consistent functionality across all layers.

Table 1. Summary of Testing Scenarios and Validation Results

No	Testing Scenario	Objective	Test Result	Log and Detection Evidence
1	Unauthorized inter-subnet access	Validate network segmentation (SG & NACL)	Access denied; connection failed	Figure 6
2	Unauthorized user login	Validate IAM Role & Policy enforcement	Access denied	Figure 7
3	Suspicious login activity	Ensure CloudTrail & CloudWatch detect anomalies	Failed login activity recorded	Figure 8
4	Private EC2 remote access via NLB	Validate indirect access without public IP exposure	Website accessible via NLB and ALB	Figure 9 and Figure 10

In addition to validating the security structure, the functionality testing confirmed that the designed architecture remained efficient and stable. The NGINX-based web application installed on the private EC2 instance operated smoothly and was accessed exclusively through the ALB, demonstrating the *Load Balancer's* effectiveness in managing traffic distribution without exposing backend servers (Figure 9 and Figure 10).

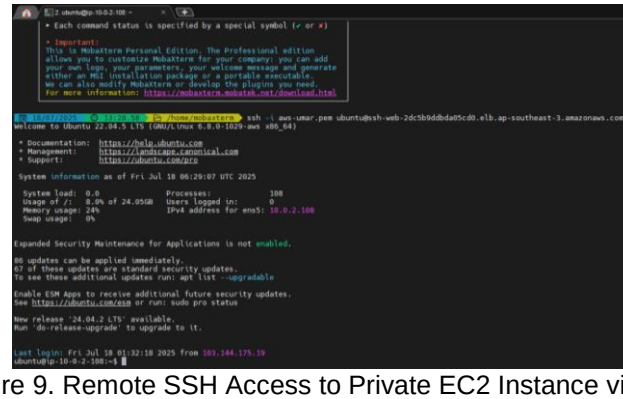

Figure 9. Remote SSH Access to Private EC2 Instance via NLB

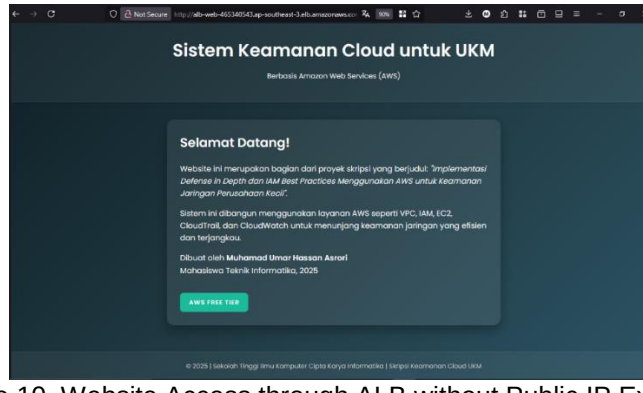

Figure 10. Website Access through ALB without Public IP Exposure

The performance evaluation indicated a high rejection rate for unauthorized access attempts, rapid detection time for anomalous activities, and consistent log accuracy across *AWS CloudTrail*. Overall, the findings affirm that integrating *Defense in Depth* and *IAM Best Practices* within AWS services significantly enhances cloud network security resilience. The approach proved cost-efficient through the use of *AWS Free Tier*, auditable, and replicable, providing an effective and practical security model for SMEs to adopt in mitigating modern cybersecurity threats.

4. Discussion

The implementation of the cloud security architecture that integrates *Defense in Depth* principles and *AWS IAM Best Practices* has proven effective in enhancing organizational security posture by combining network segmentation, identity management, and continuous monitoring. Each layer of defense contributes distinct protection mechanisms aligned with industry frameworks such as the NIST Cybersecurity Framework (NIST, 2022) and AWS Security Guidelines (Amazon Web Services, 2023). The network segmentation implemented through *Virtual Private Cloud (VPC)* ensures strict control over data flow and entry points. By isolating the *Application Load Balancer (ALB)* within the public subnet and application servers within private subnets, the attack surface is significantly reduced—an approach consistent with findings by Aditya and Ramadhan (2022), who emphasized subnet isolation as a core network defense measure. The enforcement of *Security Groups (SG)* and *Network Access Control Lists (NACL)* further validated network integrity by filtering traffic at multiple levels, consistent with *Defense in Depth* practices discussed by Shaw, Rogers, and Kumar (2022) and Saputra and Dwi (2023). Equally critical, the application of IAM policies reinforced internal security through precise access control mechanisms. Following AWS and NIST recommendations, the *least privilege* principle ensures that users operate strictly within the boundaries of their assigned roles (Amazon Web Services, 2023; Wulandari & Puspitasari, 2022). Multi-Factor Authentication (MFA) implementation, as advised by Machado (2025), added an essential layer of defense against brute-force and credential-based attacks, thereby minimizing insider threats. The combination of fine-grained IAM roles and JSON-based access policies mirrors best practices highlighted by Gudelli (2022) and Tolt *et al*. (2023), demonstrating that properly configured IAM systems can effectively mitigate unauthorized privilege escalation. Meanwhile, continuous monitoring through *AWS CloudTrail* and *Amazon CloudWatch* provided visibility into system operations and acted as an active threat detection system. This aligns with the work of

Afriansyah and Huda (2023), who highlighted the capability of integrated monitoring tools in detecting anomalies and supporting incident response in real-time. The implemented architecture allowed early detection of suspicious actions such as failed logins or unauthorized attempts to modify configurations—capabilities identified by Bhattacharyya and Nair (2022) as essential components of a proactive cybersecurity strategy. When compared with traditional on-premises security setups, this solution offers significant operational advantages. It eliminates the capital expenses associated with physical infrastructure while introducing scalable and flexible protection measures tailored for SMEs (Reece *et al*., 2023; Kanikathottu, 2024). Compared to standard cloud deployments lacking layered defenses, this architecture provides more granular control, stronger authentication policies, and real-time visibility into security events (Mukherjee, 2024). However, certain trade-offs remain. While *AWS Free Tier* demonstrates cost efficiency for prototyping, scaling the model into production may incur additional costs for services such as NAT Gateways and continuous monitoring tools (Kominfo, 2023). The complexity of implementing detailed IAM policies also introduces administrative overhead and requires specialized expertise (Darmawan & Nugroho, 2020). Additionally, routing traffic through ALB or NLB may result in minimal latency—although this effect is negligible for SME-scale environments (Alavizadeh *et al*., 2020).

In terms of scalability, the modular architecture of the segmented VPC allows SMEs to expand resources and services without compromising existing security controls, supporting long-term adaptability (Anthony, 2018; Shields, 2022). However, the architecture has limitations in addressing sophisticated threats such as supply chain compromises or lateral movement attacks through application vulnerabilities. These risks could be further mitigated by integrating advanced AWS security services such as *GuardDuty*, *AWS Inspector*, or *AWS Security Hub* (Amazon Web Services, 2023; Bhattacharyya & Nair, 2022). As noted by Susanti and Pratama (2022), continuous improvement and threat intelligence integration are essential to achieving a more comprehensive security posture. Overall, this discussion reaffirms that combining *Defense in Depth* and *IAM Best Practices* on AWS provides a balanced and sustainable security framework that enhances resilience, visibility, and operational agility. The approach not only strengthens the technical foundation for SMEs but also aligns with global cybersecurity standards, offering a replicable model for secure and cost-effective cloud adoption in an increasingly complex digital threat landscape.

5. Conclusion

The study demonstrates that integrating *Defense in Depth* strategies with *Identity and Access Management (IAM) Best Practices* within an AWS-based cloud infrastructure can significantly enhance network security and operational resilience. The structured implementation within the AWS Free Tier environment validated the system's ability to reject unauthorized access attempts and detect suspicious activities in real time. The results confirmed that a combination of network segmentation, least-privilege access control, and centralized monitoring provides a robust, multi-layered defense mechanism that aligns with modern cybersecurity standards. Beyond its technical success, this approach emphasizes cost efficiency, scalability, and adaptability—making it particularly relevant for small and medium-sized enterprises (SMEs) that require secure yet affordable cloud solutions. For service-oriented SMEs such as consulting firms, enforcing strict IAM policies is essential to safeguard sensitive data, while for e-commerce SMEs, a segmented architecture with load balancing plays a critical role in mitigating exposure to external threats.

Although this study achieved its objectives within a controlled simulation, it acknowledges certain limitations, such as the absence of external penetration testing and advanced threat simulation. Future research is recommended to integrate automated threat detection and compliance tools, including *AWS GuardDuty* for intelligent anomaly analysis and *AWS Config* for automated policy enforcement. Expanding the framework to include *Infrastructure as Code (IaC)* practices using *AWS CloudFormation* or *Terraform* could further enhance consistency, scalability, and reproducibility. Moreover, incorporating incident response simulations and automated remediation workflows would strengthen the system's ability to withstand real-world security incidents, ensuring the model remains both practical and resilient for evolving SME cybersecurity needs.

Acknowledgment

All praise and gratitude are devoted to Allah Subhanahu Wa Ta'ala, who has granted the author mercy, health, and ease throughout the completion of this research, allowing it to develop into a comprehensive scientific work. Without His guidance and blessings, none of these efforts would have been possible. The author sincerely expresses deep appreciation to the *Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika (STIKOM CKI)* for its academic support, research facilities, and conducive learning environment. Special thanks are extended to Mr. Fadillah Said, S.Kom., M.Kom., the supervising lecturer, for his invaluable guidance, advice, and constructive feedback throughout the writing and research process. The author also extends heartfelt gratitude to all lecturers and staff of STIKOM CKI for the knowledge, experience, and encouragement they have provided, as well as to fellow students who have been valuable partners in discussion and knowledge sharing during the course of study. Appreciation is further given to the Small and Medium Enterprise (SME) community, whose real-world challenges and needs in adopting cloud-based network security inspired the focus of this research. On a personal note, the author expresses profound gratitude to his beloved wife for her unwavering patience, prayers, and emotional support throughout this academic journey. Special thanks are also dedicated to the author's 9-month-old child, whose presence has been a source of boundless motivation and joy during the completion of this final project. May every form of support, prayer, and goodwill extended be rewarded by Allah Subhanahu Wa Ta'ala with abundant mercy and blessings.

References

Aditya, R., & Ramadhan, D. (2022). Penerapan keamanan jaringan Virtual Private Cloud (VPC) menggunakan firewall rule dan access control list. *Jurnal Teknologi dan Sistem Komputer, 10*(2), 135–142. https://doi.org/10.14710/jtsiskom.10.2.135-142

Afriansyah, A., & Huda, N. (2023). Implementasi CloudTrail dan CloudWatch untuk deteksi ancaman siber pada infrastruktur AWS. *Jurnal Teknologi Informasi dan Ilmu Komputer, 11*(1), 55–62. https://doi.org/10.14710/jtik.11.1.55-62

Alavizadeh, H., Aref, S., Kim, D. S., & Jang-Jaccard, J. (2020). *Evaluating the security and economic effects of moving target defense techniques on the cloud.* arXiv. https://doi.org/10.48550/arXiv.2009.02030

Amazon Web Services. (2023). *Amazon VPC documentation.* https://docs.aws.amazon.com/vpc

Amazon Web Services. (2023). *AWS identity and access management user guide.* https://docs.aws.amazon.com/IAM/latest/UserGuide

Amazon Web Services. (2023). *AWS security best practices.* https://docs.aws.amazon.com

Amazon Web Services. (2023). *Logging API activity with AWS CloudTrail.* https://docs.aws.amazon.com/cloudtrail

Amazon Web Services. (2023). *Monitoring cloud resources using Amazon CloudWatch.* https://docs.aws.amazon.com/cloudwatch

Amazon Web Services. (2023). *Security best practices in IAM.* https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

Anthony, A. (2018). *AWS: Security best practices on AWS.* Packt Publishing.

Bhattacharyya, A., & Nair, A. (2022). *Defense-in-depth strategies for zero trust security models.* ResearchGate. https://www.researchgate.net/publication/364910753

Check Point Research. (2023). *Cyber attack trends: 2023 mid-year report.* https://research.checkpoint.com

Darmawan, R., & Nugroho, Y. (2020). Implementasi keamanan IAM pada infrastruktur cloud menggunakan AWS. *Jurnal Informatika, 14*(2), 122–130. https://doi.org/10.30591/ji.v14i2.1821

Gudelli, V. R. (2022). Data encryption and IAM policies: Best practices for AWS ecosystems. *CNDR Journal, 2*(2).

Kanikathottu, H. (2024). *AWS security cookbook: Practical solutions for securing AWS cloud infrastructure.* Packt Publishing.

Kitchenham, B. (2007). *Guidelines for performing systematic literature reviews in software engineering.* EBSE Technical Report.

Kominfo. (2023). *Keamanan siber di era cloud computing.* https://kominfo.go.id

Machado, L. (2025). *AWS IAM advanced best practices.* AWS Community Blog. https://aws.amazon.com/blogs/security/aws-iam-advanced-best-practices

Mukherjee, A. (2024). *The complete guide to defense in depth.* Packt Publishing.

National Institute of Standards and Technology. (2022). *Cybersecurity framework.* https://www.nist.gov/cyberframework

Reece, M., Lander, T., & Yager, A. R. (2023). *Systemic risk and vulnerability analysis of multi-cloud environments.* arXiv. https://doi.org/10.48550/arXiv.2306.11528

Sarimole, M., & Firdaus, H. R. (2020). Implementasi IoT dalam pengendalian keamanan gudang menggunakan mikrokontroler di PT Netsolution. *CKI On Spot, 13*(2), 45–51.

Saputra, H., & Dwi, L. (2023). Perancangan sistem keamanan berlapis pada cloud computing menggunakan defense in depth. *Jurnal Rekayasa Sistem dan Teknologi Informasi, 12*(1), 21–30.

Shields, D. (2022). *AWS security.* Manning Publications.

Sulaiman, F., & Setiawan, A. (2021). Implementasi IAM pada AWS untuk meningkatkan keamanan sistem cloud. *Jurnal Teknologi dan Sistem Komputer, 9*(1), 15–22. https://doi.org/10.14710/jtsiskom.9.1.15-22

Susanti, D., & Pratama, R. (2022). Analisis strategi defense in depth pada keamanan cloud computing. *Jurnal Teknologi Informasi dan Komputer, 10*(1), 33–40.

Tolt, S., *et al*. (2023). *The role of IAM in securing AWS DevSecOps pipelines.* ResearchGate. https://www.researchgate.net/publication/373219301

Verdet, A., Montoya, D., & Kim, J. (2023). *Exploring security practices in infrastructure as code: An empirical study.* arXiv. https://arxiv.org/abs/2301.12792

Wulandari, E., & Puspitasari, T. (2022). Manajemen akses berbasis IAM role dan policy pada layanan cloud AWS. *Jurnal Ilmiah Teknologi dan Komputer, 7*(2), 98–105.

Shaw, B., Rogers, S., & Kumar, H. (2022). *Defense-in-depth principles for protecting cloud workloads.* CrowdStrike Blog. https://www.crowdstrike.com/blog/defense-in-depth-principles