# EDUKASI KEAMANAN AWS: MENGAMANKAN AKUN, DATA, DAN KEPATUHAN CLOUD DENGAN AWS IAM

**[1]Ibnu Mansyur Hamdani✉, [2]Adi Syahadi, [3]A. Hermina Julyaningsih, [1]Arminas**
[1]Teknik Perawatan Mesin, Akademi Komunitas Industri Manufaktur Bantaeng, Indonesia
[2]Unit Informasi dan Teknologi, Laz Al-Bahjah, Indonesia
[3]Teknologi Industri Pertanian, Universitas Hasanuddin, Makassar, Indonesia
Email: ibnumansyur@akom-bantaeng.ac.id

DOI: https://doi.org/10.46880/methabdi.Vol5No1.pp112-118

***ABSTRACT***

*Cloud computing service security is a crucial aspect in managing data and information technology infrastructure. Amazon Web Services (AWS) provides security features such as AWS Identity and Access Management (IAM) to control access to resources. However, the lack of user understanding in implementing this system increases the risk of data leaks and cyberattacks. This community service activity aims to improve digital security literacy, especially in the use of AWS IAM. The training was held online on February 2, 2025, via Zoom and was attended by 24 participants from a total of 30 registrants. The methods used include theory and direct practice using an AWS Academy account. Evaluation was carried out through pre-tests and post-tests as well as a Google Form survey. The results showed an increase in understanding, with an average pre-test score of 60 increasing to 85 in the post-test. In addition, 92% of participants stated that the material presented was relevant, 88% felt the training was practically useful, and 90% were more confident in managing their AWS accounts. These results show that education about AWS security is essential to reduce the risk of misconfiguration and improve the security of cloud-based systems.*

***Keyword: Cloud Computing, AWS IAM, Community Service.***

**ABSTRAK**

*Keamanan layanan cloud computing menjadi aspek krusial dalam pengelolaan data dan infrastruktur teknologi informasi. Amazon Web Services (AWS) menyediakan fitur keamanan seperti AWS Identity and Access Management (IAM) untuk mengontrol akses terhadap sumber daya. Namun, kurangnya pemahaman pengguna dalam mengimplementasikan sistem ini meningkatkan risiko kebocoran data dan serangan siber. Kegiatan pengabdian kepada masyarakat ini bertujuan untuk meningkatkan literasi keamanan digital, khususnya dalam penggunaan AWS IAM. Pelatihan dilaksanakan secara daring pada 2 Februari 2025, melalui Zoom dan diikuti oleh 24 peserta dari total 30 pendaftar. Metode yang digunakan mencakup teori dan praktik langsung menggunakan akun AWS Academy. Evaluasi dilakukan melalui pre-test dan post-test serta survei Google Form. Hasil menunjukkan peningkatan pemahaman dengan rata-rata skor pre-test 60 meningkat menjadi 85 pada post-test. Selain itu, 92% peserta menyatakan materi yang disampaikan relevan, 88% merasa pelatihan bermanfaat secara praktis, dan 90% lebih percaya diri dalam mengelola akun AWS mereka. Hasil ini menunjukkan bahwa edukasi mengenai keamanan AWS sangat diperlukan untuk mengurangi risiko kesalahan konfigurasi dan meningkatkan keamanan sistem berbasis cloud.*

***Kata Kunci: Cloud Computing, AWS IAM, Pengabdian kepada Masyarakat.***

## PENDAHULUAN

Dalam era digital yang semakin berkembang, teknologi *cloud computing* (*cloud computing*) telah menjadi solusi utama bagi berbagai sektor, termasuk bisnis (Vankayalapati, 2025), Pendidikan (Chahal et al., 2024), dan

pemerintahan (Ikwuanusi et al., 2024). Amazon Web Services (AWS) sebagai salah satu penyedia layanan *cloud computing* terbesar menawarkan fleksibilitas dan skalabilitas yang tinggi dalam pengelolaan infrastruktur teknologi informasi (TI) (Vishwakarma & Dalvi, 2024). Namun, dengan meningkatnya ketergantungan terhadap teknologi *cloud computing*, tantangan dalam hal keamanan juga semakin kompleks.

Kasus kebocoran data, pencurian identitas digital, dan serangan dunia maya (siber) semakin marak terjadi (Nyame et al., 2024), menunjukkan pentingnya kesadaran dan pemahaman mengenai keamanan *cloud computing* bagi para pengguna. Keamanan dalam lingkungan *cloud computing* tidak hanya bergantung pada penyedia layanan, tetapi juga menjadi tanggung jawab pengguna untuk mengelola akun, mengatur hak akses, serta melindungi data dari ancaman siber, dalam AWS dikenal sebagai *Shared Responsibility Model* (Amazon Web Services, 2025). Dalam konteks ini, Amazon Web Services Identity and Access Management (AWS IAM) menjadi salah satu fitur utama yang memungkinkan pengguna mengontrol akses terhadap sumber daya mereka dengan lebih aman dan efisien (Amazon Web Services, 2025). Kurangnya pemahaman dan implementasi yang tepat terhadap sistem keamanan ini dapat meningkatkan risiko keamanan data yang berpotensi menyebabkan kerugian besar (Sadok & Bednar, 2015), sehingga edukasi mengenai keamanan Amazon Web Services sangat diperlukan agar masyarakat dapat lebih memahami dan menerapkan langkah-langkah perlindungan yang sesuai.

Sebagai bentuk pengabdian kepada masyarakat, kegiatan ini bertujuan untuk meningkatkan literasi keamanan digital, khususnya dalam penggunaan Amazon Web Services *Cloud*. Seiring meningkatnya adopsi layanan *cloud computing*, risiko serangan siber terhadap sistem berbasis *cloud computing* pun turut meningkat, dengan banyak kasus yang disebabkan oleh kesalahan konfigurasi keamanan, akses yang tidak sah, API yang tidak aman, pembajakan akun, dan serangan siber (Basaad & Jain, 2025). Oleh karena itu, pelatihan ini dirancang untuk memberikan pemahaman yang lebih mendalam mengenai model tanggung jawab bersama Amazon Web Services, pengelolaan Amazon Web Services Identity and Access Management, serta strategi perlindungan akun dan data dalam Amazon Web Services.

Pendekatan yang digunakan dalam kegiatan ini mencakup teori dan praktik, sehingga peserta tidak hanya memahami konsep keamanan *cloud computing* secara teoritis, tetapi juga memiliki keterampilan praktis dalam mengamankan lingkungan *cloud computing* mereka. Untuk memastikan aksesibilitas yang lebih luas, kegiatan ini akan dilaksanakan secara daring, memungkinkan partisipasi dari berbagai latar belakang dan terbuka bagi masyarakat umum. Dengan metode penyampaian yang mudah dipahami dan aplikatif, diharapkan setiap peserta mampu menerapkan prinsip-prinsip keamanan Amazon Web Services secara efektif.

Urgensi pelatihan ini semakin diperkuat oleh beberapa penelitian yang menunjukkan bahwa implementasi keamanan *cloud computing* diperlukan untuk mencegah ancaman serius terhadap data dan sistem informasi (Basaad & Jain, 2025; Kapoh et al., 2024; P. Anusha et al., 2024). Salah satu kerangka dasar keamanan *cloud computing* adalah IAM yang memastikan pengguna sah dapat mengakses sumber daya penting dalam system computer dan mencegah orang yang tidak memiliki akses untuk mengakses data (Premsai, 2024). Oleh karena itu, melalui kegiatan ini, diharapkan peserta dapat memahami pentingnya keamanan dalam *Cloud* serta mampu menerapkan praktik terbaik dalam mengelola identitas, akses, dan data mereka. Dengan edukasi yang tepat, masyarakat dapat mengurangi risiko serangan siber serta meningkatkan keamanan sistem *cloud computing* mereka secara lebih efektif, sehingga mendukung ekosistem digital yang lebih aman dan andal.

## TUJUAN DAN MANFAAT

Tujuan dari pelaksanaan kegiatan pengabdian kepada masyarakat ini adalah untuk meningkatkan literasi dan kesadaran masyarakat mengenai keamanan dalam layanan *cloud*

*computing*, khususnya Amazon Web Services (AWS). Dengan adanya kegiatan ini, peserta diharapkan dapat memahami prinsip-prinsip dasar keamanan AWS, mengelola identitas dan akses dengan Amazon Web Services Identity and Access Management (AWS IAM), serta menerapkan langkah-langkah perlindungan terhadap data dan sistem berbasis AWS.

Selain itu, kegiatan ini bertujuan untuk membekali peserta dengan keterampilan praktis dalam mengamankan akun dan infrastruktur *cloud* mereka. Melalui pendekatan yang menggabungkan teori dan praktik, peserta akan memperoleh pengalaman langsung dalam konfigurasi keamanan AWS, yang dapat mereka terapkan dalam penggunaan sehari-hari maupun dalam lingkungan kerja profesional.

Manfaat yang diharapkan dari kegiatan ini antara lain adalah meningkatnya kesadaran masyarakat terhadap pentingnya keamanan data dan sistem informasi berbasis *cloud*. Dengan pemahaman yang lebih baik, peserta dapat mengurangi risiko kebocoran data, serangan siber, dan kesalahan konfigurasi yang berpotensi merugikan. Selain itu, dengan meningkatnya keterampilan peserta dalam pengelolaan keamanan AWS, diharapkan akan tercipta ekosistem digital yang lebih aman dan andal.

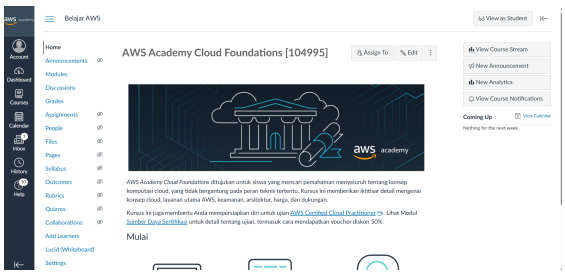
Secara lebih luas, kegiatan ini juga berkontribusi dalam mendukung perkembangan transformasi digital yang lebih aman, baik di sektor bisnis, pendidikan, maupun pemerintahan. Dengan adanya edukasi dan pelatihan yang berkelanjutan, masyarakat dapat lebih siap menghadapi tantangan keamanan informasi di era digital saat ini.

## METODE PELAKSANAAN

Kegiatan pengabdian kepada masyarakat ini dirancang dengan pendekatan berbasis edukasi dan praktik langsung untuk memastikan peserta memahami serta dapat menerapkan keamanan dalam layanan Amazon Web Services (AWS). Kegiatan ini akan dilakukan secara daring agar dapat menjangkau peserta dari berbagai latar belakang dan lokasi.

Pelaksanaan kegiatan ini terdiri dari pemaparan teori melalui webinar, demonstrasi langsung penggunaan AWS IAM, serta sesi latihan dan diskusi interaktif. Webinar akan menghadirkan pemateri yang berpengalaman di bidang *Cloud* dan layanan AWS, yang akan menjelaskan konsep-konsep keamanan *cloud* serta memberikan contoh kasus nyata. Selain itu, peserta akan diberikan akses ke simulasi langsung guna memperkuat pemahaman dan meningkatkan keterampilan teknis dalam mengamankan layanan AWS.

Kegiatan ini bekerja sama dengan komunitas pengguna AWS dan akademisi yang akan bertindak sebagai pemateri dan fasilitator dalam sesi pelatihan. Salah satu dukungan utama dalam pelaksanaan kegiatan ini adalah kerja sama antara pemateri dan pihak AWS dalam menyediakan akun AWS Academy bagi para peserta. AWS Academy ini ditunjukkan pada Gambar 1. Akun ini memungkinkan peserta untuk mengakses berbagai materi pelatihan dan melakukan praktik langsung dalam lingkungan *cloud* yang aman dan terstruktur. Selain itu, kegiatan ini juga akan menggunakan platform konferensi daring seperti Zoom atau Google Meet untuk mendukung komunikasi dan interaksi selama sesi berlangsung. Materi pembelajaran akan disediakan dalam bentuk modul digital dan video edukatif guna memudahkan peserta dalam memahami konsep-konsep yang diajarkan.




**Gambar 1**. Tampilan AWS Academy

Kegiatan dapat diikuti oleh peserta dari berbagai daerah tanpa keterbatasan geografis karena dilaksanakan secara daring. Sasaran utama dari program ini adalah masyarakat umum, termasuk individu yang tertarik atau bekerja dalam bidang teknologi informasi, akademisi,

mahasiswa, serta pelaku industri yang ingin meningkatkan pemahaman mereka mengenai keamanan *cloud computing*. Dengan pendekatan yang terstruktur dan berbasis praktik, diharapkan peserta dapat mengembangkan keterampilan yang dapat langsung diterapkan dalam dunia kerja maupun dalam penggunaan layanan AWS secara pribadi.

Dengan metode pelaksanaan ini, peserta tidak hanya memperoleh pemahaman teoritis mengenai keamanan AWS, tetapi juga mendapatkan pengalaman praktik yang mendukung penerapan keamanan *cloud computing* dalam skenario nyata.

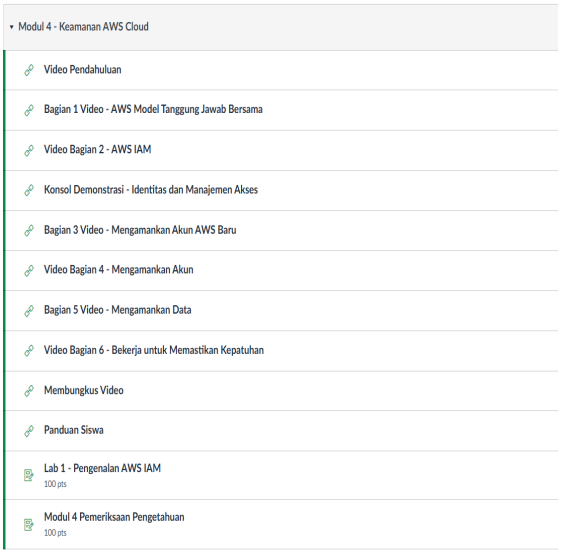
## HASIL DAN PEMBAHASAN

Kegiatan pengabdian kepada masyarakat ini telah dilaksanakan pada Hari Minggu, 2 Februari 2025, secara daring menggunakan platform Zoom. Kegiatan ini terdiri dari beberapa tahapan utama yang dilakukan secara sistematis untuk memastikan efektivitas pembelajaran bagi peserta, yaitu persiapan, pelaksanaan, dan evaluasi.

### Persiapan

Tahap persiapan dimulai dengan pembuatan grup WhatsApp pada 25 Januari 2025. Grup ini digunakan sebagai media komunikasi utama antara penyelenggara dan peserta untuk menyampaikan informasi terkait kegiatan, termasuk jadwal, tautan Zoom, serta materi pendukung. Setelah itu, pada 27 Januari 2025, dilakukan pembuatan akun Amazon Web Services Academy (AWS Academy) bagi peserta. Akun ini memungkinkan peserta untuk mengakses berbagai materi pelatihan serta melakukan praktik langsung dalam lingkungan *cloud* yang aman dan terstruktur.

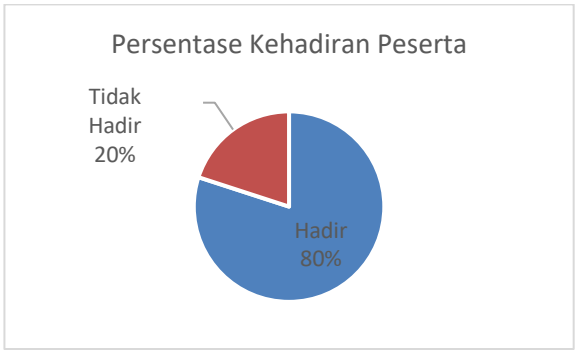
Agar peserta dapat menggunakan akun AWS Academy dengan optimal, pada 29 Januari 2025 diselenggarakan sesi tutorial singkat mengenai cara login, navigasi platform, serta pemanfaatan fitur yang tersedia. Dengan langkah-langkah persiapan ini, peserta diharapkan siap mengikuti pelatihan dengan baik dan dapat langsung mempraktikkan materi yang diberikan dalam kegiatan inti.




**Gambar 2.** Materi Pelatihan dalam Akun AWS Academy

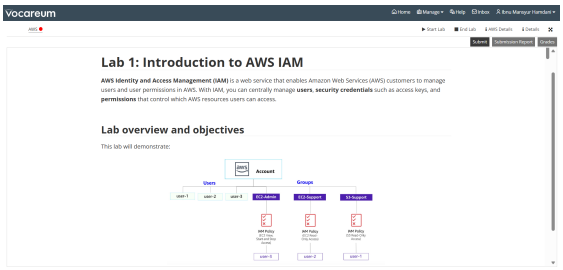
### Pelaksanaan

Kegiatan inti dilaksanakan pada 2 Februari 2025 melalui Zoom. Dari total 30 peserta yang terdaftar, sebanyak 24 peserta hadir, sementara 6 peserta tidak hadir (20% dari total peserta).




**Gambar 3.** Grafik Kehadiran Peserta

Pelaksanaan kegiatan ini mencakup pemaparan teori, demonstrasi penggunaan Amazon Web Services Identity and Access Management (AWS IAM), serta latihan langsung menggunakan akun AWS Academy. Materi disampaikan secara interaktif melalui diskusi dan sesi tanya jawab.




**Gambar 4.** Lab AWS IAM

## Evaluasi

Evaluasi dilakukan melalui *pre-test* dan *post-test*, serta Google Form untuk umpan balik peserta.

- Hasil *Pre-test* dan *Post-test*

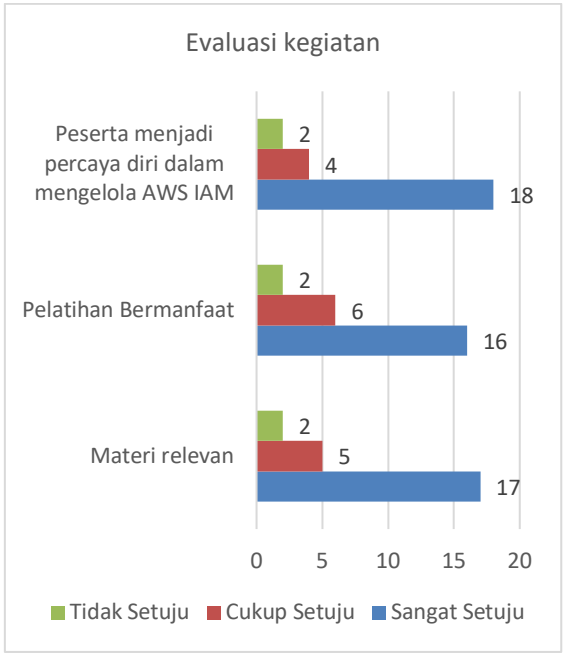
  Pengukuran tingkat pemahaman peserta sebelum dan sesudah pelatihan ditunjukkan dalam Gambar 5, di mana P1 adalah peserta pertama dengan nilai berada dalam rentang 1—100.


**Gambar 5.** *Pre-test* vs *Post-test*

Hasil evaluasi menunjukkan adanya peningkatan signifikan dalam pemahaman peserta, dengan rata-rata *pre-test* 60 dan meningkat menjadi 85 pada rata-rata *post-test*.

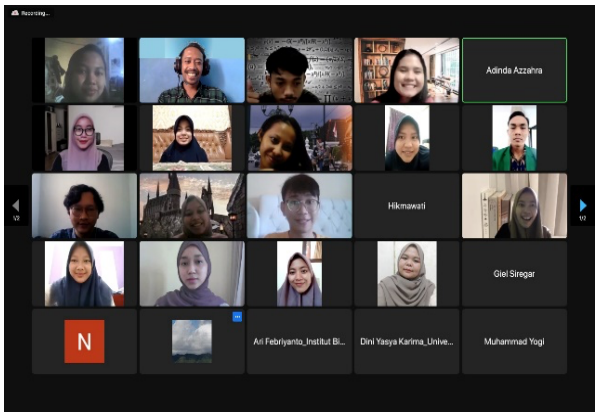
- Hasil Evaluasi Google Form

  Evaluasi kepuasan peserta dilakukan menggunakan Google Form, dengan hasil sebagai berikut:




**Gambar 6.** Grafik Evaluasi Kegiatan

Dari hasil evaluasi ini dapat disimpulkan bahwa mayoritas peserta merasa materi yang disampaikan sangat relevan (92%), pelatihan memberikan manfaat praktis (88%), dan pelatihan meningkatkan kepercayaan diri peserta dalam mengelola akun AWS (90%).




**Gambar 7.** Foto Bersama Peserta

## KESIMPULAN

Kegiatan pengabdian kepada masyarakat mengenai keamanan layanan *cloud computing* Amazon Web Services (AWS) telah berhasil dilaksanakan secara daring pada 2 Februari 2025 melalui platform Zoom. Dengan total 30 peserta terdaftar dan 24 peserta hadir (80% kehadiran), kegiatan ini memberikan wawasan mendalam mengenai Amazon Web Services Identity and Access Management (AWS IAM) serta praktik terbaik dalam mengelola keamanan layanan AWS.

Melalui metode edukasi berbasis teori dan praktik, peserta mendapatkan kesempatan untuk memahami konsep-konsep keamanan *cloud* serta menerapkan langsung langkah-langkah pengamanan akun dan data mereka. Evaluasi hasil pelatihan menunjukkan adanya peningkatan pemahaman peserta, dengan rata-rata skor *pre-test* 60 yang meningkat menjadi 85 pada *post-test*.

Selain itu, umpan balik peserta melalui Google Form menunjukkan bahwa 92% peserta merasa bahwa materi yang disampaikan relevan dengan kebutuhan mereka, 88% peserta menyatakan bahwa pelatihan ini memberikan manfaat praktis dalam penerapan keamanan AWS, dan 90% peserta merasa lebih percaya diri dalam mengelola akun dan keamanan AWS mereka setelah mengikuti pelatihan.

Berdasarkan hasil tersebut, dapat disimpulkan bahwa kegiatan ini berhasil meningkatkan kesadaran dan literasi keamanan *cloud computing* bagi para peserta. Dengan edukasi yang tepat, pengguna layanan AWS dapat mengurangi risiko kesalahan konfigurasi dan ancaman keamanan yang berpotensi menyebabkan kebocoran data. Oleh karena itu, pelatihan serupa dengan berbagai topik dalam bidang *cloud computing* perlu terus diselenggarakan agar semakin banyak individu dan organisasi yang memperoleh pemahaman yang lebih mendalam mengenai teknologi ini.

## DAFTAR PUSTAKA

Amazon Web Services. (2025). *AWS Identity and Access Management*. Retrieved March 13, 2025, from https://aws.amazon.com/id/iam/

Amazon Web Services. (2025). *Shared Responsibiliity Model*. Retrieved March 12, 2025, from https://aws.amazon.com/compliance/shared-responsibility-model/

Basaad, J., & Jain, V. (2025). Enhancing Cloud Security Strategies to Mitigate Critical Threats. In M. D. Lytras, A. N. Alkhaldi, & P. O. de Pablos (Eds.), *In Harnessing AI, Blockchain, and Cloud Computing for Enhanced e-Government Services* (pp. 279–302). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-7678-2.ch009

Chahal, D., Chahal, S., & Kumar, S. (2024). Status of Utilization of Cloud Computing in Education and Research in India. *International Journal of Applied and Behavioral Sciences*, *01*(01), 97–111. https://doi.org/10.70388/ijabs24712

Ikwuanusi, U. F., Onunka, O., Owoade, S. J., & Uzoka, A. (2024). Digital transformation in public sector services: Enhancing productivity and accountability through scalable software solutions. *International Journal of Applied Research in Social Sciences*, *6*(11), 2744–2774. https://doi.org/10.51594/ijarss.v6i11.1724

Kapoh, H., Aprilyana, P., Sumampow, Y., Mailake, M., Manimpurung, F., & Pakaya, H. (2024). Data Security and Data Protection in Cloud Privacy Systems. *Jurnal Syntax Admiration*, *5*(11), 4801–4809. https://doi.org/10.46799/jsa.v5i11.1768

Nyame, Lord, Marfo-Ahenkorah, E., Abrahams, A., Ashley-Osuzoka, J., Ashong, G., & Aboagye, D. (2024). Rise in Cyber Threats in the United States and the Need for Advanced Cyber Risk Mitigation Tools and Adequate Skills to Combat Cyber Threats. *Preprints*. https://doi.org/10.20944/preprints202409.1813.v1

P. Anusha, P. Sridhar, S. Yeshwanth, & Adnan. (2024). Optimizing Cloud Security Through Data Splitting and Replication. *International Journal of Advanced Research in Science, Communication and Technology*, 355–361. https://doi.org/10.48175/IJARSCT-22651

Premsai, R. (2024). Mitigating Cyber Threats With Robust Identity And Access Management Techniques. *Interantional Journal Of Scientific Research In*

*Engineering And Management*, *08*(12), 1–7. https://doi.org/10.55041/IJSREM17705

Sadok, M., & Bednar, P. M. (2015). Understanding Security Practices Deficiencies: A Contextual Analysis. *HAISA*, 151–160.

Vankayalapati, R. K. (2025). Public clouds: The pillar of scalability and innovation. In *Deep Science Publishing*. Deep Science Publishing. https://doi.org/10.70593/978-81-984306-5-6_3

Vishwakarma, A. V., & Dalvi, P. S. (2024). Unveiling the Cloud: An Evaluation of AWS Infrastructure Against Traditional On-Premise Solutions. *International Journal of Advanced Research in Science, Communication and Technology*, *4*(3), 294–302. https://doi.org/10.48175/ijarsct-18932