International IT Journal of Research (IITJR), ISSN: 3007-6706
Volume 3, Issue 1, January- March, 2025
Available online at: https://itjournal.org/index.php

Securing Microservices in Cloud-Native Architectures: A Comparative Analysis of AWS Lambda and Azure Functions

Deepak Singh

Advisory Solution Architect, Gainwell Technologies, USA

ABSTRACT

Cloud-native application development adopting Serverless computing is transforming application development through the speed of deployment, scalability and without the requirement to manage the infrastructure. The literature explores security architectures of AWS Lambda and Azure Functions on important aspects like authentication, data encryption and microservices access control. This is a study using an explanatory research design and secondary qualitative and quantitative data to compare the strengths and weaknesses of the security features of each platform. The results show the need to have least privilege access; use of controls, like firewalls and intrusion prevention systems; and real time monitoring to balance the vulnerabilities. This is essential for performance, compliance and resilience in such a dynamic environment where security strategies and tools are their top priority.

Keywords: Serverless Computing, AWS Lambda, Azure Functions, Microservices Security, Cloud-Native Architecture, Access Control

INTRODUCTION

Background to the Study

Microservices, Serverless computing are at the forefront in application deployment in fast-paced adoption of cloud native architecture. AWS Lambda and Azure Function are event driven and scalable environment for use in modern application development [1]. The security on the system must be robust and these platforms are becoming increasingly vital to organisations.

On every platform, security models, threats and protection mechanisms are different in terms of their ability to provide service integrity, confidentiality and availability [2]. This research investigates the security aspects of employing AWS Lambda and Azure Functions with microservices architecture, to highlight their strengths, weaknesses and the practices of securing cloud-native applications.

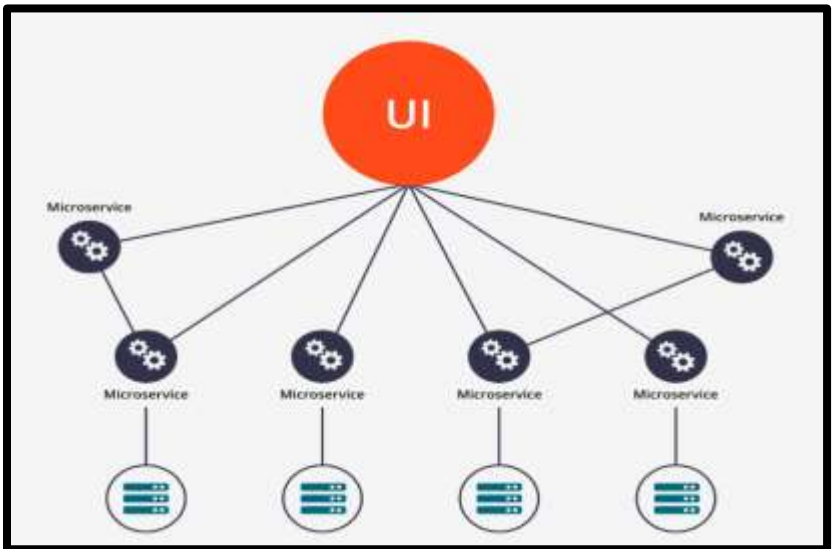

Figure 1: Microservices Architecture

International IT Journal of Research (IITJR), ISSN: 3007-6706
Volume 3, Issue 1, January- March, 2025
Available online at: https://itjournal.org/index.php

Overview

In this research, AWS Lambda and Azure Functions are analysed comparatively focusing on security of microservices based cloud-native deployment architecture. It looks at the security models, access controls, data protection and the vulnerability management done by each platform. The study intends to evaluate which service provides more complete security for dynamic and distributed environment by assessing their strengths and weaknesses. This analysis also explores real world use cases along with current best practises to provide practical guidance for developers and companies. The findings of this research should be helpful for people to make informed decisions to choose a serverless platform and aligns with performance and security requirement.

Problem Statement

Adoption of serverless computing platforms has been rapidly accelerated as organisations transition to cloud-native architectures based on microservices. Although these platforms provide scalability, lesser infrastructure management and faster deployment, they bring in new security challenges [3]. They are risks related to unauthorised access, insecure APIs, code injection, data breach and lack of isolation between services. However, in spite of this popularity, there exists very little comprehensive and comparative research as far as assessing the security mechanisms of AWS Lambda and Azure Functions in the context of microservices. The problem of this gap is that developers and decision makers lack certainty when deciding on a secure platform. This needs to be addressed so that microservices operate safely in cloud environments.

Objectives

The objectives are: 1. To discuss the security architectures and protection features of AWS Lambda and Azure Functions in microservices-based cloud-native applications. 2. To explore how each platform deal with key security aspects like authentication, data encryption, access control. 3. To identify common vulnerabilities and threats for serverless microservices in AWS and Azure systems and their related mitigation strategies. 4. To evaluate the best practices to secure microservices using AWS Lambda and Azure Functions following industry standards and real-world cases.

Scope and Significance

This study looks in to security aspect of AWS Lambda and Azure Functions in the cloud-native microservices based architectures. It reviews security mechanisms like authentication, authorisation, data encryption, isolation, vulnerability management and compliance support. The research has the scope of analysis to these leading serverless platforms, allowing for a focused and highly relevant and practical comparison for organisations undergoing digital transformation [4]. This study is significant as it can help IT professionals, developers and decision-makers make a choice of secure serverless environment to their operational and regulatory requirements. The findings help to secure microservices in the cloud also supporting development of safer and more resilient application infrastructures.

LITERATURE REVIEW

The Security Architectures and Protection Features

AWS Lambda and Azure Functions are highly secure for microservices based cloud-native applications protecting data and authorisation. AWS Lambda integrations tightly with AWS Identity and Access Management (IAM) to determine permissions, providing users with fine-grained access policies for each function [5]. It also provides the ability to encrypt data at rest via AWS Key Management Service (KMS), as well as encryption in transit via TLS.

Figure 2: AWS Environment of Protection Features

Azure Functions rely on Azure Active Directory (AAD) for authentication and role-based access control (RBAC), so only the authorised entities can invoke functions. Data is protected with the use of secrets and cryptographic services which are managed by Azure Key Vault [6]. For example, a retail business as taking customer orders on AWS Lambda can use strictly IAM roles that keep the function away from any resources other than the necessary ones [7]. These platforms isolate functions into secure runtime environments to minimise the risk of being executed on multi-tenant cloud installation.

Key Security Aspects of Platforms

Security aspects like authentication, data encryption and access control are supported as integrated cloud-native security in AWS Lambda and Azure Functions. For example, IAM is used for access control to AWS Lambda functions with fine grained permission polices per function and allows authentication via Amazon Cognito, OAuth providers [7]. In contrast, Azure Functions use 'Azure Active Directory' (AAD) for safe authentication and then fine grained RBAC for access control. Data is protected via encryption protocols and utilisation of Azure Key Vault [6]. For example, a medical practitioner can leverage Azure Functions to process patient information, authorise users using AAD, keep credentials safely stored within Key Vault.

Vulnerabilities and Threats for Serverless Microservices

Serverless microservices present common vulnerabilities in the form of insecure function permissions, injection attacks, insufficient input validation and third-party dependency risks. AWS Lambda or Azure Functions may suffer from privilege escalation in case of excessive function privileges [8]. AWS can apply the principle of least privilege via IAM roles and Azure prevents access via RBAC to mitigate these issues [9]. These platforms support the use of input validation, code scanning and secret management tools such as AWS Secrets Manager and Azure Key Vault [10]. In addition, dependency regular updates and the use of runtime protection on the serverless microservices are equally essential on the platforms to prevent exploitation.

Figure 3: Threats for Serverless Microservices

The Best Practices to Secure Microservices

AWS Lambda and Azure Functions easily apply key industry best practises like least privilege access, encrypted data transmission, secure identity management and continuous monitoring to securing microservices. To minimise the attack surface, functions should operate with minimum permissions available with AWS IAM or Azure RBAC [10]. Secrets would be managed on AWS Secrets Manager or Azure Key Vault and authentication would be conducted using a secure protocol like OAuth or Azure Active Directory [11]. For example, Capital One makes use of AWS Lambda to work with sensitive customer data [12]. All data is encrypted and strict IAM roles are enforced, with automated security tools integrated to provide PCI DSS compliant security for microservices.

METHODOLOGY

Research Design

In this research, an explanatory design is employed to explore and explain the security features of AWS Lambda and Azure Functions in cloud-native, microservices based architectures. The explanatory approach is suitable for understanding why the differences exist and how the mechanisms can explain the observed differences in security practices and performance

between the platforms [13]. It conducts an analysis of industry standards and practical case studies and security incident reports as the purpose of offering concise and structured comparison. This design helps to recognise the relationships between the platform specific security implementation choices and their applicability in the real world. This also provides actionable insights to developers and IT professionals who are currently engaged in securing their serverless applications.

Data Collection

Secondary qualitative and quantitative data are employed to examine the security aspects in AWS Lambda and Azure Functions. Qualitative data are collected from academic journals, industry reports and different expert opinions to know the design principles, security models and best practises beneficial to each platform [14]. Quantitative data are collected using statistics on cloud utilization, graph and performance data presented by standard organisations. The integration of these methods allows for the balanced analysis of theoretical and practical dimensions of platform security. The research employs secondary data to offer extensive coverage of information since the analysis of an entire comparison that supports conclusions and recommendations.

CASE STUDIES/EXAMPLES

Case Study 1: Performance Evaluation of Amazon's, Google's, and Microsoft's Serverless Functions

In this case study, three major serverless cloud platforms (AWS Lambda, Azure Functions and Google Cloud Functions) are evaluated, based on a standardised environment with Node.js v12 and JavaScript, for their performance and limitations. A code developed in Visual Studio Code is developed to process datasets from 500 to 100,000 records to simulate a real-workload of a real-world application [15]. Their ability to deal with data intensive operations were examined and compared based on response time and data retrieval efficiency on each platform. The objective was to identify the best performing platform, with the least amount of configuration effort, to make useful comparisons about what platform is best suited for scalable, efficient business applications with serverless functions.

Case Study 2: Implementing Zero Trust Architecture in Cloud-Native Environments: Challenges and Best Practices

This case study examines the application of Zero Trust Architecture (ZTA) to cloud-native environments and describes as applied in a commercial context. The basis for discussions about the practical challenges and gaps in current deployment strategies. The study examines ZTA principles of continuous authentication, identity and access management, network segmentation and least privilege enforcement, used to secure containerised applications, microservices and DevOps driven infrastructures [16]. It also investigates challenges in scaling security controls, ensuring interoperability among diverse cloud services and enforcing policy as minimising performance impact. The successful and problematic implementations are illustrated with real word use cases. The paper concludes with a full set of guidelines to assist organisations with implementation of ZTA to achieve sound security while retaining the agility and scalability demanded by the contemporary cloud-native ecosystem.

Evaluation Metrics

Table 1: Evaluation Metrics

Metric	Description
Authentication & Access Control	Assesses how each platform manages identity verification and permission settings.
Data Protection	Evaluates encryption methods for data at rest and in transit [6].
Isolation Mechanisms	Reviews how well workloads are separated to prevent cross-function interference.
Vulnerability Management	Examines how platforms detect, report, and address security threats or flaws [8].
Compliance Support	Looks at alignment with industry standards (e.g., GDPR, HIPAA, ISO).
Logging and Monitoring	Assesses tools provided for detecting, logging, and responding to security incidents.
Third-Party Integration Security	Evaluates security when connecting with external services or APIs.

(Source: Self-developed)

International IT Journal of Research (IITJR), ISSN: 3007-6706
Volume 3, Issue 1, January- March, 2025
Available online at: https://itjournal.org/index.php

The table highlights the main metrics of evaluation applied to compare AWS Lambda and Azure Functions based on important security factors such as access control, data security, compliance, and vulnerability management in microservices.

RESULTS

A. Data Presentation

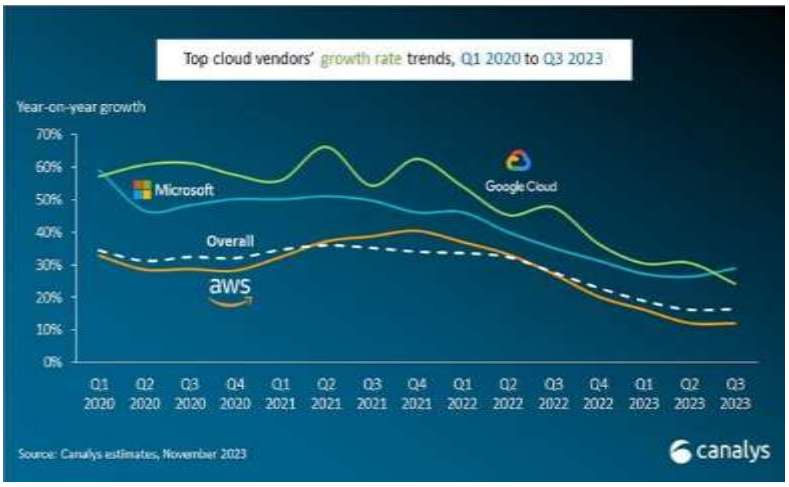

Figure 4: Growth Rate of Cloud-Native Architectures

The graph below shows year on year growth trends for the top cloud vendors, Microsoft (on Azure), AWS and Google Cloud from Q1 2020 to Q3 2023. There was a general decline post 2022, all vendors experienced the decline, with Microsoft having consistently led in terms of growth rate. AWS has slowed to around 10% Y-o-Y till Q3, 2023 [17]. Similarly, the overall cloud market growth involved also follows downward trend indicating that the industry and market is maturing and saturated. When considering cloud-native platforms such as AWS Lambda or Azure Function this trend becomes critical.

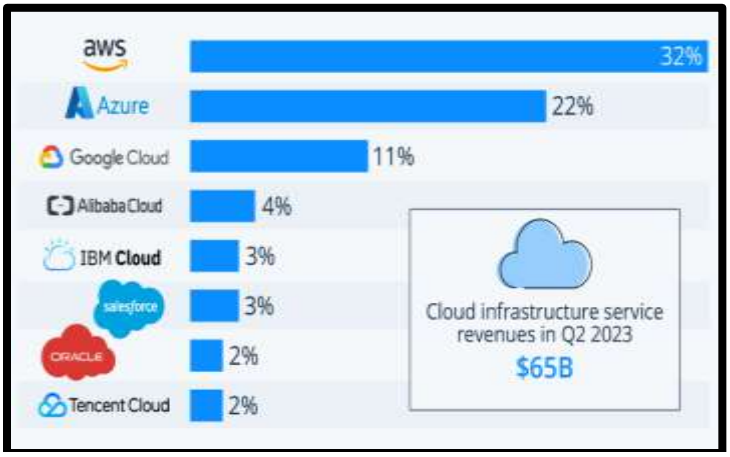

Figure 5: Market Share of Cloud-Native Architectures

According to the graph, the global cloud infrastructure total revenues of $65 billion and market share in Q2 2023 has been demonstrated. However, Amazon Web Services (AWS) was still leading with 32% share, down from 34 percent in 2017. Next, Microsoft Azure gained a share of 22% while Google Cloud had 11%, as indicate at increased momentum for both [18]. IBM Cloud and Salesforce each had 3%, while Alibaba Cloud had 4%. The graph has showed Oracle and Tencent Cloud with 2 percent. AWS and Azure continue to dominate the market, accounting for nearly two–thirds of revenues. It is

particularly important as it relates to serverless security in cloud-native architectures, because AWS Lambda and Azure Functions are in the lead of the enterprise adoption.

Findings

The findings indicate a notable pattern in the development and the acceptance of cloud-native architectures among leading cloud service providers. Cloud computing is still growing but is showing signs of maturity as growth rates have slowly been declining over the past several years [17]. In terms of how many enterprises are using them, AWS and Azure have been leading on this and ahead of all the remaining providers with regards to enterprise adoption, particularly for serverless computing models based on AWS Lambda and Azure Functions. This dominance points to their continued investment in innovation, scalability and in integration with more general cloud services. It also indicates a shift in competitive momentum, as emerging providers slowly increase their presence in the market dynamics [18]. These findings are crucial to understanding the landscape of cloud-native security when organisations increasingly depend on serverless architectures that necessitate effective, flexible and scalable security solutions that align with current businesses requirements.

Case Study Outcomes

Table 2: Case Studies Key Outcomes

Case Study	Key Outcomes
Case Study 1: Performance Evaluation of Amazon's, Google's, and Microsoft's Serverless Functions	● Performance of AWS Lambda, Azure Functions and Google Cloud Functions is different based on data-intensive workloads, with variation in response time as well as efficiency [15]. ● AWS Lambda and Azure Functions are ready for scalable and scalable delivery of serverless business applications with minimal configuration effort.
Case Study 2: Implementing Zero Trust Architecture in Cloud-Native Environments: Challenges and Best Practices	● Continuous authentication, network segmentation and enforcement of least privilege all configured for cloud-native microservices and containerised apps is necessary for the successful implementation of ZTA. ● Scaling security controls and policy enforcement across various cloud services without negatively impacting the system's performance necessitates adaptive security models [16].

(Source: Self-Developed)

The table summarises the key findings of two case studies, highlighting serverless platform performance variations and significant challenges and best practices for implementing Zero Trust Architecture in cloud-native applications.

International IT Journal of Research (IITJR), ISSN: 3007-6706
Volume 3, Issue 1, January- March, 2025
Available online at: https://itjournal.org/index.php

Comparative Analysis of Literature Review

Table 3: Comparative Analysis of Literature

Author	Focus	Key Findings	Literature Gap
[5]	Securing weak points in serverless architectures.	Highlights risk areas and importance of access control and monitoring [5]	Lacks detailed cloud platform comparison.
[6]	Serverless backend deployment on AWS Lambda and Azure Functions.	Explores deployment processes and performance.	Limited security analysis.
[7]	Cloud security across AWS, Azure, and GCP [7].	Broad overview of security strategies	Missing microservices-specific focus.
[8]	Cloud security controls analysis.	Reviews IAM, encryption, and compliance.	Few practical real-world examples [8].
[9]	Serverless function lifecycle and portability.	Discusses scalability and portability issues [9].	Minimal security focus.
[10]	Security issues in cloud-IoT systems.	Identifies security challenges for novice developers.	Narrow scope, IoT-centric.
[11]	Execution of AWS Lambda serverless functions.	Examines function performance and environment [11].	Lacks comparative security evaluation.

(Source: Self-Developed)

The table summarises key focuses, findings, and gaps in the literature, highlights serverless deployment and security strengths as indicating the necessity for more comparative and real-world security assessments across cloud environments.

DISCUSSION

Interpretation of Results

The results showed that that AWS Lambda and Azure Functions all offer good support for serverless computing, and these also help to performing better and easier to configure for scale applications. Zero Trust Architecture (ZTA) implementation to cloud-native deployments showed some security-related challenges including handling continuous authentication, segmentation at the network level and enforcement of least privilege on dynamically and widely distributed infrastructure [16]. In spite of all these challenges, ZTA needs to be implemented in order to enhance security without hampering

performance. The results indicate the need to select a suitable serverless platform and the deployment of complex, flexible security models for effective and secure deployment of cloud-native applications.

Practical Implications

These findings support for organisational planning to adopt serverless computing and cloud-native security. AWS Lambda or Azure Functions offers a solution to enhance the performance of the application and keep it simple to maintain for quick development and scalability. Zero Trust Architecture is necessary to secure the microservices but its enforcement requires a strong strategy which can resolve issues like continuous authentication and policy enforcement without reducing the system's performance [16]. Invest in flexible security frameworks and continue in the use of native and third-party tools to maintain visibility and control. This allows businesses to optimise serverless deployments and protect data and infrastructure, contributing to secure and efficient cloud-native operations.

Challenges and Limitations

There are challenges in terms of continuous authentication, network segmentation and policy enforcement in what are in principle dynamic cloud-native environments [5]. The implementation of robust security measures such as Zero Trust Architecture, may involve performance trade-offs. The limitations of the study include the reliance on secondary data which may not capture all real-world scenarios and the study mostly restricts itself to AWS Lambda and Azure Functions, without considering other emerging platforms [13]. Furthermore, findings may be quickly outdated because cloud technologies continue to evolve quickly.

Recommendations

Serverless deployments using AWS Lambda or Azure Functions are tremendously efficient and provide value for organisations in terms of performance and ease of use and should be prioritised in balancing the two. Adopting a flexible Zero Trust Architecture based on automated policy enforcement and continuous monitoring is a key step to addressing security challenges [16]. Native or third-party monitoring tools can be integrated to improve visibility and threat detection. Resilient, scalable and secure cloud-native applications can be ensured by maintaining the implementation of security practises regularly and updated with emerging cloud technologies.

CONCLUSION AND FUTURE WORK

This research has presented a complete comparison between AWS Lambda and Azure Functions for securing microservices in cloud-native architectures. They also emphasised fundamentals like authentication, data encryption, access control and monitoring and showed that both the platforms have solid security frameworks. Both AWS and Azure have a good offering for identity and secrets with IAM and Secrets Manager in AWS and Azure Active Directory and Key Vault in Azure. Effective implementation of Zero Trust Architecture and monitoring tools were demonstrated via real world case studies, showcasing the strengths and weaknesses of each platform’s security abilities.

Future work for further investigation includes cross platform interoperability, the integration of AI driven threat detection and how serverless security is affected by regulatory compliance. Furthermore, the research could be expanded to other platforms such as Google Cloud Functions for a broader scope. As cloud-native technologies continue to develop rapidly, continuous updates to best practises will be essential.

REFERENCES

[1]. KODAKANDLA, N., 2021. Serverless Architectures: A Comparative Study of Performance, Scalability, and Cost in Cloud-native Applications. Iconic Research and Engineering Journals, 5(2), pp.136-150.
[2]. Venugopal, M.V.L.N. and Reddy, C.R.K., 2021. Serverless through cloud native architecture. Int. J. Eng. Res. Technol, 10, pp.484-496.
[3]. Rahaman, M.S., Islam, A., Cerny, T. and Hutton, S., 2023. Static-analysis-based solutions to security challenges in cloud-native systems: systematic mapping study. Sensors, 23(4), p.1755.
[4]. Theodoropoulos, T., Rosa, L., Benzaid, C., Gray, P., Marin, E., Makris, A., Cordeiro, L., Diego, F., Sorokin, P., Girolamo, M.D. and Barone, P., 2023. Security in cloud-native services: A survey. Journal of Cybersecurity and Privacy, 3(4), pp.758-793.
[5]. de Oliveira, A., 2022. Securing Weak Points in Serverless Architectures. Resources Trend Micro, pp.1-31.
[6]. Arturo, P.R. and Almudena, G., 2021. Serverless Backend Development with Node. js: Deploying Functions on AWS Lambda and Azure Functions. International Journal of Trend in Scientific Research and Development, 5(6), pp.2077-2086.

[7]. Estrin, E., 2022. Cloud Security Handbook: Find out how to effectively secure cloud environments using AWS, Azure, and GCP. Packt Publishing Ltd.
[8]. Sailakshmi, V., 2021. Analysis of Cloud Security Controls in AWS, Azure, and Google Cloud.
[9]. Hartauer, R., Manner, J. and Wirtz, G., 2022. Cloud Function Lifecycle Considerations for Portability in Function as a Service. In CLOSER (pp. 133-140).
[10]. Corno, F., De Russis, L. and Mannella, L., 2022. Helping novice developers harness security issues in cloud-IoT systems. Journal of Reliable Intelligent Environments, 8(3), pp.261-283.
[11]. Srivastava, S., Gupta, B.K., Tandon, D., Singh, A.K., Husain, M., Ali, A., Alshmrany, S., Gupta, S. and Dubey, S., 2023. Execution of Serverless Functions Lambda in AWS Serverless Environment. International Journal of Recent Trends in Computing and Communication, 11(9), p.9014.
[12]. Capital One, 2023. Embracing AWS Lambda and serverless architecture. Available at: https://www.capitalone.com/tech/cloud/aws-lamba-serverless-architecture/. [Accessed 25 May 2024].
[13]. Sharma, L.R., Bidari, S., Bidari, D., Neupane, S. and Sapkota, R., 2023. Exploring the mixed methods research design: types, purposes, strengths, challenges, and criticisms. Global Academic Journal of Linguistics and Literature, 5(1), pp.3-12.
[14]. Djafar, H., Yunus, R., Pomalato, S.W.D. and Rasid, R., 2021. Qualitative and quantitative paradigm constellation in educational research methodology. International Journal of Educational Research & Social Sciences, 2(2), pp.339-345.
[15]. Zaman, F.U., Khan, A.H. and Owais, M., 2021. Performance evaluation Of Amazon's, Google's, and Microsoft's serverless functions: A comparative study. Int. J. Sci. Technol. Res, 10, pp.189-192.
[16]. Dommari, S. and Khan, S., 2023. Implementing Zero Trust Architecture in Cloud-Native Environments: Challenges and Best Practices.
[17]. Medium, 2023. Analysis of Hyperscalers (AWS, AZURE & GCP) from GARTNER MQ for SCPS 2023 context. Available at: https://medium.com/@dilip.nathani/analysis-of-hyperscalers-aws-azure-gcp-from-gartner-mq-for-scps-2023-context-740b4511548a [Accessed 22 May 2024].
[18]. Kumar, P.V.S. and Baldelovar, M., 2024. Green Cloud Computing and Its Role in Reducing Carbon Footprint. Technoarete Transactions on Internet of Things and Cloud Computing Research, p.44.
[19]. Chintale, P., & Gupta, G. (2025). Blockchain-Based Authentication Scheme/Framework for Secure Data Sharing. In AI and Blockchain in Smart Grids (pp. 107-126). Auerbach Publications.
[20]. Venna, S. R. (2019). Regulatory Operations in the Digital Age: Optimizing eCTD Workflows with Data Analytics. Available at SSRN 5270757.