ESP-JETA
ESP Journal of Engineering & Technology Advancements
ISSN: 2583-2646 / Volume 2 Issue 2, June 2022 / Page No: 176-182
Paper Id: JETA-V2I2P120 / Doi: 10.56472/25832646/JETA-V2I2P120

Original Article

Exploring Azure Security Center: A Review of Challenges and Opportunities in Cloud Security

Godavari Modalavalasa[1], Sumit Pillai[2]
[1,2]*Independent Researcher, USA.*

***Abstract*:** *Several businesses now need cloud services as their fundamental operational element. Cloud providers need to respect security and privacy regulations to ensure data confidentiality with their customer base. Cloud providers use non-consistent security and privacy methods while ongoing efforts exist to create cloud security standards. Azure Security Center works as a complete cloud security solution that advances the defensive measures of cloud infrastructures. This paper examines the features, challenges, and opportunities associated with the use of Azure Security Center in organizational cloud security frameworks. This work addresses issues related to configuring Azure Security Center maintenance while focusing on its role in threat intelligence development automated security procedures and standard compliance requirements. Furthermore, the paper explores Azure's data protection capabilities, including redundancy and disaster recovery options, that contribute to secure data storage and management. A survey of past publications explores cloud security research which serves as basis for developing superior integration methods and functional enhancements for Azure Security Center. The research finds that Azure Security Center provides an effective security framework although solving current limitations will improve its efficiency for diverse organizational needs.*

Keywords: *Cloud Computing, Cloud Security, Microsoft Azure, Azure Security Center, Compliance Monitoring, Cloud Workload Protection.*

I. INTRODUCTION

The combination of digital transformation with networking technology has boosted cloud computing adoption because organizations can now use effective scalable flexible affordable IT solutions. Businesses benefit from cloud environments that offer limitless computing resources, vast storage opportunities and easy access thus promoting industrial innovation [1]. The move to cloud-based infrastructures brought security complexities along with it because companies must defend crucial information keep within regulatory standards and safeguard their workloads from current cyber threats [2].

Security in the cloud is becoming an important concern for businesses and companies that provide cloud services [3]. Cloud environments have a distributed nature with dynamic elements which create distinct security issues that include unauthorized access [4] to data breaches misconfigurations and compliance risks [5]. Cloud providers supply security framework tools which let organizations monitor security incidents in real-time to mitigate threats [6]. Microsoft has developed Azure Security Center (ASC) as a complete security management platform for improving cloud resource security postures [7].

A study of Azure Security Center demonstrates both technical difficulties and potential solutions within cloud security. The security platform of Azure Security Center protects organizations from threats while observing their security status and adhering to compliance requirements throughout multiple cloud systems. Through AI and automation, along with behavioral analytics, ASC enables organizations to find security weak points and build security practices which help them avoid risks in a predictive manner[8][9]. Through this assessment the author examines security concerns of cloud environments using ASC and identifies ways to enhance cloud security implementation [10]. This research analyzes Azure Security Center as a tool for enhancing cloud security and resilience to combat new cyber threats.

A. Research motivation and Significance

Cloud environments require much attention due to growing adoption of cloud computing, especially through Azure platforms. The security features of Azure Security Center remain robust yet organizations confront multiple technical and operational and financial barriers. This paper investigates Azure Security Center challenges as well as opportunities so organizations can learn how to enhance its use and manage its constraints. The significance of this research lies in its potential to guide organizations in enhancing cloud security, improving best practices, and informing security policy decisions, contributing valuable knowledge to the field of cloud security management.

B. Structure of paper

The rest of this paper is divided into many sections: Section II provides an overview of Landscape of cloud security. Section III discusses the challenges and opportunities associated. Section IV focuses on data protection strategies within Azure

Security Center. In Section V, a literature review is presented, summarizing previous research on cloud security. Section VI concludes the paper, offering recommendations

II. EVOLVING LANDSCAPE OF CLOUD SECURITY

Cloud computing has enabled scalability, flexibility, and cost-efficiency in today's ever evolving digital world, making it a vital tool for enterprises of all sizes. The increasing reliance on cloud services has, however, raised serious concerns about the safety of cloud infrastructures. To guarantee data availability, integrity, and secrecy, cloud architects and business IT security experts must comprehend and use cutting-edge cloud security solutions and tactics [11]. This article explores the latest developments in multi-cloud security strategies and cloud infrastructure protection, providing insights into best practices and emerging trends that can safeguard organizations against the increasing threat landscape. The shared responsibility paradigm between cloud service providers and users makes traditional security measures inadequate in the cloud computing scenario [12]. Figure 1 illustrates the environments of cloud security.

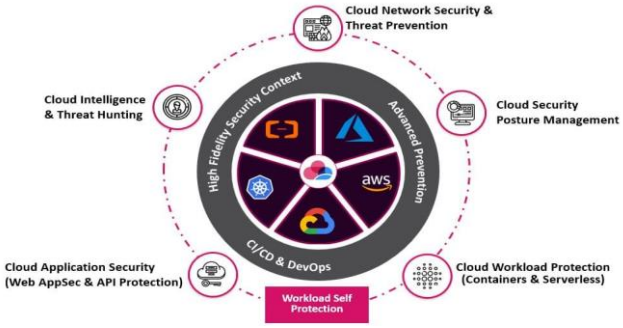

Figure 1 : Cloud Security Environment

The expansion of data privacy regulations, such as GDPR and CCPA, has also influenced cloud security practices. Organizations must ensure compliance with these laws, demanding increased control over data residency, encryption, and access management. Network origin is no longer an issue with zero-trust security models, which place an emphasis on constant identity and access permission verification [13]. The evolution of cloud security focuses on enhancing resilience through threat intelligence alongside adaptive risk management approaches because sophisticated cyber threats continue to develop. This proactive approach toward protecting cloud-based assets represents the current progress of security measures which strive to maintain innovation against security risks.

A. Proactive Security Measures of cloud

It is insufficient to depend just on responses that are reactive to security events. To accomplish targeted security goals in the cloud, a proactive strategy makes use of resources such as Azure Security Centre and Microsoft Defender for Cloud. Specifically for the cloud, here are some important preventative steps:

- Continuous Monitoring and Threat Detection: The Microsoft Defender for Cloud and Azure Security Centre tracks dangerous behaviours and faults within cloud resources. The monitoring system detects security threats so that appropriate responses can be taken before the threats execute their damaging actions.
- Security Configuration Management: The Azure Security Centre can advise you on how to keep your cloud environment safe. Security holes from misconfigurations become less frequent when professionals follow these recommended steps.
- Data Security Measures: Azure provides encryption services which safeguard data regardless of its current state or movement status. Additional security layers against unauthorized access come from implementing strong access control systems.
- Incident Response Planning: A coordinated and effective reaction to cloud security problems is possible with a well-established incident response strategy. Everyone on the appropriate teams in your company should be involved in this strategy.

B. Importance of Security in Cloud-Based Systems

Cloud computing adoption is expanding quickly throughout every software domain because developers obtain multiple benefits from development to flexibility and cost efficiency to process management[14]. The expanding use of cloud technology generated substantial security issues that require increased importance for protection measures. Cloud-based software runs in specific development and maintenance environments where security needs must be built into software development lifecycle processes. Specific security protocols aiming at cloud software needs must be implemented due to their unique operational characteristics. These mechanisms should.

- Ensure Secure Development and Maintenance: Security measures need to integrate across the complete cloud-based software development lifecycle starting from development through deployment until maintenance completes.

- Implement Security-Based Software Development Processes: Cloud software development requires security as an essential element because it demands thorough security testing of all components.
- Utilize Inspection Mechanisms: Cloud-based application integrity relies on the practice of regular software component assessment and verification processes.
- Adapt Known Security Mechanisms: Cloud security strategies should integrate well-established security techniques while adapting them to the evolving cloud environment[15].
- Develop and Test Secure Software Models: New development models should be introduced to improve security, including secure integration testing methodologies.

C. Key Benefits of Cloud Security Managed Services

There are several benefits of using managed service for cloud security, illustrated in Figure 2. Security is always on the agenda for providers of digital services, and constant monitoring 24/7 is no easy task. SECaaS (Security as a Service) adds an extra layer of protection to secure your data [16]. Security breaches are expensive, and managed services provide the proof and dependability that your data is safe. It also removes the hassle of employing security professionals or being concerned with constant upgrades in hardware and software.

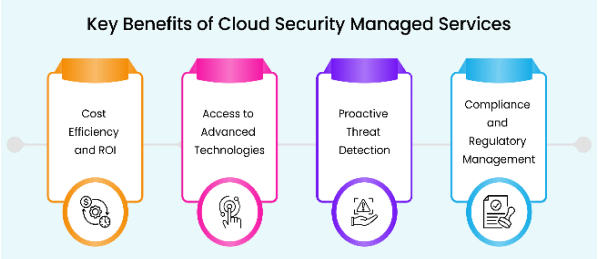

Figure 2 : Benefits of Cloud Security

MSPs play a crucial role in enhancing a company's security posture by offering real-time threat detection and response, proactively preventing security incidents from escalating. They simplify compliance management, ensuring businesses adhere to industry regulations and standards. By outsourcing security, organizations can focus on their core operations while maintaining a strong safety stance, giving them a strategic advantage. Additionally, MSPs provide continuous security enhancements, agile solutions, and updates, which support business continuity and disaster recovery, ensuring rapid recovery from potential security incidents.

- Cost Efficiency and ROI: Cloud security managed services reduce the need for costly in-house teams, offering scalable solutions that help businesses pay only for what they use, boosting financial efficiency.
- Access to Expertise and Advanced Technologies: MSPs provide access to top-tier security experts and advanced technologies, ensuring businesses stay ahead of cyber threats.
- Proactive Threat Detection and Incident Response: MSPs detect threats early and respond quickly, preventing costly security breaches with effective incident management.
- Compliance and Regulatory Management: MSPs handle compliance challenges by ensuring businesses meet industry standards, avoiding penalties and reducing regulatory risks.

III. OVERVIEW OF AZURE SECURITY CENTER

With Azure Security Centre, you can better monitor and manage the security of your Azure resources, as well as identify and react to any attacks [17]. It allows you to manage policies and conduct integrated security monitoring across all of your Azure subscriptions, find risks that could otherwise go undetected, and interface with a wide variety of security solutions (see Figure 3). Azure Security Centre also facilitates security operations by giving you a centralized dashboard that displays actionable warnings and suggestions. With the Azure Security Centre interface, fixing problems is often as easy as clicking a button.

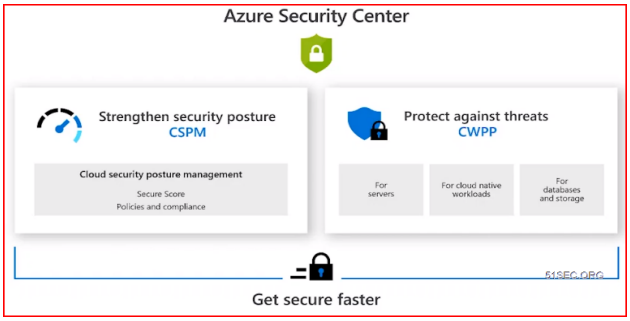

Figure 3 : Azure Security Center

Safeguarding your Azure cloud environment is centralized with Azure Security Centre (ASC). It's an all-inclusive SIEM (security information and event management) system that can monitor security posture, identify threats, and provide visibility. Among ASC's primary features are:

- Workload Protection: ASC keeps a close eye on the company's Azure resources, looking for any potential security holes or misconfigurations. Their cloud assets, including virtual machines, storage accounts, databases, and more, are identified as possible security threats.
- Security Best Practice Recommendations: ASC is more than simply problem identification. It offers doable suggestions to improve the security posture of the company. By addressing vulnerabilities and enhancing the organization's overall security hygiene, these suggestions are in line with industry standards and security best practices.
- Vulnerability Management: ASC checks the organization's Azure resources for known flaws in setups, apps, and operating systems [17]. It ranks these vulnerabilities according to their severity and offers instructions for fixing them.

A. Challenges In Azure Security Centre

Azure Security Centre, while offering a robust set of security features, presents several challenges that organizations may face when using it.

a) Technical Challenge

The most technical challenge is the process of configuring and implementing Azure Security Center. It can take much time and may create chances of error while establishing Security Center to begin guard various resource type especially in complex and big scale. Interoperability is an activity of coordinating the resources from different cloud providers (e.g., AWS, Google Cloud) where a bulk of addition configuration is needed to guarantee standard security monitoring across multiple clouds [18].

i) Operational Challenges

From an operational standpoint, a definite limitation that a company that implements and runs security solutions comes across is the unavailability of skilled personnel who are well-endowed with information on the Azure Security Center. Some establishments may not know who to consult on certain clouds issues such as security or perhaps may not be able to retain professional in the industry; this makes it very easy to overlook certain errors or even grant susceptibilities to misconfigurations. Furthermore, there are some limitations that involve the integration of Azure Security Centre with the existing organizational security frameworks and security tools: The organization might implement their programmers, which might be prior to it adopting Azure Security Centre, and such include other legacy systems or other security solutions.

ii) Cost and Licensing Challenges

Azure Security Centre works under capacity tiers and understanding costs associated with it is not easy. However, the basic security monitoring is free but, if you need more features, then you have to subscribe to Azure Defender which in return charges you. While this pricing structure is convenient for organizing public resources, this can be a problem for organizations that have a strict budget policy, organizations that may not get the maximal usability of new abilities bought with extra costs. Hence it is so important that one should first factor the expenses and weigh the advantages that come with this change against the price to upgrade.

B. Opportunities Provided By Azure Security Center

Azure Security Center offers several opportunities to enhance the security, efficiency, and compliance of cloud environments.

a) Enhanced Threat Intelligence

Azure Security Center adopted the use of artificial intelligence and machine learning [19]to boost its capability to detect threats[20]. By using it, large volumes of data can be processed virtually simultaneously to determine exposures to risk and threats. Also, it adapts with Microsoft's Threat Intelligence enabling organizations to be knowledgeable on current threats all over the world and avoid attacks. It does this proactively thus improving on the security status of organizations adopting Azure.

i) Automation and Simplification

One of the biggest advantages linked to the Azure Security Center consists in the possibility to automate most of the security processes. It can also appropriately take action against compromised assets automatically without requiring human intervention. Security teams receive security alerts and can quickly and easily mitigate problems due to SD-WAN's ability to set predetermined replies to security notifications. It also reduces workload of security operations and enhance the time taken to address incidents thus freeing organizations to engage in other tasks.

ii) Improved Compliance and Governance

Azure Security Center helps organizations in the area of compliance management because it is equipped with default compliance standards and scenarios. It has predefined control to cater for those compliance to the GDPR, HIPAA, and PCI-DSS

without the need to make significant changes. This built-in capability helps organizations to meet certain standards within the industry, simplify governance yet enhance security at the same time.

IV. DATA PROTECTION IN AZURE SECURITY CENTER

Azure Storage helps you be ready for situations when you need to recover data that has been erased or rewritten by offering data protection for both Blob Storage and Azure Data Lake Storage. Prior to an event that might jeopardise your data, it is crucial to consider the best ways to preserve it [21]. The term "data protection" is used in the Azure Storage documentation to describe methods for preventing unauthorized changes or deletions to the storage account and its contents, as well as methods for recovering lost or changed data, as seen in Figure 4. The data you store with Azure Storage may be safeguarded against service interruptions caused by hardware failures or natural catastrophes with the help of disaster recovery solutions, such as numerous layers of redundancy. Alternatively, you may switch to a secondary region via customer-managed (unplanned) failover in the event that the original region goes down.

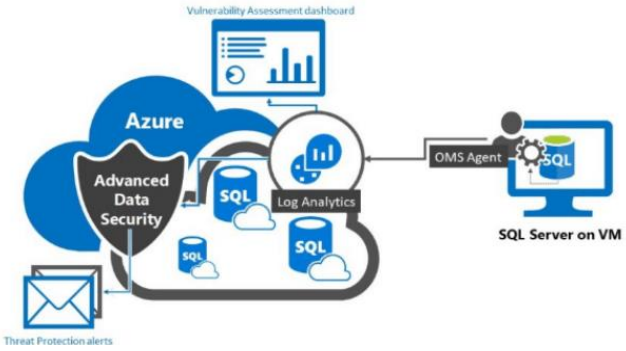

Figure 4 : Data Protection with Azure

Microsoft operations and support staff are not allowed access to client data. Only by implementing a just-in-time (JIT) architecture with rules is access to support case data permitted. The following Azure Security Policy lays out the criteria for access control:

- Customer data is not accessible by default.
- Customers' virtual machines (VMs) do not have any user or administrator accounts.
- Audit and record access requests; provide the bare minimum of privileges needed to do the job.

Microsoft and its customers must work together to ensure the success of Azure, a public cloud service. The platform is owned by Microsoft, and the company aims to provide a cloud service that satisfies our clients' demands for privacy, security, and compliance. Users are held accountable for their own systems, including their applications, data, virtual machines (VMs), and compliance with industry-specific regulatory requirements, after the accommodation has been granted.

V. LITERATURE REVIEW

In this section explores the background research on the Azure Security Center and cloud security. Some of research are given in below:

In this study, Palumbo et al (2021) experimentation enables us to provide a comprehensive performance characterization of these networks as seen by users throughout the globe, emphasizing patterns in both geographical and temporal delay, based on numerous probing approaches and a fine-grained sample rate. Finally, our research is put to use in a way that helps cloud providers and customers evaluate the performance of cloud networks (via tools for badness detection and imputation) and make deployment choices (by looking at the advantages of using several clouds). In order to encourage replication, the campaign's dataset is made freely available [22].

In this study, Ali et al (2020) locates and investigates the essential elements linked to the data protection needs of cloud services in the context of regional local governments in Australia. they polled 480 IT employees from 47 different regional local governments in Australia and spoke with 21 IT managers in the field. they provide a conceptual model for the security needs of cloud computing that includes four parts: data security, risk assessment, legal and compliance, and business and technological. This model aims to help governments see cloud security in a more balanced light. By collaborating on this approach, governments can ensure that all cloud service adoptions adhere to the same security standards [23].

In this study, Ismail and Islam (2020) created a Security Transparency and Audit Tool that allows users to gather and examine data from cloud service providers to assess compliance with regulations and specify corrective measures. This tool is meant to be used in conjunction with the proposed framework to improve security transparency by continuously testing and verifying that cloud providers satisfy user needs. The paper takes a fresh approach by bringing together disparate parts to provide businesses an easier way to achieve security transparency. They also think the contributions are significant for addressing the problems with cloud security transparency generally [24].

In this study, Shi, Jin and Li (2019) suggested integrated solution using Azure Sphere devices and Azure cloud services aims to provide a thorough and cost-effective approach to guaranteeing security from the device level all the way to the cloud, even with low resources. In order to prove that the solution is practical and efficient, they showcase the implementation details, which include the hardware, software, and Azure cloud integration [25].

In this study, Rath et al (2019) analyse Cloud SaaS security trends. They focus on patterns that address several security concerns, including privacy, data security, and system security. For SaaS developers, the production of security best practices and documenting of security expertise is an essential first step in building applications for the cloud. Further, they provide a case study of AWS and Azure security practices and remedies [4].

In this study, Kumar, Raj and Jelciana (2018) takes a look at the various cloud computing data security problems in a multi-tenant setting and suggests solutions to those problems. The article goes on to detail several models in cloud computing, including deployment and service delivery strategies. Data leaks or corruption may destroy public trust and ultimately bring down any company, especially one involved in cloud computing. A data breach affecting cloud computing would have an impact on both the cloud and the company's operations, as cloud computing is now employed in various ways by many enterprises. This is why cloud computing providers prioritise data security so much [26].

Table I summarizes key studies on cloud security and performance evaluation, highlighting their focus areas, contributions, methodologies, and limitations. While each study provides valuable insights, their limitations indicate areas requiring further research and practical validation.

Table 1 : Summary of Key Studies on Azure in Cloud Security and Performance Evaluation

Reference	Focus Area	Key Contributions	Approaches	Limitations
Palumbo et al., (2021)	Cloud-network performance evaluation	Characterizes latency trends, provides badness detection tools, supports multi-cloud deployment decisions, and releases a public dataset.	Experimentation with multiple probing methods and fine-grained sampling rate	Limited to observed network conditions; does not account for sudden network infrastructure changes.
Ali et al., (2020)	Cloud security in Australian local governments	Develops a conceptual security requirements model with four components: data security, risk assessment, legal compliance, and business/technical needs.	Conducted 21 field interviews and surveyed 480 IT staff from 47 regional local governments in Australia	Findings are specific to Australian regional governments and may not generalize globally.
Ismail and Islam, (2020)	Cloud security transparency & auditing	Develops a Security Transparency and Audit Tool for continuous cloud provider assessment, ensuring conformity and security transparency.	Framework-based tool development and analysis	Relies on cloud providers' willingness to share security-related data.
Shi, Jin and Li, (2019)	Azure-based cloud security solution	Proposes an integrated security solution using Azure Sphere and Azure cloud services, detailing hardware, software, and cloud integration.	Technical implementation and demonstration	Solution is vendor-specific and may not be applicable to other cloud platforms.
Rath et al., (2019)	Security patterns in Cloud SaaS	Provides security best practices and documentation for SaaS developers, including case studies on AWS and Azure.	Pattern-based security analysis	Lacks empirical validation of security patterns in real-world SaaS deployments.
Kumar, Raj and Jelciana, (2018)	Multi-tenant cloud security challenges	Discusses data security risks and mitigation strategies, emphasizing the importance of preventing data breaches in cloud computing.	Review of cloud security models and threat analysis	The study does not propose a concrete implementation for mitigating security risks.

VI. CONCLUSION AND FUTURE WORK

Computing, networking, and data storage are all made possible by the massive network of servers and other devices that make up the cloud. User expectations and the amount of resources needed are always evolving, making the cloud market very dynamic. In this paper, explored the Azure Security Center as a comprehensive cloud security solution, analyzing its features, challenges, and opportunities. While the implementation of Azure Security Center presents technical, operational, and cost-related challenges, it also offers significant advantages, such as enhanced threat intelligence, automation, and

improved compliance. The data protection strategies within Azure, including redundancy, failover options, and stringent access controls, further strengthen its security capabilities. The literature review highlighted ongoing research in cloud security and identified key areas where Azure Security Center can be further optimized. In conclusion, while Azure Security Center offers a robust framework for securing cloud environments, addressing the challenges discussed can enhance its adoption and effectiveness in diverse organizational settings. Future research should focus on expanding the integration of Azure Security Center with other cloud platforms and refining its automation features to improve security response times and reduce human intervention.

VII. REFERENCES

[1] S. S. S. Neeli, "Ensuring Data Quality: A Critical Aspect of Business Intelligence Success," Int. J. Lead. Res. Publ., vol. 2, no. 9, p. 7, 2021, [Online]. Available: https://www.ijlrp.com/papers/2021/9/1177.pdf%0A

[2] I. Tahirkheli et al., "A Survey on Modern Cloud Computing Security over Smart City Networks: Threats, Vulnerabilities, Consequences, Countermeasures, and Challenges," Electronics, vol. 10, no. 15, 2021, doi: 10.3390/electronics10151811.

[3] Choudhary and R. Bhadada, "Emerging threats in cloud computing," in Emerging Technology Trends in Electronics, Communication and Networking: Third International Conference, ET2ECN 2020, Surat, India, February 7--8, 2020, Revised Selected Papers 3, 2020, pp. 147–156.

[4] Rath, B. Spasic, N. Boucart, and P. Thiran, "Security Pattern for Cloud SaaS: From System and Data Security to Privacy Case Study in AWS and Azure," Computers, vol. 8, no. 2, 2019, doi: 10.3390/computers8020034.

[5] S. Elmaghraby and M. M. Losavio, "Cyber security challenges in Smart Cities: Safety, security and privacy," J. Adv. Res., vol. 5, no. 4, pp. 491–497, 2014.

[6] Belanche-Gracia, L. V Casaló-Ariño, and A. Pérez-Rueda, "Determinants of multi-service smartcard success for smart cities development: A study based on citizens' privacy and security perceptions," Gov. Inf. Q., vol. 32, no. 2, pp. 154–163, 2015.

[7] P. Pandit, "Cloud Computing Case Study on Microsoft Azure," 2021. doi: 10.13140/RG.2.2.22421.86245.

[8] T. Zhao, T. Gasiba, U. Lechner, and M. Pinto-Albuquerque, "Raising Awareness about Cloud Security in Industry through a Board Game," Information, vol. 12, no. 11, 2021, doi: 10.3390/info12110482.

[9] and P. Khare, "Cloud Security Challenges : Implementing Best Practices for Secure SaaS Application Development," Int. J. Curr. Eng. Technol., vol. 11, no. 6, pp. 669–676, 2021, doi: https://doi.org/10.14741/ijcet/v.11.6.11.

[10] Petrik and G. Herzwurm, "iIoT ecosystem development through boundary resources: a Siemens MindSphere case study," in Proceedings of the 2nd ACM SIGSOFT International Workshop on Software-Intensive Business: Start-Ups, Platforms, and Ecosystems, 2019, pp. 1–6.

[11] G. Ramachandra, M. Iftikhar, and F. A. Khan, "A Comprehensive Survey on Security in Cloud Computing," in Procedia Computer Science, 2017. doi: 10.1016/j.procs.2017.06.124.

[12] S. Tabassam, "Security and Privacy Issues in Cloud Computing Environment," J. Inf. Technol. Softw. Eng., 2017, doi: 10.4172/2165-7866.1000216.

[13] V. U. Uttarwar and A. A. Kalia, "Latest Trend in Network Security as Zero Trust Security Model," Natl. J. Comput. Appl. Sci., 2019.

[14] Godavari Modalavalasa, "The Role of DevOps in Streamlining Software Delivery: Key Practices for Seamless CI/CD," Int. J. Adv. Res. Sci. Commun. Technol., vol. 1, no. 2, pp. 258–267, Jan. 2021, doi: 10.48175/IJARSCT-8978C.

[15] K. Spanaki, Z. Gürgüç, C. Mulligan, and E. Lupu, "Organizational cloud security and control: a proactive approach," Inf. Technol. People, 2019, doi: 10.1108/ITP-04-2017-0131.

[16] M. Hussain, "SECaaS : Security as a Service for Cloud-based Applications Cloud Security at Leading Providers," Proc. Second Kuwait Conf. Eser. eSystems KCESS 11, 2011.

[17] R. Loaiza Enriquez, "Cloud Security Posture Management (CSPM) in Azure Title Number of Pages Date," no. June, 2021.

[18] J. Y. Z. Chen, "Challenges around Information Security Management in the Public Cloud," 2021.

[19] G. Modalavalasa, "Towards Sustainable Development Based on Machine Learning Models for Accurate and Efficient Flood Prediction," Int. J. Res. Anal. Rev., vol. 8, no. 2, pp. 940–944, 2021.

[20] S. C. -, "Risk Management in Advanced Persistent Threats (APTs) for Critical Infrastructure in the Utility Industry," Int. J. Multidiscip. Res., vol. 3, no. 4, Aug. 2021, doi: 10.36948/ijfmr.2021.v03i04.34396.

[21] Marshall Copeland, Cyber Security on AzureAn IT Professional's Guide to Microsoft Azure Security Center. 2017.

[22] Palumbo, G. Aceto, A. Botta, D. Ciuonzo, V. Persico, and A. Pescapé, "Characterization and analysis of cloud-to-user latency: The case of Azure and AWS," Comput. Networks, 2021, doi: 10.1016/j.comnet.2020.107693.

[23] O. Ali, A. Shrestha, A. Chatfield, and P. Murray, "Assessing information security risks in the cloud: A case study of Australian local government authorities," Gov. Inf. Q., 2020, doi: 10.1016/j.giq.2019.101419.

[24] U. M. Ismail and S. Islam, "A unified framework for cloud security transparency and audit," J. Inf. Secur. Appl., 2020, doi: 10.1016/j.jisa.2020.102594.

[25] J. Shi, L. Jin, and J. Li, "The integration of azure sphere and azure cloud services for internet of things," Appl. Sci., 2019, doi: 10.3390/app9132746.

[26] P. R. Kumar, P. H. Raj, and P. Jelciana, "Exploring Data Security Issues and Solutions in Cloud Computing," in Procedia Computer Science, 2018. doi: 10.1016/j.procs.2017.12.089.