



COMPREHENSIVE CLOUD SECURITY USING AZURE KEY VAULT, MANAGED IDENTITIES, AND ENTRA

Saatwik Gilakattula*

*Purdue university, Indianapolis

Abstract

The extensive use of cloud computing has a serious security issue to identity management, secret protection and access governance. Conventional security models and stasis credentialing mechanisms targets the perimeter security to achieve security in the dynamic and spread-out cloud environments. The current cloud security strategies put identity-first and zero-trust as a focal point, which is authenticated using identity, context, and policy. The cloud security is discussed in detail in this review with references to the Azure Key Vault, Managed Identities and Microsoft Entra as a complex of security measures in Microsoft Azure. Azure key vault is an encryption and hardware security modules based and centralized system and key cryptographic and secret and certificate management system which ensures the security of sensitive resources. The controlled Identities are applied to eliminate hard coded credentials in which one can now authenticate safely with identities and temporary tokens that are managed by the platform. Microsoft Entra extends these attributes by offering identity management, conditional access and zero-trust implementation in the cloud and hybrid setups. The design, security value, and constraints of various components are discussed and even how the different components can be integrated together to reduce the attack surfaces, improve compliance and assist in offering scalable governance of clouds. The configuration complexity, operational overhead, and the issue of vendor dependency are also discussed along with the directions in the future, which include passwordless authentication, and automated identity risk management. Overall, the current review demonstrates how the existing models of identity-based security and integration can be relevant to the existing cloud security requirements.

Keywords: Cloud Security; Azure Key Vault; Managed Identities; Microsoft Entra; Zero Trust Architecture

1. Introduction

Cloud computing has revolutionized based on the design, deployment, and management of information systems, which enables flexibility and cost efficiency. Nevertheless, this change has presented complicated issues of security involving protection of data with identity issues. Clouds are dynamic and distributed by nature, increasing the attack surface and exacerbating the risk of credential leakage, unauthorized access and improperly configured security controls [1]. Since organizations are moving workloads and sensitive information to the cloud in large volumes, the need to come up with robust security mechanisms is not a desirable add-on, but a necessity. The old methods of security that are highly dependent on perimeter-based security and hard-coded credentials are inadequate in the highly dynamic cloud-native setting. Hard coded secrets, and manually rotating credential practice is a significant risk factor of breaches, especially in large

scale environments where there are many services and users [2]. As such, the paradigm has shifted to identity-centric and zero-trust security models, where all access requests are continually authenticated using identity, context, and policy as opposed to network location only.

The Microsoft Azure can address these problems by offering security services that are integrated to address secure identity management, secret and policy-guided access. Azure Key Vault is a central and secure solution that is intended to manage cryptographic keys. So, the secrets and certificates with the help of hardware security modules and fine-granular access control to conceal sensitive data [3]. Also, Managed Identities do not need explicit credential management since they enable the secure authentication of Azure resources with automatically managed identities. Such an approach will reduce the risk of exposure of credentials to create applications and work. Furthermore, Microsoft Entra (formerly Azure Active Directory) will play a significant role in the implementation of identity governance and zero-trust environment in the cloud environment and the hybrid environment. Entra enables the least-privilege access implementation in organisations and allows auditing the activity of authentication through the use of features such as conditional access and constant verification of the identity [4]. The three components of Azure Key Vault, Managed Identities, and Microsoft Entra, which address the underlying concerns of secrecy, integrity, and access management. It is a review paper where the analysis has been done based on the cloud security of Azure Key Vault, Managed Identities, and Microsoft Entra. It talks about their various capabilities, their integration in architecture, their benefits in security, and their limitations and how they can be used together to support the existing zero-trust and identity-first security strategies in the cloud.

2. Background and related work

Cloud computing environments provide a common, highly virtualized infrastructure that fundamentally challenges the orthodoxy of security. In contrast, cloud platforms are based on multi-tenancy, which exposes organizations to risks of data breaches, insecure interfaces, and privilege escalation attacks [5]. These problems have prompted the development of cloud security systems to address confidentiality, integrity, and availability without compromising scalability. The cloud threat landscape and risk models are a single research topic. The literature review points out that cloud security breaches through misconfiguration, inadequate identity control, and imprecise credential management are some of the top causes of security breaches in the cloud [6]. Due to the high rate of cloud services development, the responsibility of security is shared between the types of cloud service providers and customers, and it requires the existence of clear governance models and constant monitoring. Scholars have emphasized the need to implement proactive security policies that combine risk management, implementing policies and policies and implementing automated remediation as a measure of reducing these emerging threats.

The cloud security literature has also focused greatly on secrets management. Initial deployments of clouds tended to use the static credentials in the application code or configuration files, which greatly amplifies the chances of secret leakage and unauthorized access [7]. In order to resolve this problem, the current researches recommend centralized secrets management tools that provide both encryption at rest and transit, fine-grained access control, and automatic rotation of keys. The mechanisms reduce human error, but also enhance that of regulatory standards like ISO 27001 and SOC 2. Identity and Access Management (IAM) has proved to be an essential component of safe cloud designs. Old IAM systems were more directed towards enterprise directory services and they did not fit very well in cloud environments where service-to-service communication is highly dynamic. Recent research suggests identity-centric approaches to use federated identities, short-lived tokens, and role-based access control to reduce attack surfaces and implement least privilege concepts [8]. This development is much in line with zero-trust security paradigms, where the meaning of trust is never implicit and access policies are always re-assessed depending on identity, context and policy. Although the current literature offers great insights into the threats of clouds, secrets management, and IAM strategies, numerous researches discuss these elements separately. Substantial reviews are still necessary that can evaluate the effectiveness of integrated platform-native solutions within the context of increased cloud security.

Specifically, there has been little scholarly research that investigated the joint application of secrets management, managed identities, and centralized identity governance on one cloud ecosystem. This gap explains why it is important to consider the case of Azure Key Vault, Managed Identities, and Microsoft Entra as a security model that makes sense in a contemporary cloud-based environment.

3. Azure security architecture overview

In the Microsoft Azure, cloud security is designed on the basis of the model of shared responsibility and layers that explicitly outlines security responsibilities between the cloud service provider and the customer. In this paradigm, Microsoft will take the responsibility of securing the underlying infrastructure (physical data centers, networking and host operating systems) whereas customers will handle the responsibility of securing data, identities, applications, and access settings installed to the cloud environment [9]. This joint responsibility model implies a powerful native security service that enables customers to have solid identities and sensitive resources controls. The security architecture of Azure is built under the concept of a secure by design, wherein security controls are infused into the core services provided by Azure. Network isolation, encryption, monitoring, and identity-based access control are some of the main architectural features. Instead of focusing only on perimeter-based security measures, Azure puts identity in focus as the key security boundary, which is consistent with the current zero-trust principles [10]. This change is based on the increased realization that users, applications and services should be continuously authenticated and authorized regardless of their network location.

The security framework of Azure is based on identity and access control. Azure uses centralized identity management to verify users and workloads as well as implement the least-privilege access by role-based access control (RBAC). RBAC facilitates assigning permissions, at a fine-grained level, according to the pre-defined roles, as opposed to each individual, which minimizes administrative load, as well as limiting the chance of excessive permission [11]. This solution promotes scalable control over huge and detailed cloud deployments, where permission control by hand is no longer viable. Besides the enforcement of identity, Azure also employs extensive encryption systems to secure the data at rest and transit. Faith Platform-level encryption can be ensured, which implies using strong cryptographic algorithms to protect the stored data, and transport-layer security can be used to protect the communications between services. Nonetheless, the proper encryption of the information is inadequate without the safe management of keys. It is noted that inappropriate management of cryptographic keys is one of the most common vulnerabilities in cloud environments, which supports the necessity of the centralized and controlled management of key solutions [12].

4. Azure key vault – secure secrets management

Secrecy and assurance of cryptographic keys, secrets and certificates are important in cloud environments where applications often communicate with various services as well as external systems. Mishandling of sensitive credentials may result into serious breach of security in which unauthorized access of data and compromise of service can occur. The Azure Key Vault manages these issues and can be defined as an implementation of a centralized and secure service to manage secrets and apply stringent access control and auditing services [13]. Azure Key Vault is a service aimed at protecting three main categories of sensitive data: cryptographic keys, secrets, including passwords and API keys, and digital certificates. Such assets are secured with powerful encryption algorithms and both software-based security and hardware-based security support are provided with Hardware Security Modules (HSMs). Keyboards supported by HSM have increased protection since cryptographic content does not exit the secure hardware perimeter, that is why the chances of key extraction or manipulation are minimal [14]. This feature is especially significant to the organizations that have to work in controlled industries where high levels of assurance in cryptographic transactions are noted.

The authentication and fine-grained authorization are some of the policies that manage access to Azure Key Vault based on identities. Applications and users authenticate by using Azure identities instead of using fixed credentials and access secrets securely and auditably. Access control and policy enforcement mechanisms are based on roles where only authorized parties can carry out certain actions such as reading secrets or carrying out cryptographic functions [15]. This model is also in line with the least privilege principle and the harm to the least possible extent of people having compromised identities. The other considerable benefit of Azure Key Vault is the fact that it supports secure lifecycle management of keys. The studies have indicated that a weak key rotation and lifecycle control are weaknesses in cloud security implementation [16]. Azure Key Vault is able to provide automated key rotation, versioning, and expiration rules, eliminating the need to rely on manual operations and minimizing the possibility of error. These functions improve the security of operations as well as make it easier to meet requirements of numerous standards, including ISO 27001 and PCI DSS. Also, Azure Key Vault demonstrates modern secrets management by addressing the fundamental issues of confidentiality, integrity, and governance. The combined managed identities and Microsoft Entra as part of an integrated security model. It may help, through integration with identity services and support for hardware-backed security of secure cloud deployments.

In addition to core secrets protection, Azure Key Vault is of great importance in regulatory compliance and governance in the cloud environments. Numerous regulatory frameworks demand rigid management of cryptographic content, such as safe storage, limited access and audit trail. Research shows that centralized key management systems are necessary to comply with the requirements in cloud infrastructures because decentralized systems of key management are not always consistent and visible [17]. Azure Key Vault facilitates compliance through access policies, logs, and cryptographic isolation, which is provided by specific vaults. The other reason to consider about Azure Key Vault is that it has been integrated with cloud-native applications and DevOps workflows. Contemporary software development processes are strongly dependent on the principles of automation and continuous deployment that can potentially reveal secrets in case they are not handled in a secure manner. It has been noted that the integration of secrets into deployment pipelines or source code repositories continues to be a common security threat [18]. Azure Key Vault avoids this threat by enabling applications and automation code to access secrets in a secure manner during execution, thus avoiding the linking of sensitive information with application code and configuration files. Azure Key Vault also fulfills the needs of scalability and availability that are important to the enterprise cloud deployment. The features of high availability and geo-redundancy guarantee that even in case of the failure of the areas, cryptographic services are still available. Security-wise, the availability is one of the triad components of confidentiality-integrity-availability (CIA), and the problem with key management services may have a direct effect on the application security and reliability [19]. Azure Key Vault enhances the overall cloud-based system security posture by offering resilient and scalable key management functionality.

5. Managed identities – eliminating credential exposure

One of the security challenges that are hard to eradicate in cloud computing environments is credential management. Conventional authentication methods may have application software keep secrets, like usernames, passwords or access keys, which may accidentally leak out of a source code repository, configuration file or logging system. Credential leakage is reported by empirical research as the primary cause of cloud security breaches, especially in large-scale and automated environments [20]. The introduction of Managed Identities in Microsoft Azure was the solution to this problem since explicit credential handling does not exist anymore. Managed Identities allow Azure resources to get an automatically managed identity that one can use to securely authenticate to other Azure services. The Azure platform issues and maintains these identities and there is no need by the developers or administrators to generate or rotate the credentials or store it. Security wise, it has a considerable impact by minimizing the attack surface since credentials will not be visible to application code or configuration artifacts [21]. Authentication is, instead, done by short-lived tokens issued by the identity provider of Azure, which is more secure than long-lived static secrets.

Azure allows two kinds of identities, including system-assigned and user-assigned identities. System-assigned identities are closely linked to an individual Azure resource and are automatically disposed when the resource is deleted, which reduces the chances of orphaned identities. Instead, user-assigned identities are decoupled resources that may be reused within a variety of services, and therefore provide more flexibility with complex architectures. According to research on identity lifecycle management, identity provisioning and deprovisioning should be strictly regulated, so that privilege creep and unauthorized access are prevented [22]. Managed Identities are compatible with role-based access control of Azure. Access is controlled by assigning roles to the identity and not by fixing access privileges into applications. This disaggregation of identity and authorization eases the governance and promotes the least privilege principle. Research on best practices in cloud IAM underlines that it is crucial to limit the length and the extent of privileges as a means to lessen the effects of identity compromise [23]. Organizations can impose accurate access controls through managed identities where role assignments are scoped and operational efficiency remains efficient (Figure 1).

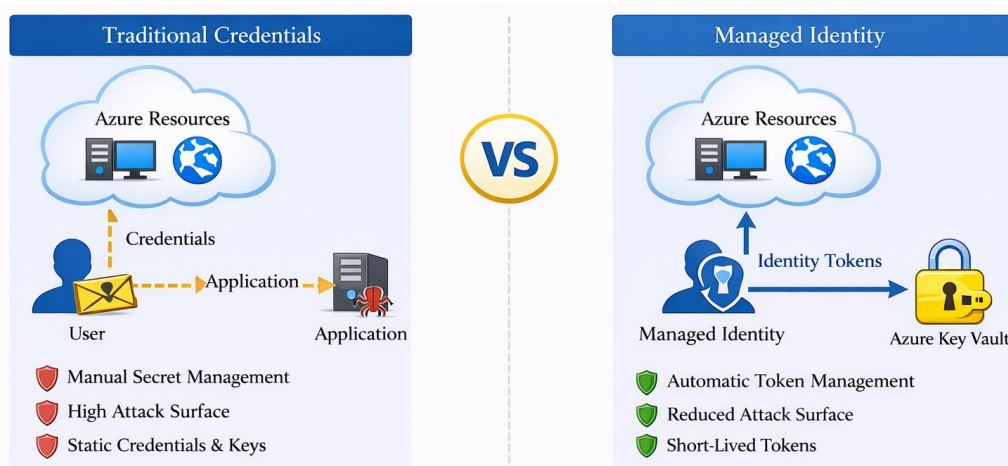


Figure 1: Authentication approach comparison.

This diagram is a comparison of the standard credential based authentication versus Managed Identity in Azure. It compares the dangers of the manual secret management and the unchanging credentials on the left to the advantages of the automated token management and minimal attack surface on the right.

6. Microsoft entra – identity governance and zero trust

With the increase in complexity of cloud environments and the subsequent growth in the number of users across organization and geographic scales, identity governance has taken a center-stage in cloud security. Microsoft Entra is a single identity and access management tool that is created to impose security in authentication, authorization, and administration of clouds and hybrid environments. Studies have shown that identity-based security models are necessary to reduce the contemporary threats especially credentials compromise and lateral movement attacks [24]. One of the important features of Microsoft Entra is that it supports the principles of Zero Trust security. Zero Trust presupposes that all users, devices and applications cannot be considered as trusted, even when it is located in a trusted network perimeter. Rather, it makes dynamic access decisions using identity, device posture, location and risk signals [25]. The Microsoft Entra model is used to implement this model by the use of conditional access policies that analyze contextual attributes before access is granted or denied. Such a dynamic enforcement will go a long way in discouraging the possibility of unauthorized access through stolen or re-used credentials.

The issue of access lifecycle management is also solved in identity governance of Microsoft Entra. In a big company, identity sprawl, as well as excess privileges might grow over time and heighten the risks of insider threats and unintentional abuse. Researchers note that automated identity governance controls, including access reviews, entitlement management and role certification, are essential to the continued operation of least-privilege access in dynamic cloud settings [26]. The Microsoft Entra also includes these mechanisms so

that the access rights are constantly assessed and modified according to the organizational policies. The next feature that must be discussed in relation to Microsoft Entra is the possibility to use multi-factor authentication (MFA) and passwordless authentication. Scholarly and practical studies have continued to reveal that MFA reduces considerably the success rate of credential-based attacks as it necessitates extra verification attributes to passwords [27]. Microsoft Entra also allows integrating biometric authentication, hardware tokens, and risk-based MFA, which enhance the assurance of the identity and enhance the experience of the user.

In architecture, Microsoft Entra is the core trust authority that allows secure communications between users, applications, and cloud services. Its support with Azure-native services, such as Azure Key Vault and Managed Identities, enables organizations not only to apply uniform policies to identities in workloads but also to execute access controls to sensitive resources securely. Microsoft Entra can support a comprehensive Zero Trust approach, which is consistent with current cloud security needs by combining governance. In general, Microsoft Entra is not just a directory service, but a platform that delivers a full-fledged identity governance and Zero Trust implementation environment. It is a core element in secure cloud architectures (Figure 2) because of its capabilities, which handle critical challenges of access sprawl, credential abuse, and enforcement of policies (Table 1).

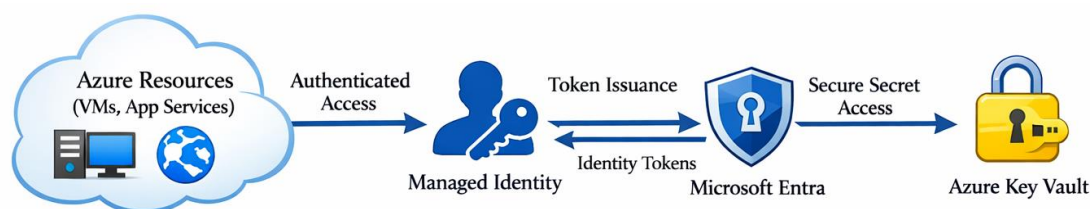


Figure 2: Baked-in Azure cloud security architecture.

This scheme is used to describe the flow of secure authentication and access in Azure. Azure Resources (VMs, App services) is authentication that is based on Managed Identity and acquires identity tokens at Microsoft Entra.

Table 1. Comparison of Azure key vault, managed identities, and microsoft entra in cloud security

Azure Security Component	Primary Function	Key Security Features	Security Benefits	Potential Limitations
Azure Key Vault	Secure storage and management of secrets, keys, and certificates	Encryption at rest and in transit, HSM support, access policies, audit logging	Protects sensitive credentials, supports compliance, centralizes key management	Risk of misconfiguration, dependency on proper access control policies
Managed Identities	Authentication for Azure resources without explicit credentials	Platform-managed identities, token-based authentication, RBAC integration	Eliminates credential exposure, reduces attack surface, simplifies authentication	Limited to supported Azure services, requires careful role scoping

Microsoft Entra	Identity governance and access management	Conditional access, MFA, identity lifecycle management, Zero Trust enforcement	Enforces least-privilege access, mitigates credential-based attacks, supports governance	Policy complexity, potential administrative overhead
------------------------	---	--	--	--

7. Challenges, limitations, and future directions

Although Azure Key Vault, Managed Identities, and Microsoft Entra offer strong security benefits, they also have several challenges and limitations. Configuration complexity is one of the major issues. Although such services are aimed at improving security, they may introduce vulnerabilities by default through improper configuration of access policy, role assignment, or condition access rule. Research shows that misconfigurations remain one of the primary causes of cloud security events, which tend to undermine the benefits of sophisticated security measures [28]. The other limitation is related to operational and organizational factors. Adopting identity-first and zero-trust security models will entail a transformation in the conventional security procedures, including sufficient expertise and governance procedures. Smaller organizations or teams that are less mature in cloud security might not be able to effectively control policy sprawl, identity lifecycle control, and continuous monitoring. Also, using platform-native services increases the risk of vendor lock-in, making multi-cloud environments less portable.

Technically, the performance overheads and dependencies on services may also be problematic. The identity verification, issuing tokens and policy evaluation add more layers to the process of flow access, and can affect latency in a high-throughput system. Studies indicate that there is still no close-ended solution to the security versus performance optimization when operating a large scale cloud deployment [29]. As a prospective viewpoint, upcoming changes in the field of cloud security will focus on the aspects of passwordless authentication, confidential computing, and AI-based identity risk detection. The effectiveness of integrated security models can also be improved with the help of improvements in automated policy management and cross-cloud identity federation. The consideration of usability, automation, and interoperability will be essential to the maximization of the long-term value of identity-centric cloud security architectures.

8. Conclusion

The identity-based and zero-trust models have been developed to address the increased complexity and threat landscape of modern cloud environments. The paper reviewed how Azure Key Vault, Managed Identities, and Microsoft Entra can offer an integrated and holistic cloud security framework. Azure Key Vault provides secure management of secrets and keys, Managed Identities eliminate the exposure of credentials through automated authentication, and Microsoft Entra implements identity and zero-trust access controls. The collective effect minimizes attack surfaces, increases compliance, and enables scalable security governance. The configuration and performance represent a major improvement over the conventional security approach. The rate of cloud adoption in the secure storage and access of sensitive information in distributed cloud settings.

References

- [1] Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4(1), 1–13.
- [2] Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., & Inácio, P. R. M. (2014). Security issues in cloud environments: A survey. *International Journal of Information Security*, 13(2), 113–170.
- [3] Jang, J., Han, D., Lee, S., & Kim, J. (2017). Secure key management in cloud systems using hardware security modules. *IEEE Transactions on Cloud Computing*, 5(3), 455–468.
- [4] Gambo, M. L., & Almulhem, A. (2026). *Zero Trust Architecture: A systematic literature review*. *Journal of Network and Systems Management*, 34, Article 25.
- [5] Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in cloud. *Journal of Network and Computer Applications*, 36(1), 42–57.
- [6] Behl, A., & Behl, K. (2017). *Cybersecurity and cyberwar: What everyone needs to know*. *Oxford University Press*, 1(1), 1–256.
- [7] Myers, A., Shull, F., & Weinstock, C. (2018). Secure configuration management in cloud computing. *IEEE Software*, 35(2), 72–79.
- [8] Ferraiolo, D., Kuhn, D. R., & Chandramouli, R. (2016). Role-based access control. *Computer*, 49(2), 83–87.
- [9] Pearson, S. (2013). Privacy, security and trust in cloud computing. *Privacy and Security for Cloud Computing*, 1(1), 3–42.
- [10] Kindervag, J. (2010). Build security into your network's DNA: The zero trust network architecture. *Forrester Research*, 1(1), 1–14.
- [11] Sandhu, R., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *Computer*, 29(2), 38–47.
- [12] Zhang, Q., Chen, M., Li, L., & Li, S. (2018). A secure cloud storage system based on encryption and access control. *Journal of Cloud Computing*, 7(1), 1–14.
- [13] Gaw, S., Felten, E. W., & Fernandez-Kelly, P. (2006). Secrecy, flagging, and paranoia: Adoption criteria in encrypted email. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1(1), 591–600.
- [14] Dandass, Y. S., & King, S. T. (2016). Hardware security modules for cryptographic key protection. *IEEE Security & Privacy*, 14(2), 14–22.
- [15] Hu, V. C., Kuhn, D. R., Ferraiolo, D. F., & Voas, J. (2015). Attribute-based access control. *Computer*, 48(2), 85–88.
- [16] Barker, E. (2019). Recommendation for key management: Part 1—General. *NIST Special Publication*, 800(57), 1–147.
- [17] Takabi, H., Joshi, J. B. D., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, 8(6), 24–31.

- [18] Rahman, M. M., Williams, L., & Snipes, W. (2016). Security smells in infrastructure as code. *Proceedings of the 8th International Workshop on Cooperative and Human Aspects of Software Engineering*, 1(1), 103–110.
- [19] Stallings, W., & Brown, L. (2018). Computer security: Principles and practice. *Pearson Education*, 3(1), 1–840.
- [20] Shostack, A. (2014). Threat modeling: Designing for security. *Wiley*, 1(1), 1–432.
- [21] Almutairi, A., Sarfraz, M., Basalamah, S., Aref, W., & Ghafoor, A. (2017). A distributed access control architecture for cloud computing. *IEEE Software*, 29(2), 36–44.
- [22] Bertino, E., & Takahashi, K. (2010). Identity management: Concepts, technologies, and systems. *Artech House*, 1(1), 1–350.
- [23] Garrison, C. P., & Ncube, M. (2011). A longitudinal analysis of data breaches. *Information Management & Computer Security*, 19(4), 216–230.
- [24] Crampton, J., & Sellwood, J. (2014). Path conditions and principal matching: A new approach to access control. *ACM Transactions on Information and System Security*, 17(3), 1–34.
- [25] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. *NIST Special Publication*, 800(207), 1–58.
- [26] Fuchs, L., Pernul, G., & Sandhu, R. (2011). Roles in information security—A survey and classification of the research area. *Computers & Security*, 30(8), 748–769.
- [27] Florencio, D., & Herley, C. (2010). A large-scale study of web password habits. *Proceedings of the 16th International World Wide Web Conference*, 1(1), 657–666.
- [28] Gupta, E. (2025). ENABLING ANALYTICS GOVERNANCE IN AGILE PRODUCT TEAMS: A SCALABLE TAGGING AND QA FRAMEWORK. *International Journal of Applied Mathematics*, 38(7s), 1161-1172.
- [29] Fernandes, D. A. B., Freire, M. M., Inácio, P. R. M., & Gonçalves, J. F. (2015). Performance analysis of security mechanisms in cloud computing. *Future Generation Computer Systems*, 50, 1–12.