International Journal of Multidisciplinary Research and Publications
ISSN (Online): 2581-6187

# Mitigating Credential-Based Attacks in Google Cloud: A Proactive Approach to Identity and Access Management and Multi-Factor Authentication

Nagesh Manmeeth[1], Simranjeeth Singh[2], Praveen Kaur[3], Neha Nikhath[4]
Department of Computer Science and Engineering, Chandigarh University, Mohali, Punjab, India-140413
Email address: faheemneha153@gmail.com

***Abstract*—***Implementing proactive security measures for Google Cloud Platform becomes essential due to the rising complexity of credential-based cloud attacks. The basic password-dependent security models alongside standard access controls show insufficient capability against current attack types, including phishing intrusion, brute-force attacks, and credential stuffing. This investigation presents a proactive security method for Google Cloud credential-based attacks through IAM strategies that combine with advanced MFA protection mechanisms. The paper explains Google Cloud IAM principles and demonstrates how role-based access control creates smaller impact areas during security breaches. This research evaluates progressive MFA solutions along with hardware security keys and biometric authentication mechanisms, yet it examines traditional single-factor authentication account weaknesses for keeping out complex attacks. A proposed architectural framework presents a secure structural design that unites IAM with MFA to form multiple usability barriers that defend Google Cloud infrastructures from credential-based assaults.*

***Keywords*—** *Access control: Biometric authentication: Credential-based attacks: Google Cloud Platform: Identity and Access Management (IAM): Multi-Factor Authentication (MFA): Phishing: Role-based access control (RBAC): Security architecture.*

## I. INTRODUCTION

Through cloud computing, organizations can now access innovative features for their data management, which combines scalability with flexibility and cost-effectiveness [11]. Cloud infrastructure has become an attractive target for hackers because the increased adoption of cloud technology has created new security threats. User credentials serve as one of the most prevalent and damaging threats since adversaries use them to gain unauthorized entry to critical resources. Google Cloud Platform provides extensive security solutions to organizations, yet organizations need active implementation and configuration of these tools to properly defend against credential-based attacks. Advancing industry security demands a comprehensive security system to handle the developing threats in the market [1]. This paper emphasizes the importance of establishing an advanced strategy to protect Google Cloud infrastructures using strong mechanisms for identity and access management and multi-factor authentication systems. The controls of IAM serve organizations by defining digital identity management for users as well as applications and devices, which grant specific resource access to authorized entities [3]. As part of Google Cloud functionality, IAM provides administrators with precise control over access permissions that determine which users can operate on specific resources with their assigned permissions. Authentication security controls have gained increased importance due to the speedy growth of the Internet, according to [9]. The security measure MFA ensures safe access by prompting users to provide multiple authentication methods before entry so that compromised authentication factors remain ineffective. Identity and Access Management in Google Cloud

The foundational security element of Google Cloud Identity and Access Management gives organizations complete control over resource access at detailed levels. Through an effective deployment of IAM, organizations can safeguard their systems by granting users permissions at the level required for their work tasks, which reduces the damage of account compromise incidents [3]. Through the IAM feature, administrators can create roles consisting of permissions used to determine user capabilities for defined cloud resources. The roles within the IAM framework become assignable to users and groups as well as service accounts, thus offering scalable access control management for organizations across different levels. The IAM system creates a unified platform to regulate access permissions of user identities, where administrators can conduct simple audits and monitor user activities. IAM maintains integration with Google Cloud services, which include Cloud Storage, together with Compute Engine and BigQuery, to deliver continuous access control throughout the entire cloud environment. Any organization that adopts remote work must prioritize IAM capabilities to guarantee all users maintain secure access to their company resources. Enterprise identity management and cross-network management functions through IAM systems, which represent information systems [5, 6]. The urgent requirement for adaptable access control models became essential because both remote work strategies and advanced cloud environments have expanded in recent times.

Managers should implement System-Specific Policy and Access Control Policy alongside developing employee trust and performing overlapping risk management with access control alongside proper spending and obtaining liability or insurance policy protection for managing access controls within the organization. Figure 1 shows the different types of access control for the management strategy.



Nagesh Manmeeth, Simranjeeth Singh, Praveen Kaur, and Neha Nikhath, "Mitigating Credential-Based Attacks in Google Cloud: A Proactive Approach to Identity and Access Management and Multi-Factor Authentication," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 8, Issue 1, pp. 33-36, 2025.


Figure 1: Management Strategy

The system operates by abandoning perimeter security measures to protect both users and devices and provides secure network access no matter the insecure connectivity conditions. Cloud IAM follows a hierarchical model in Google Cloud, where policies established at the organizational level spread throughout all project resources and individual elements. The inheritance model creates efficient access management because administrators set general organization-level policies before adjusting them specifically per lower organizational levels. The framework produces an entire asset performance overview that creates interdepartmental transparency for knowledgeable strategic decision-making.

## II. Multi-Factor Authentication for Credential Protection

Users must present multiple authentication factors through Multi-Factor Authentication to obtain access authorization, which strongly boosts security measures. When applied properly, MFA establishes multiple security checkpoints that protect against unauthorized sign-ins despite factors such as passwords being discovered by attackers. The method stands out from single-factor authentication since it requires multiple security checks beyond username-password combinations, which exposes the system to phishing attacks, brute-force tactics, and password duplication [15, 27]. MFA performs identity authentication by evaluating three security criteria, which are your personal password, your physical security token, and your biological authentication. Knowledge-based factors consist of passwords or security questions, while ownership factors serve as smart cards or smartphones, and biometric factors require fingerprints or facial recognition [14, 26]. Users can select from a range of MFA approaches in Google Cloud due to its support of one-time passwords from authenticator applications, together with hardware security keys and Google Prompt verification options. Organizations must mandatorily implement MFA protection for everyone, and specifically for employees with privileges to critical assets, because this reduces credential-based attack vulnerabilities. MFA establishes improved security through its dual authentication protocol that obstructs attackers from breaching the system. Organizations implement multi-factor authentication within their systems through their access controls to safeguard stored information according to [10]. Software development teams running the systems choose which authentication method should be deployed. MFA should serve as an authentication interface that ensures fast, reliable access through user-friendly processes for service entry [16].

## III. Mitigating Credential-Based Attacks

Old-fashioned credential bombings represent major cloud security perils because they permit unauthorized system entry by exploiting faulty credentials and weak authentication [17]. Businesses need to employ a proactive IAM approach with MFA implementation to defend their sensitive Google Cloud resources against imminent attacks [18]. The implementation of proactive security practices lets organizations both decrease their vulnerable areas and lower the extent of successful attacks [16]. Companies need to create stringent password requirements that demand complex passwords, schedule periodic password changes, and block the re-use of passwords to minimize password vulnerabilities. Through the Identity Platform, organizations can use Google Cloud to set robust password requirements and monitor credential compromise. Users need security awareness training, which shows them how to recognize phishers through normal social engineering attacks and lessons on detecting dangerous email attachments and URLS [14]. Organizations need to establish account lockout protocols that will disable user accounts automatically when users enter multiple incorrect login attempts. Security data protection demands a consolidated implementation of multiple defense solutions according to [15].


Figure 2: Cloud Computing used in cybersecurity

The graphical authentication approach functions as an alternative solution to traditional methods of multi-factor authentication [4]. Figure 2 shows the uses of Cloud security for cybersecurity [7]. User behavior and access monitoring activities enable the detection of abnormal actions that indicate compromised accounts [14, 25, 28]. Using Google Cloud Security Command Center, organizations can track their cloud infrastructure for security threats and unauthorized activities. Statistical research confirms that organizations should automatically enable MFA for commercial accounts to enhance their cybersecurity framework [10, 21].



Nagesh Manmeeth, Simranjeeth Singh, Praveen Kaur, and Neha Nikhath, "Mitigating Credential-Based Attacks in Google Cloud: A Proactive Approach to Identity and Access Management and Multi-Factor Authentication," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 8, Issue 1, pp. 33-36, 2025.

The cloud computing practice brings substantial advantages through its scalability and cost effectiveness, yet security and incident response capabilities remain insufficient according to [6]. Security researchers have identified an increasing number of system flaws, which have led to daily security advisory publications [8]. Organizations persistently face major hurdles in protecting their cloud-based data and applications with both integrity, full availability, and absolute confidentiality [12. 22].

According to Ajish, in 2024, cloud-based cyberattacks grew by almost 48% during 2022 because cloud services have become more lucrative targets for cybercriminals. Cloud adoption gain continues to rise, so organizations need to emphasize implementing advanced security protocols to defend their cloud systems from new security dangers [18, 23]. The defense mechanism known as cloud security protects all elements of data, software, and infrastructure that exist in public, private, and hybrid cloud environments. New hacking tools that target cloud computing have increased interest in cybersecurity development, according to [19]. The protection of cloud networks against attacks becomes most effective when intrusion detection systems operate through networks in association with anomaly detection methods [20, 29].

## IV. Conclusion

The protection of Google Cloud from credential-based attacks demands a proactive method that unites strong IAM approaches with MFA. A combination of strong password standards and user-enforced MFA to secure all accounts, security training programs for users, and active user behavior monitoring enables businesses to decrease their vulnerabilities. The security approaches of organizations must remain attentive because cloud environments continue to develop, and new security threats and weaknesses emerge. Organizations must dedicate their resources to cybersecurity protection because they speed up digital transformation by using mobile devices combined with cloud services, social media, and Internet of Things platforms. Businesses need to develop proactive security measures for their technical infrastructure and data since they face increasingly advanced cyberattacks. Strong cybersecurity investments protect company data as well as enable business operation continuity while building client confidence. Strong security postures rely on staying updated about advancing cyber tactics and industry-leading practices since cyber threats persist in becoming more complex and advanced. Continuous improvement is essential for cybersecurity because businesses, technologies, and cyber threats undergo constant changes.

Cloud security stands as a top priority today because organizations heavily depend on cloud services for their data storage, application operations, and business activities. Increasing cyberattack frequencies coupled with advanced techniques force organizations to adopt preventive security measures for defending their cloud infrastructure from unauthorized entry, data breaches, and other security threats. Organizations should adopt a 'need-to-know' security methodology as the foundation for their protection approach, which effectively defends enterprise information and stops breaches. Through cloud security mechanisms, organizations maintain data and application confidentiality and integrity, as well as system availability, which lets them execute their operations with complete trust [13, 24]. Organizations that put in place strong security measures avoid data breach costs, comply with industry regulations, and protect their reputation. The practices and technologies of Cybersecurity function to protect both networks, computer systems, and data from cyberattacks. Organizations that use effective cybersecurity measures can safeguard their sensitive information while maintaining continuous operations and fostering customer trust. Organizations, regardless of their size, require cybersecurity to manage risks because it reduces financial and operational damage from cyberattacks. The combination of networked systems known as clouds encounters the same security problems associated with computers and networks, including requirements for data protection and data integrity, as well as system uptime.

## References

[1] Ahmadi, S. (2024). Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. Journal of Information Security, 15(2), 148. https://doi.org/10.4236/jis.2024.152010

[2] Almorsy, M., Grundy, J., & Müller, I. (2016). An Analysis of the Cloud Computing Security Problem. In arXiv (Cornell University). Cornell University. https://doi.org/10.48550/arxiv.1609.01107

[3] Addula, S. R., & Sajja, G. S. (2024, November). Automated Machine Learning to Streamline Data-Driven Industrial Application Development. In 2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES) (pp. 1-4). IEEE.

[4] Baseer, S., & Charumathi, K. S. (2024). Multi-Factor Authentication: A User Experience Study. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4840295

[5] DiMicco, J. M., & Millen, D. R. (2007). Identity management (p. 383). https://doi.org/10.1145/1316624.1316682.

[6] V. K. Kasula et al., "Federated Learning with Secure Aggregation for Privacy-Preserving Deep Learning in IoT Environments," 2025 IEEE Conference on Computer Applications (ICCA), Yangon, Myanmar, 2025, pp. 1-7, doi: 10.1109/ICCA65395.2025.11011120.

[7] M. Yenugula et al., "A Graph Neural Diffusion Network for Sophisticated Persistent Threat Hunting in IoT Environments," 2025 IEEE Conference on Computer Applications (ICCA), Yangon, Myanmar, 2025, pp. 1-6, doi: 10.1109/ICCA65395.2025.11011108.

[8] A. R. Yadulla et al., "Enhanced Cybersecurity Entity Recognition Using DeBERTa, Transformer-CNN Hybrids, and BiLSTM-Softmax," 2025 37th Conference of Open Innovations Association (FRUCT), Narvik, Norway, 2025, pp. 323-330, doi: 10.23919/FRUCT65909.2025.11008057.

[9] B. Konda et al., "Enhancing Traceability and Security in mHealth Systems: A Proximal Policy Optimization-Based Multi-Authority Attribute-Based Encryption Approach," 2025 29th International Conference on Information Technology (IT), Zabljak, Montenegro, 2025, pp. 1-6, doi: 10.1109/IT64745.2025.10930307.

[10] P. Pawar et al., "Exploring Blockchain-Enabled Secure Storage and Trusted Data Sharing Mechanisms in IoT Systems," 2025 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI), Gwalior, India, 2025, pp. 1-6, doi: 10.1109/IATMSI64286.2025.10984499.

[11] Gander, M., Felderer, M., Katt, B., Tolbaru, A., Breu, R., & Moschitti, A. (2013). Anomaly Detection in the Cloud: Detecting Security Incidents via Machine Learning. In Communications in Computer and Information Science (p. 103). Springer Science+Business Media. https://doi.org/10.1007/978-3-642-45260-4_8.

[12] Kasula, V.(2024). Leveraging Deep Learning Techniques for Enhancing Financial Security Systems: A Comprehensive Review of Methods,

Applications, and Challenges. International Journal of Communication Networks and Information Security (IJCNIS), 16(5), 969–978.
[13] R. Azmeera et al., "Enhancing blockchain communication with named data networking: A novel node model and information transmission mechanism," J. Recent Trends Comput. Sci. Eng. (JRTCSE), vol. 10, no. 1, pp. 35–53, 2022.
[14] Pawar, P. P., Kumar, D., Meesala, M. K., Pareek, P. K., Addula, S. R., & KS, S. (2024, November). Securing Digital Governance: A Deep Learning and Blockchain Framework for Malware Detection in IoT Networks. In 2024 International Conference on Integrated Intelligence and Communication Systems (ICIICS) (pp. 1-8). IEEE.
[15] C. Tumma et al., "Data Security and Privacy Protection in Artificial Intelligence Models: Challenges and Defense Mechanisms," Int. J. Sci. Res. Eng. Manag., vol. 7, no. 12, pp. 1–11, 2022.
[16] Addula, S. R., Tyagi, A. K., Naithani, K., & Kumari, S. (2024). Blockchain-Empowered Internet of Things (IoTs) Platforms for Automation in Various Sectors. Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing, 443-477.
[17] Rachana, C. R., Banu, R., Ahammed, G. F. A., & Parameshachari, B. D. (2017). Cloud Computing – A Unified Approach for Surveillance Issues. In IOP Conference Series Materials Science and Engineering (Vol. 225, p. 12073). IOP Publishing. https://doi.org/10.1088/1757-899x/225/1/012073.
[18] Konda, B. (2024). Explore Data Mining (DM) Techniques That Data Scientists Adopt in IT.
[19] Pawar, P. P., Kumar, D., Ananthan, B., Christopher, S. B., & Surya, R. (2024, May). An advanced Wasserstein-enabled generative adversarial network enabled attack detection for blockchain-Assisted Intelligent Transportation System. In 2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT) (pp. 1-6). IEEE.
[20] Yenugula, M. (2024). Challenges With Accountability, Trust & System Security in Google Cloud Platform (GCP).
[21] Sachdev, A., & Bhansali, M. (2013). Enhancing Cloud Computing Security using AES Algorithm. In International Journal of Computer Applications (Vol. 67, Issue 9, p. 19). https://doi.org/10.5120/11422-6766
[22] G. S. Nadella et al., “Generative AI-Enhanced Cybersecurity Framework for Enterprise Data Privacy Management,” Computers, vol. 14, no. 2, p. 55, Feb. 2025. doi:10.3390/computers14020055.
[23] Yadulla, A. R. (2024). A qualitative approach to data breaches in mobile devices.
[24] S. Ayyamgari et al., "Quantum Computing: Challenges and Future Directions," Int. J. Adv. Res. Sci. Commun. Technol., vol. 3, no. 3, pp. 1343–1347, 2023.
[25] S. Menon et al., “Streamlining task planning systems for improved enactment in contemporary computing surroundings,” SN Computer Science, vol. 5, no. 8, Oct. 2024. doi:10.1007/s42979-024-03267-5
[26] Gonaygunta, H., Nadella, G. S., Meduri, K., Pawar, P. P., & Kumar, D. (2024). The Detection and Prevention of Cloud Computing Attacks Using Artificial Intelligence Technologies. International Journal of Multidisciplinary Research and Publications (IJMRAP), 6(8), 191-193.
[27] Maturi, M. H. (2024). Optimizing energy efficiency in edge-computing environments with dynamic resource allocation. environments, 13(07), 01-08.
[28] Pawar, P. P., Kumar, D., Ananthan, B., Pradeepa, A. S., & Selvi, A. S. (2024, May). An efficient ddos attack detection using attention based hybrid model in blockchain based SDN-IOT. In 2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT) (pp. 1-5). IEEE.
[29] B. Y. R. Thumma et al., "Cloud Security Challenges and Future Research Directions," Int. Res. J. Mod. Eng. Technol. Sci., vol. 4, no. 12, pp. 2157–2162, 2022.