Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 05 Issue: 06 | June-2025

Securing Data Endpoints in Google Cloud: A Data-Driven Approach to Anomaly Detection and Threat Mitigation

Mamatha Gugulothu

Department of Computer Science and Engineering, Vaagdevi College of Engineering

---***---

Abstract - Using Google Cloud requires a complete defensive plan combining data-based anomaly alerts with early threat response systems to protect confidential information. Modern cloud environments require active security monitoring because their complexity continues to increase while cyber threats become more complex. Traditional security practices fail to handle the fluid characteristics of cloud-based data breaches because organizations must move towards security systems based on data intelligence. The research presents an analysis of advanced anomaly detection methods through statistical analysis, machine learning algorithms, and behavior analytics for observing and responding to abnormal data access patterns and security incidents in Google Cloud infrastructures. Organizations that deploy robust anomaly detection systems create better capabilities for threat detection, along with threat mitigation, and ensure compliance with strict regulatory requirements. Companies require integrated security platforms because cyber dangers combine with financial problems and system breakdowns within a single detection foundation.

Key Words: Cloud Computing, Security, Data Endpoint Security, Identity Access Control

1. INTRODUCTION

Cloud computing has undergone rapid expansion, which has transformed data handling practices, but it has brought forth new security problems [1]. Organizations, both small and large, frequently use the Google Cloud Platform because it provides complete data storage and analytical capabilities alongside management services. Cloud infrastructure systems face various attacks due to their shared infrastructure, while the rising data volume and processing speed create obstacles for detecting and responding to security incidents. The identification of abnormal activities inside cloud networks depends on data anomaly detection systems. Cloud security measures have limitations against updated cyber threats in cloud infrastructure, so organizations must use data analytics to actively stop and block potential threats [23].

The pay-per-use model, along with the internet dependency of cloud computing, which stores user data in provider servers, requires enhanced security measures. Specialized security tools must address cross-VM side-channel attacks because cloud environments contain unique security challenges that need exact attention to their complexities and specific threats. Anomaly detection methods used for cloud security investigations have demonstrated their inadequate capabilities, thereby leading researchers to develop advanced solutions [13].

Cloud security requires anomaly detection techniques to identify rare patterns and security breaches in cloud infrastructure. The identification of an anomaly marks the occurrence of irregular behavior, which reveals potential failures and operational weaknesses or security hazards. Analyzing extensive datasets allows the detection of anomalies by identifying deviations from normal patterns, according to [9]. Anomaly detection serves multiple applications, which include fraud detection alongside cybersecurity and fault detection. AI systems that detect anomalies are developing autonomous capabilities along with self-learning abilities to identify fresh attack paths without demanding large-scale system retraining, according to [25]. Cloud service dependency necessitates robust measures for guaranteeing reliability, security, and availability. Many industries now use cloud computing as the demand increases, which requires enhanced cybersecurity solutions to protect cloud infrastructure and network systems.

2. Data Endpoint Security in Google Cloud

The Google Cloud platform offers its clients access to multiple data storage and processing solutions, such as Cloud Storage, together with BigQuery and Cloud SQL. A thorough approach must be implemented to secure data endpoints, which must address security risks between unauthorized access and data breaches and compliance violations. Strong access regulations, along with encryption procedures and surveillance protocols, serve as required protective measures for sensitive Google Cloud data storage systems. Some organizations hesitate to deliver full cloud computing adoption because of their security concerns regarding data protection. Businesses confront substantial technical challenges when they aim to provide data and application confidentiality together with integrity and availability in cloud-based systems [11]. Security measures for cloud environments require the solution of weaknesses that exist during data storage and transmission operations [20].

Identical access control systems play a vital role in maintaining endpoint data accessibility by defining user permissions. Authenticating users with multiple factors establishes a protection barrier against unauthorized personnel who seek access to critical data. Data encryption functions as an integral security technique that defends information both when it rests and while it moves. The encryption process blocks unauthorized parties from accessing important data because the encryption methods remain operative through storage or network infrastructures. Data Loss Prevention solutions function by stopping the unauthorized export of sensitive information outside the organization. The monitoring process must remain active alongside logging operations because they enable security incident detection and response capabilities. Monitoring logs releases important information about both the activities of users and system operations and potential security hazards [21].

A surge in cloud customers has coincided with an increase in malicious activities throughout the cloud domain [8]. The security protection of sensitive information requires cloud computing security protocols [10]. Cloud service providers need to establish rigorous defensive security protocols that guard against breaches of customer data, along with unauthorized access attempts. [4]. Figure 1 talks about security and data management.

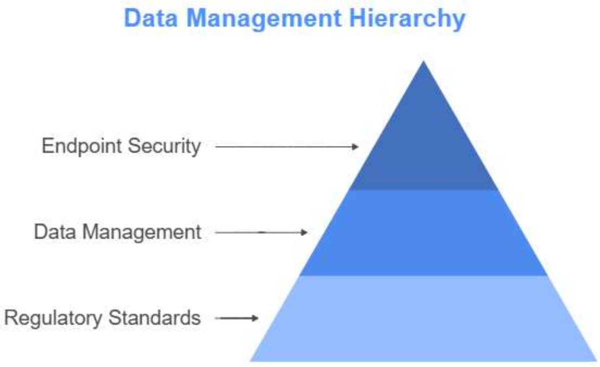


Figure 1: Data management

The management of data needs to follow strict regulatory standards because it represents a vital element of endpoint security. An organization needs to follow specific privacy regulations that include HIPAA, in addition to GDPR and PCI DSS, based on its data storage types during its Google Cloud presence. Cloud providers are required to establish suitable security controls that match specific requirements [15].

3. ANOMALY DETECTION APPROACH

The procedure of anomaly detection through data relies on machine learning algorithms to analyze unusual patterns within data [5]. The algorithms use past data for training purposes to master the typical system activity patterns before they monitor unseen deviations from normal operation [22, 29]. The detection process depends on specific contextual information [16]. A system of three anomaly groups exists: individual points, context-dependent anomalies, and collective deviations [14]. The three fundamental approaches of machine learning for anomaly detection include supervised learning, along with both semi-supervised and unsupervised methods [12].

For anomaly detection work, machine learning offers several valid algorithms, which consist of clustering algorithms, classification algorithms, and time series analysis algorithms. The neural network architecture known as autoencoders functions for anomaly detection through deep learning, where it reconstructs the original input at the output [19].

Autoencoders generate reconstruction errors during test-data reconstruction, which signifies the presence of anomalies [6].

How to choose an algorithm comes from both the data analysis type and the system requirements [10]. The detection methods differ in their benefits and constraints based on model-driven or data-driven operation alongside analytics functions and their application to image, video, or time-series dataset analysis [5]. The main goal of metaheuristics in detecting anomalies in big data consists of optimizing machine learning algorithms. By integrating the metaheuristic method, the algorithm becomes more efficient and develops enhanced precision during its search for optimal parameters.

Vast dataset management capability of Metaheuristics makes them essential tools for conducting anomaly detection operations in the big data era [7]. The isolation forest algorithm stands out for anomaly detection since it works effectively to identify anomalies without needing complicated pre-processing or modeling of the data [24]. The algorithm uses random partitioning of data space to measure partition counts, which isolate each point until each point requires few partitions, and identify anomalies from these points [26, 27]. The isolation forest method decreases the expense of processing big datasets. Therefore, it makes anomaly detection systems more practical for real-world use [3].

Anomaly detection allows users to detect distinctive data points that deviate largely from standard behavior so they can identify valuable information hidden in data repositories [6]. Significant but unusual events, such as network infiltrations, together with fraudulent activities, manifest as anomalies according to [17].

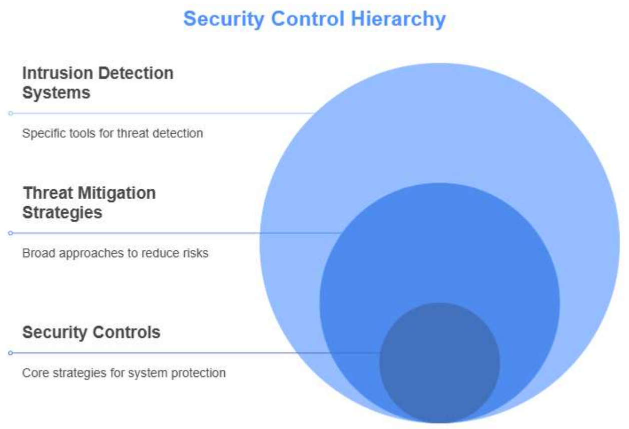
Autoencoders function as neural networks that learn to reproduce their received data. Autoencoders achieve the capability of detecting significant data characteristics through their ability to compress and reconstruct data in reduced latent dimensional spaces [14].

4. THREAT MITIGATION STRATEGIES

Security controls form part of threat mitigation strategies, which protect systems from security dangers and decrease their harmful effects. Intrusion detection systems serve as essential tools for defense against security threats and their effect [13]. By merging anomaly-based detection with misuse detection methods, hybrid intrusion systems improve their ability to identify security events while decreasing false alert rate reports [2].

Next-generation threat detection systems keep watch over network analytics and system logs to find abnormal activity while employing automatic responses through dangerous traffic blocking procedures and contaminated system isolation protocols [18].

The organization relies on incident response plans to define security incident management processes. The security plans must provide documented procedures to find security incidents, followed by steps to contain them before elimination, while enabling the restoration process [17, 28]. The intelligence platforms generate helpful data regarding current threats and present vulnerabilities. Figure 2 shows the security control related to intrusion and threat management.


Security Control Hierarchy
Intrusion Detection Systems
Specific tools for threat detection
Threat Mitigation Strategies
Broad approaches to reduce risks
Security Controls
Core strategies for system protection

5. CONCLUSIONS

Data endpoint security in Google Cloud can only be accomplished through an integrated implementation of defense methodologies that combine data and threat protection methods alongside anomaly detection and response prevention strategies. Organizations can protect their Google Cloud data from breaches while maintaining its confidentiality, integrity, and availability by implementing the mentioned measures.

Organizations need to establish new protection techniques across their systems to stop additional losses caused by these attacks to their business, along with customer information and company reputation. To combat new and emerging cyber threats, cybersecurity solutions need continuous updates on their defensive methods. Security protection demands the creation of adaptable security frameworks that possess robust capabilities. Traditional security methods prove insufficient to stop present-day threats due to attackers who create advanced threat procedures. Research success emerges through various interdisciplinary investigations, which help scientists develop comprehensive and powerful security solutions. These solutions defend against threats in the developing risks of the digital world while protecting individuals and their network infrastructure. To achieve complete security protection, organizations should adopt defense-in-depth techniques that utilize multiple security barriers. Organizations must conduct constant security audits and penetration tests to discover vulnerabilities that threaten the system. Robust authentication techniques form a critical element for protecting cloud environments, according to the survey reports. Organizations need to abandon traditional perimeter security models because cloud-based cyberattacks will increase by 48% in 2022. The security requirements demand immediate real-time threat prevention capabilities, which can be achieved by implementing machine learning and artificial intelligence systems into security networks. Organizations that use these approaches will enhance their cybersecurity position and minimize the potential for cyberattacks.

REFERENCES

1. Al-amri, R., Murugesan, R. K., Man, M., Fareed, A., Al-Sharafi, M. A., & Alkahtani, A. A. (2021). A Review of Machine Learning and Deep Learning Techniques for Anomaly Detection in IoT Data [Review of A Review of Machine Learning and Deep Learning Techniques for Anomaly Detection in IoT Data]. Applied Sciences, 11(12), 5320. Multidisciplinary Digital Publishing Institute. https://doi.org/10.3390/app11125320
2. 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.
3. 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.
4. Thumma, B. Y. R., Ayyamgari, S., Azmeera, R., & Tumma, C. (2022). Cloud Security Challenges and Future Research Directions. International Research Journal of Modernization in Engineering Technology and Science, 4(12), 2157-2162.
5. 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.
6. Vadakkethil, S. E., Polimetla, K., Alsalami, Z., Pareek, P. K., & Kumar, D. (2024, April). Mayfly Optimization Algorithm with Bidirectional Long-Short Term Memory for Intrusion Detection System in Internet of Things. In 2024 Third International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE) (pp. 1-4). IEEE.
7. 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.
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. Sajja, G. S., et al. (2024, November). Automation using robots, machine learning, and artificial intelligence to enhance production and quality. In 2024 Second International Conference on Computational and Characterization Techniques in Engineering & Sciences (IC3TES) (pp. 1–4). IEEE.
10. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection [Review of Anomaly detection]. ACM Computing Surveys, 41(3), 1. Association for Computing Machinery. https://doi.org/10.1145/1541880.1541882
11. Pawar, P. P., Kumar, D., Ananthan, B., Christopher, S. B., & Surya, R. (2024, May). An advanced Wasserstein-enabled generative adversarial network enables attack detection for blockchain-assisted Intelligent Transportation systems. In 2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT) (pp. 1-6). IEEE.
12. V. K. Kasula et al., "Enhancing Hyperledger Fabric Security with Lightweight Post-Quantum Cryptography and National Cryptographic Algorithms," 2025 37th Conference of Open

Innovations Association (FRUCT), Narvik, Norway, 2025, pp. 93-99, doi: 10.23919/FRUCT65909.

13. Daniel, V. A. A., Vijayalakshmi, K., Pawar, P. P., Kumar, D., Bhuvanesh, A., & Christilda, A. J. (2024). Enhanced affinity propagation clustering with a modified extreme learning machine for segmentation and classification of hyperspectral imaging. E-Prime-Advances in Electrical Engineering, Electronics and Energy, 9, 100704.
14. Kumar, N., Addula, S. R., Seranmadevi, R., & Tyagi, A. K. (2025). Advanced Banking Solutions for Industry 5.0: From Industry's Perspective. In *Creating AI Synergy Through Business Technology Transformation* (pp. 1-24). IGI Global.
15. A. R. Yadulla et al., "Lightweight Neural Networks for Adversarial Defense: A Novel NTK-Guided Pruning Approach," 2025 37th Conference of Open Innovations Association (FRUCT), Narvik, Norway, 2025, pp. 331-337, doi: 10.23919/FRUCT65909.2025.11008002.
16. 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
17. 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
18. 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
19. Tumma, C., Azmeera, R., Ayyamgari, S., & Thumma, B. Y. R. (2022). Data Security and Privacy Protection in Artificial Intelligence Models: Challenges and Defense Mechanisms. International Journal of Scientific Research in Engineering and Management, 7(12), 1-11.
20. Yadulla, A. R., Konda, B., & Kasula, V. K. (2025). Blockchain for Secure Communication. In S. Alangari (Ed.), Blockchain Applications for the Energy and Utilities Industry (pp. 103-140). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-2439-5.ch006.
21. 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.
22. 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.
23. Meesala, M. K. (2024). Security Policy Compliance Among Remote Workers Using BYOD Policies.
24. Kasula, V. K. (2024). Awareness of Cryptocurrency Scams (Doctoral dissertation, University of the Cumberlands).
25. Konda, B. (2022). The Impact of Data Preprocessing on Data Mining Outcomes. World Journal of Advanced Research and Reviews, 15(3): 540-544
26. Yenugula, M. (2023). Boosting Application Functionality: Integrating Cloud Functions with Google Cloud Services. International Research Journal of Education and Technology, 6(10): 369-375.
27. Yadulla, A. R. (2023). Leveraging Secure Multi-Party Computation and Blockchain for Collaborative AI in IoT Networks on Cloud Platforms. Journal of Recent Trends in Computer Science and Engineering (JRTCSE), 11(2), 54–59.
28. Meesala, M. K., Vallabhaneni, R., Mathapati, M., Pareek, P. K., & Metan, J. (2024, September). Arithmetic Optimized Bi-GRU: A Swift Approach to Combat Fake News in the Digital Sphere. In 2024 International Conference on Distributed Systems, Computer Networks and Cybersecurity (ICDSCNC) (pp. 1-6). IEEE.
29. Sajja, G. S., & Meesala, M. K. (2024). Integrating AI in Sustainable Supply Chain Practices: Comparative Analysis Between the USA and Europe. International Journal of Computer Applications, 186(58), 55–62. https://doi.org/10.5120/ijca2024924342