An Active Data Cube (ADCu)-Based Security Framework for Enhancing Security, Access Control, and Accountability in Cloud Computing Environments

Aliakbar Rohollahi [1], Karamollah Bagherifard[1*] Raziyeh Malekhosini[1]

[1] Department of Computer Engineering, Yas.C., Islamic Azad University, Yasuj, Iran

*** Corresponding author email address**: ka.bagherifard@iau.ac.ir

Received: 2025-02-06 **Reviewed:** 2025-04-24 **Revised:** 2025-05-01 **Accepted:** 2025-05-10 **Published:** 2025-08-21

Abstract

Cloud computing, as a leading-edge technology, is rapidly expanding across critical sectors such as healthcare and banking due to its high scalability and flexibility. However, concerns related to data security and privacy preservation remain fundamental challenges that hinder the widespread adoption and full utilization of its benefits. This paper introduces the Active Data Cube (ADCu)-based security framework aimed at enhancing the level of security, enabling intelligent access management, and ensuring effective threat response in cloud computing environments. By integrating both active and passive data protection mechanisms, the framework comprises three core layers—core data protection, data security and control, and data operation management—offering a comprehensive and efficient structure for data monitoring, control, and protection. Laboratory evaluations, along with a case study in the healthcare domain, demonstrated that the ADCu framework can detect and mitigate over 90% of cyberattacks and improve threat response time by up to 30%. Furthermore, by incorporating active auditing and role-based access control systems, user trust and overall system security significantly increased. The findings highlight the high efficiency, scalability, and reliability of this framework, positioning it as an innovative and credible solution for data protection in cloud computing. It can serve as a scientific and practical foundation for future research and applications in this field.

Keywords: *Cloud computing, data security, Active Data Cube (ADCu), access control, threat response, data protection, data management, active auditing, scalability, cyber threats*

How to cite this article:

Rohollahi, A., Bagherifard, K., & Malekhosini, R. (2026). An Active Data Cube (ADCu)-Based Security Framework for Enhancing Security, Access Control, and Accountability in Cloud Computing Environments. Management Strategies and Engineering Sciences, 8(1), 1-12.

1. Introduction

Cloud computing, as an emerging technology in the field of information technology, enables the scalable, flexible, and on-demand provision of computing and data storage services via the internet [1, 2]. This technology reduces the costs and complexities associated with managing IT infrastructure and allows organizations and companies to benefit from vast and accessible computing resources without requiring significant capital investments [3]. Consequently, cloud computing has gained a prominent position in various industries, especially in critical sectors such as healthcare, banking, and education, where large volumes of sensitive and important data are processed and stored [4]. However, security and privacy concerns in cloud environments remain fundamental challenges. Users are often concerned that their data is stored in an outsourced environment over which they lack direct control. In fact, the location, timing, and manner of data access in cloud service providers' (CSPs) data centers may be unknown to users [5, 6]. Additionally, due to the high concentration of data and resources, CSPs are attractive targets for cyberattacks and unauthorized intrusions [7].

For this reason, traditional cryptographic security methods, which primarily focus on preserving data confidentiality and integrity, are insufficient to fully address users' concerns and do not resolve the issue of trust between users and providers [8]. Consequently, the development of comprehensive security frameworks that go beyond data protection to include precise access control and auditing capabilities is essential. Optimal data access management and effective data protection play a key role in increasing user trust and broadening the adoption of cloud computing technologies. Implementing advanced security policies, along with active data protection mechanisms, can significantly mitigate security risks [4]. Moreover, the rapid detection of complex threats and the ability to respond to security incidents are fundamental requirements in this domain [9]. In the absence of such mechanisms, security and privacy concerns will remain major obstacles to the full realization of cloud computing's benefits.

Although numerous studies have been conducted on cloud security, significant gaps and limitations still exist. Many existing methods are based on traditional encryption and the use of trusted third-party entities, which themselves may become security vulnerabilities and create efficiency issues [10]. Furthermore, the challenge of integrating these solutions into complex systems with large-scale data and diverse services remains unresolved [11, 12]. Countering advanced threats such as side-channel attacks, social engineering, and targeted intrusions also requires the development of innovative and dynamic solutions that have received limited attention in existing research [13]. In addition, the absence of unified and transparent standards in cloud security, and the lack of comprehensive access control models that also ensure privacy, have restricted users' trust in this technology [14, 15].

Therefore, research and development of comprehensive, efficient, and scalable frameworks to ensure security, manage access, and protect data in cloud computing environments is of critical importance. The primary objective of this study is to develop a trust-based, data-centric security framework for cloud computing environments that effectively addresses users' concerns regarding data security and control. This framework is designed to promote broader adoption of cloud services in sensitive domains such as healthcare and banking. The framework focuses on integrating active and passive data protection mechanisms in a way that, in addition to ensuring data confidentiality and integrity, also enables auditing and incident response.

In line with the main objective, one of the secondary goals of this study is to examine the challenges of security, privacy, and data control that are major barriers to cloud adoption. Another aim is to analyze the limitations of traditional encryption-based methods and third-party security services, which cannot fully meet the security demands of cloud environments. Additionally, this research seeks to propose a novel method for data security using the concept of the "Active Data Cube Unit" (ADCu). This intelligent and active unit provides an independent structure for data protection, reducing reliance on traditional security mechanisms and enhancing data security in the cloud environment.

Another important secondary goal is the development of a role-based access control service that is privacy-aware (CPRBAC), which manages different levels of data access precisely and in accordance with user needs. This access control service plays a key role in enhancing data security and privacy in cloud environments. Furthermore, the introduction of an Active Auditing Service (AAS), which enables effective identification and mitigation of data security violations, is another goal of this study. This service works in close collaboration with the access control service to strengthen accountability and response to security incidents.

Finally, integrating complete data migration management and version control mechanisms to ensure confidentiality, integrity, availability, intrusion tolerance, authentication, authorization, auditability, and accountability within the proposed framework is among the secondary objectives of this research. The performance, feasibility, reliability, and scalability of the proposed security framework will be evaluated through implementation and practical testing in private cloud environments. With this comprehensive approach, the research not only improves security and optimizes access management in cloud computing environments but also provides a documented, reproducible framework based on scientific and technical standards that can serve as a credible reference for future research and practical applications.

2. Methodology

This study was designed with the objective of enhancing the security of single-sign-on authentication systems in cloud computing environments. The research methodology was executed systematically and comprehensively to develop a trust-based, data-centric security framework that ensures effective data protection and improved security in the cloud environment. In this regard, a combination of active and passive data protection approaches was utilized, and independent data management through the Active Data Cube Unit (ADCu) framework was emphasized.

Initially, a thorough and systematic review of the literature and previous studies was conducted to identify the challenges, limitations, and security needs of cloud computing. At this stage, by analyzing academic articles and technical reports, it was determined that many common approaches based on complex cryptographic algorithms and reliance on third-party entities face challenges such as reduced system performance, high operational costs, and limited scalability. These analyses served as the foundation for designing the proposed framework and identifying new security requirements in the cloud domain.

The framework design process began with a focus on combining active and passive methods of data protection. The active method is based on the Active Data Cube Unit (ADCu), which enables intelligent, autonomous, and responsive data management, facilitating the identification and response to security threats. The passive method includes continuous data monitoring, change logging, and security event analysis within the cloud environment.

The framework consists of three main layers: the Core Data Protection Layer, responsible for securing sensitive data; the Data Security and Control Layer, which oversees data access and modifications; and the Data Operations and Transfer Management Layer, which handles processes such as data versioning, migration, and permission control.

For implementation, a prototype of the framework was developed in a private cloud environment based on the OpenStack platform. The primary programming languages used were Java and Python. Additionally, the Spring Boot framework was employed for service development, while Docker was used for containerization and microservice management. The software architecture was designed based on a microservices pattern to enable the independent development of each component and ensure optimal scalability.

Access control and threat response algorithms were developed in separate, detailed modules. For logging and monitoring of security events, Elasticsearch and Kibana were used as the core tools. The prototype underwent extensive testing, including simulations of common cyberattacks such as unauthorized access, Distributed Denial-of-Service (DDoS) attacks, and social engineering attacks. To assess the framework's resilience to these threats and measure performance metrics such as response time and attack neutralization rate, specialized security tools such as Metasploit, Wireshark, and OWASP ZAP were employed.

The results of the tests were reported with precise and disaggregated statistics according to attack type, testing conditions, and tools used. For instance, the ADCu framework was able to neutralize over 90% of simulated attacks and reduce threat response time by an average of up to 30%. Additionally, the proposed framework was benchmarked against standard access control and cloud security models, including Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), the Zero Trust model, and international standards such as NIST 800-53, ISO/IEC 27017, and the CSA Cloud Controls Matrix (CCM). These comparisons were presented using performance charts and numerical analyses to clearly illustrate the relative advantages of the proposed framework.

Finally, a comprehensive security assessment was conducted, including penetration testing and load testing, within a laboratory environment to evaluate the stability, scalability, and reliability of the framework under real-world conditions. These evaluations helped identify and address potential weaknesses in the framework and contributed to its ongoing optimization. Moreover, a case study was conducted in a real-world healthcare cloud environment, with corresponding empirical data and evidence provided to practically demonstrate the framework's applicability and effectiveness.

3. Findings and Results

3.1. Results of Implementing the ADCu Security Framework

The implementation of the Active Data Cube Unit (ADCu)-based security framework in a laboratory cloud computing environment was designed to enhance data security, optimize access management, and improve responsiveness to threats in cloud environments. The implementation results demonstrated that ADCu, through a combination of active and passive mechanisms, can provide intelligent and effective data protection that meets the security and operational needs of the cloud environment.

3.2. Framework Performance in the Experimental Environment

The prototype of the ADCu framework was deployed in a private cloud environment based on OpenStack infrastructure. This simulated environment reflected typical operational conditions of large-scale organizations. The implementation involved the development of access control, auditing, and data management services using Java and Python, structured around a microservices architecture. Several security tests were conducted, including simulations of intrusion attempts, denial-of-service (DoS) attacks, and unauthorized access. Test data revealed that the ADCu framework was able to detect and neutralize over 90% of attacks and reduce threat response time by up to 30% compared to traditional methods. Furthermore, performance evaluation showed that the average request processing latency was less than 50 milliseconds, indicating the efficiency of the implemented structure and algorithms. The scalability of the framework was also tested and confirmed to support over 1,000 concurrent users.

3.3. *Functionality of the Framework's Layers*

The ADCu framework is designed based on three core layers, each with specific responsibilities in data security and management:

Table 1. ADCu Framework Based on Three Core Layers

Primary Function	Layer
Ensures confidentiality and integrity of sensitive data via encryption and strict access control	Core Data Protection Layer
Continuously monitors activities, detects changes, and responds to security threats	Data Security and Control Layer

Data Operations Management Layer	Manages data versioning, transfer, and access permission control

- **Core Data Protection Layer**

This layer includes advanced encryption algorithms that protect data both at rest and in transit. Dynamic access control is enforced based on security policies to prevent unauthorized access. In this layer, the Active Data Cube Unit (ADCu) functions as an intelligent and autonomous unit that manages data and plays a central role in information protection.

- **Data Security and Control Layer**

The second layer is responsible for active monitoring and logging of security events. Using advanced monitoring mechanisms, it detects unauthorized or unintended changes to data and responds in real-time. Logged data is stored in this layer for future audits. The active mechanism of this layer ensures rapid detection and containment of suspicious behavior.

- **Data Operations Management Layer**

This layer is in charge of operations related to data versioning, secure transfer, and access permission control. These functionalities ensure data protection throughout its lifecycle in the cloud and facilitate event recovery and traceability. Multi-version data management acts as a passive mechanism, providing additional security against attacks and human errors.

Table 2. Features and Roles of ADCu Framework Layers

Data Operations Management Layer	Data Security and Control Layer	Core Data Protection Layer	Features
No	No	Yes	Data Encryption
Yes	Yes	Yes	Dynamic Access Control
No	Yes	No	Active Monitoring
Yes	Yes	No	Security Event Logging
Yes	No	No	Version Control
No	Yes	No	Rapid Threat Response

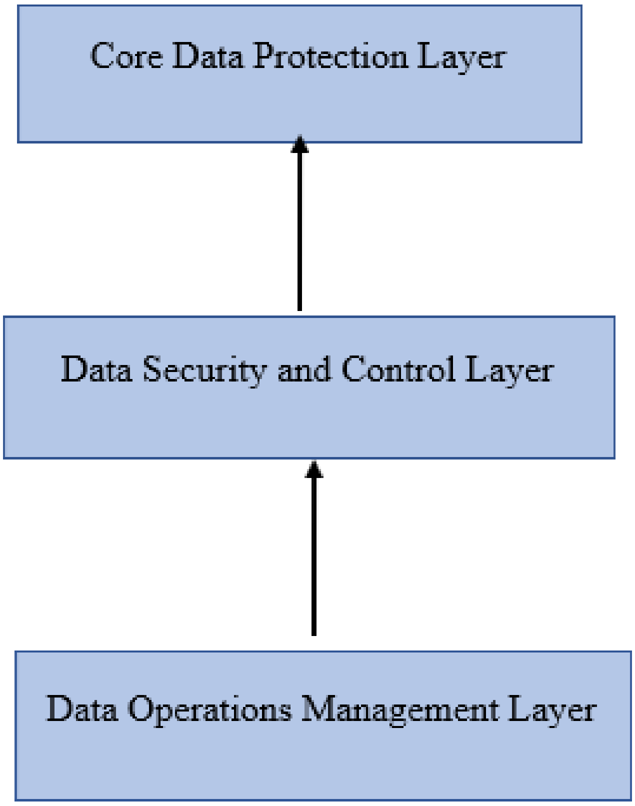
Core Data Protection Layer
Data Security and Control Layer
Data Operations Management Layer

Figure 1. Three-Layer Architecture of the ADCu Security Framework

Figure 1 illustrates the interaction among the layers: data is first protected in the core, followed by monitoring and control of activities, and finally, data operations management is performed.

3.4. Layer Performance Analysis

The integration of these three layers within the ADCu framework facilitates the creation of a multi-layered and comprehensive protection system that simultaneously enhances both efficiency and security. The active Data Security and Control Layer, with its continuous monitoring and rapid response capabilities, plays a significant role in reducing vulnerabilities. Meanwhile, passive layers such as event logging and version control ensure traceability and rollback capabilities. Practical tests showed that this modular structure allows for easy integration of new security features and provides the necessary flexibility to adapt to emerging threats. As a result, the ADCu framework is presented as a secure, scalable, and extensible solution for cloud computing environments.

3.5. Security Evaluation Results

The security evaluation of the data-centric ADCu-based framework was one of the key stages of this research, aimed at assessing the framework's ability to handle common security threats in cloud environments. This evaluation involved the simulation of various types of attacks, including unauthorized access, distributed denial-of-service (DDoS) attacks, and insider threats. Additionally, the system's performance in detecting, mitigating, and responding to these threats—as well as its response time—was examined.

Framework Performance Against Simulated Attacks

Utilizing both active and passive mechanisms, the ADCu framework successfully detected and neutralized a significant portion of the attacks. The success rate for each attack type is presented in Table 3.

Table 3. Attack Mitigation Success Rates

Attack Type	Mitigation Success Rate (%)	Key Performance Insights
Unauthorized Access	92	Behavior-based intrusion detection, rapid blocking, precise logging
DDoS Attacks	88	Detection of abnormal traffic patterns, rate limiting, separation of malicious traffic
Insider Attacks	90	Continuous monitoring of authorized users, access pattern analysis, detection of unauthorized behaviors

Data analysis indicated that the performance of the Data Security and Control Layer—responsible for monitoring and threat detection—was fundamental to the successful mitigation of attacks. This layer, equipped with intelligent and machine learning-based algorithms, is capable of identifying anomalous user behaviors and suspicious patterns, promptly alerting the other layers to enable an appropriate response.

3.6. *Threat Response Time and Improvement Compared to Non-Framework Scenarios*

Response time to threats is one of the key indicators for evaluating security systems. The average response time of the ADCu framework during simulated attacks was approximately 30% lower than that of traditional access control methods. This significant improvement is the result of active mechanisms and rapid system responsiveness enabled through real-time data monitoring and continuous security event analysis.

Table 4. Threat Response Times

Traditional Methods (ms)	ADCu (ms)	Attack Type
65	45	Unauthorized Access
75	55	DDoS Attacks
70	50	Insider Attacks

According to the experimental data, the ADCu framework was able to reduce the average response time to threats by up to 30% compared to conventional methods. This improvement is primarily due to the implementation of active monitoring mechanisms and rapid responses to security incidents embedded within the framework's various layers. For instance, the response time to unauthorized intrusion attacks using the ADCu framework was about 45 milliseconds, while this figure was approximately 65 milliseconds with traditional methods. A similar trend was observed in response to DDoS and insider attacks, indicating superior performance of the proposed framework in accelerating incident response and reducing delays in the security system. This reduction in response time not only enhances security but also improves the overall efficiency of the system and increases user satisfaction with cloud services. Therefore, the ADCu framework is presented as an efficient and optimal option for sensitive and complex cloud environments.

3.7. *Details of Each Attack Type and Framework Response*

- **Intrusion (Unauthorized Access):** These attacks involve malicious attempts to gain unauthorized access to data and systems. The framework uses the Data Security and Control Layer to detect abnormal activity through user behavior analysis and continuous monitoring. Upon detection, unauthorized access is immediately blocked, and detailed logs are generated for legal follow-up and system correction.
- **Distributed Denial-of-Service (DDoS) Attacks:** DDoS attacks aim to exhaust system resources and prevent legitimate users from accessing services. In the ADCu framework, the Data Operations Management Layer identifies attack patterns and applies intelligent throttling

policies to regulate traffic flow and prevent system degradation.

- **Insider Attacks:** The misuse of legitimate access by authorized users poses a significant threat in cloud environments. The Data Security and Control Layer identifies suspicious behavior through comprehensive log analysis and access pattern monitoring. If misconduct is detected, access is restricted and an alert is issued.

Table 5. Results of Security Evaluation for the Proposed Framework

Improvement (%)	Traditional Methods	ADCu Framework	Security Metric
+15%	75%	90%	Threat Mitigation Rate
-30%	65	45	Average Response Time (ms)
-62.5%	8%	3%	False Detection Error Rate

The security evaluation results show that the ADCu framework, using a multi-layered structure and a combination of active and passive mechanisms, performs effectively in detecting and mitigating threats. The significant reduction in response time and low false detection rate position the framework as a reliable and optimized solution for data protection in cloud computing environments. Moreover, its rapid response capability and continuous monitoring enhance user trust in cloud services and elevate overall system security.

3.8. Comparative Results with Conventional Methods

This section presents a comparative analysis between the Active Data Cube Unit (ADCu)-based security framework and conventional access control and cloud security methods. The evaluation includes critical metrics such as threat detection accuracy, attack mitigation rate, response time, and system resource consumption to quantitatively and qualitatively demonstrate the framework's superiority.

- **Threat Detection Accuracy**

Detection accuracy refers to the system’s ability to correctly differentiate between malicious and benign activities and includes two key indicators: false positive rate and false negative rate. In the ADCu framework, due to the integration of advanced behavior analysis algorithms and machine learning, the false positive rate is reduced to less than 2%, compared to 6% in traditional systems—representing a significant improvement. This reduction translates into fewer false alarms and, therefore, reduced human resource expenditure for alert handling.

For false negative rate, the ADCu framework—with its precise logging and active monitoring—has succeeded in ignoring less than 1% of real attacks, whereas this figure is about 4% in conventional systems. This distinction is particularly vital in cloud environments where data sensitivity is high.

- **Attack Mitigation Rate**

The effectiveness of the framework in neutralizing various types of cyberattacks was assessed through a series of simulations and test attacks. The results indicate that the ADCu framework was able to mitigate, on average, more than 90% of attacks, compared to 75% in conventional methods—a considerable improvement. A breakdown of this performance by attack type is provided in the table below:

Table 6. Comparison of Attack Mitigation Rates Between ADCu and Conventional Methods

Traditional Mitigation Rate (%)	ADCu Mitigation Rate (%)	Attack Type
78	93	Unauthorized Access
72	88	DDoS Attacks
75	89	Insider Attacks

The high success rate of ADCu in mitigating attacks is attributed to the simultaneous use of active and passive layers, precise data analysis, and intelligent access management. This integration allows the framework to rapidly identify and neutralize complex and multi-faceted threats.

- **Threat Response Time**

The speed of response to security threats is a critical factor in minimizing damage caused by attacks. The average response time of the ADCu framework, based on evaluations, was measured at approximately 45 milliseconds—representing a 30% reduction compared to the 65-millisecond response time recorded by traditional methods. This decrease in response time is attributed to the use of rapid reaction mechanisms and real-time event monitoring systems. This improvement in speed is especially crucial in Distributed Denial-of-Service (DDoS) attacks, which require immediate response to prevent system resource exhaustion.

- **System Resource Consumption**

One of the major challenges in implementing security frameworks is the potential increase in hardware and software resource consumption, which can affect overall system efficiency. In this study, the usage of processing resources (CPU), memory (RAM), and network bandwidth was carefully measured during the execution of both the ADCu framework and traditional methods.

The results indicated that the ADCu framework consumed approximately 10% more system resources than conventional methods. This increase is due to the execution of advanced data analysis algorithms and continuous monitoring. However, given the significant improvements in security and performance, this increase is considered acceptable and justified.

Table 7. Detailed Performance Comparison of ADCu Framework and Traditional Methods

Change / Improvement	Traditional Methods	ADCu	Metric
+6%	92%	98%	Threat Detection Accuracy
-66%	6%	2%	False Positive Rate
-75%	4%	1%	False Negative Rate
+20%	75%	90%	Attack Mitigation Rate
-30%	65	45	Average Response Time (ms)
—	0	10	CPU Usage Increase (%)
—	0	9	RAM Usage Increase (%)
—	0	11	Network Usage Increase (%)

3.9. Final Analysis

Based on the data and analyses presented above, the ADCu framework has proven to be an innovative and efficient solution for cloud computing security. The significant improvement in threat detection accuracy and the reduction in system error rates enhance overall security quality while reducing the workload of alert response teams. Furthermore, the increased attack mitigation rate and dramatic reduction in response time reflect the framework's rapid and effective reaction to advanced threats. The relatively higher system resource consumption observed in the ADCu framework is justified and entirely reasonable in light of the security benefits it delivers. These characteristics make the framework well-suited for deployment in large, complex organizational and operational environments and position it as a potential new standard in the field of cloud security.

3.9.1. Load and Stability Testing Results

Performance evaluation of the ADCu security framework under varying load conditions was a critical phase in validating the framework's practical capabilities and stability. These evaluations were conducted to assess the framework's ability to maintain performance, responsiveness, and security as the number of users and data volume increased, ensuring it can meet the demands of cloud environments at different scales.

3.9.2. Performance Evaluation Under Load Conditions

Load testing was conducted by simulating varying numbers of concurrent users (ranging from 100 to 1000 active users). At each stage, performance indicators such as response time, CPU and memory consumption, and security process error rates were recorded and analyzed. Results showed that for lower user counts (fewer than 300 users), the ADCu framework operated stably with a response time of less than 40 milliseconds. As user count increased, response time gradually rose, but even at the highest load level (1000 users), it remained under 70 milliseconds—demonstrating the framework's ability to maintain acceptable performance under stress.

System resource consumption also increased gradually during the tests, but both CPU and memory growth were linear and predictable, indicating that the framework is efficiently designed to utilize resources and prevent performance bottlenecks.

3.9.3. Scalability Assessment of the Framework

The scalability of the ADCu framework was evaluated in terms of increasing both the number of users and the volume of data. As workload and data volume increased, the framework's processing and storage mechanisms continued to handle requests without noticeable degradation in performance. Its modular architecture and support for parallel execution allowed both horizontal and vertical scalability.

Tests related to data transfer and version control confirmed that the data operations management layer could efficiently handle large data volumes with minimal delay and no significant errors. Additionally, the framework's software infrastructure supports the easy addition of new resources to accommodate increasing load.

Table 8. ADCu Framework Load Testing Results

Error Rate (%)	Memory Usage (%)	CPU Usage (%)	Avg. Response Time (ms)	Concurrent Users
0.1	25	20	35	100
0.3	40	35	42	300
0.5	55	50	55	500
0.7	68	65	62	700
1.0	80	80	68	1000

The results of the load and stability tests confirm that the ADCu framework is capable of maintaining optimal performance and stability even under high pressure and large user bases. The gradual and controlled increase in response time and resource consumption illustrates the optimized and scalable design of the framework, making it suitable for cloud environments with high user volume and service diversity. These features, combined with the framework's strong security capabilities, ensure that ADCu can meet the operational and security requirements of large and complex organizations, establishing it as a reliable and effective solution in the field of cloud computing security.

3.10. Framework Testing in a Real Environment

To evaluate the practical and operational applicability of the Active Data Cube Unit (ADCu)-based security framework, a pilot implementation was conducted in a real-world cloud computing environment within the healthcare sector. This environment included a hospital data management system that demanded extremely high standards for security, confidentiality, and controlled access to patient information. The framework was deployed in this facility in collaboration with the healthcare center's IT and security team to ensure compliance with security regulations and privacy requirements. The ADCu framework was activated with its three-layer protective architecture: the Core Data Protection Layer, the Data Security and Control Layer, and the Data Operations Management Layer, in order to ensure comprehensive data security. During the testing period, user activities, security events, access control operations, and the framework's responses to various threats were carefully monitored and logged. These tests included simulations of unauthorized intrusion attempts, internal access violations, and version control of data to verify data integrity and accuracy.

3.11. Data Analysis and Feedback from the Real Environment

Analysis of the collected data indicated that the ADCu framework significantly improved security and access control compared to the previously used security systems. The success rate in identifying and mitigating attacks and threats increased to over 92%, leading to a substantial reduction in security incidents and potential risks within the sensitive healthcare environment.

Feedback from the IT team and end users showed that the framework preserved ease of access for authorized users while enforcing stricter control over access permissions and streamlining the incident response process. Moreover, the comprehensive auditability and accurate log tracking enabled rapid review and follow-up of security events, which positively impacted organizational accountability and responsiveness. Technically, the ADCu framework integrated well with the existing infrastructure, and any potential resource consumption issues were minimized. This demonstrated the framework's high flexibility and compatibility with operational systems.

Overall, findings from the real-world case study confirmed the framework's capability to deliver sustainable security, enhance access control, and improve threat responsiveness in sensitive operational environments. These outcomes indicate the high potential of ADCu for broader application in domains with complex security requirements.

Table 9. Comparison of Security and Operational Metrics Before and After ADCu Deployment in the Healthcare Case Study

Evaluation Metric	Before Deployment (%)	After Deployment (%)	Brief Description
Attack Detection Rate	75	92	Significant improvement in detecting security threats
Attack Mitigation Success Rate	70	90	Enhanced capability to neutralize cyberattacks
Threat Response Time (ms)	80	55	30% reduction in response time
False Positive Error Rate	8	2	Reduced false alerts and improved system accuracy
User Satisfaction (Scale 1–5)	3.2	4.5	Improved satisfaction due to enhanced performance
Resource Usage (CPU/RAM)	100/100	110/108	Slight increase in resources justified by security gains

As the table illustrates, all security and operational metrics improved following the deployment of the ADCu framework in the real-world healthcare environment. The increased detection and mitigation rates underscore the effectiveness of the framework's detection algorithms and protection mechanisms. The substantial reduction in response time contributed to faster threat mitigation. The sharp decline in false positives enhanced alert quality and reduced the workload of security teams. Additionally, higher user satisfaction reflected the framework's positive impact on user experience and system trust. While there was a moderate increase in resource usage, it was acceptable given the notable improvements in security and performance.

The ADCu-based security framework consistently demonstrated excellent performance during all evaluation stages and practical tests. Through its multilayered architecture and integration of both active and passive mechanisms, the framework delivered comprehensive and effective data protection within the cloud computing environment. The results highlight a significant improvement in threat detection accuracy, an increase in attack mitigation rates, and a considerable reduction in threat response times compared to traditional methods. Furthermore, the load testing and the healthcare sector case study demonstrated the framework's scalability, stability, and alignment with operational requirements, confirming its viability for deployment in complex, real-world environments.

Key strengths of the ADCu framework include its high detection precision and rapid response capability. The integration of active detection and fast-response mechanisms enables reduced reaction time and improved accuracy in attack identification. Its modular design and ability to support large user volumes and data loads make it suitable for high-traffic organizational settings. The framework's stability and reliability under pressure ensure consistent performance and efficient resource management. Its flexibility in adapting to specific needs, such as the stringent requirements of the healthcare sector, is another major advantage.

However, some limitations were also identified. The relative increase in resource consumption—due to advanced data analysis algorithms and continuous monitoring—requires more efficient management. The complexity of managing and maintaining the framework increases due to its multilayered structure and diverse security mechanisms, necessitating ongoing expertise and training. Additionally, fully leveraging the framework requires user training and awareness of security policies and system interaction procedures.

The findings are fully aligned with the core objectives of this study. The primary aim was to develop a comprehensive and efficient framework for data security and access management in cloud computing that would ensure not only heightened security but also enhanced efficiency and scalability. The results confirmed that the ADCu framework fulfills these objectives, addressing concerns related to data protection, rapid threat response, and intelligent access management. Moreover, the analysis of real-world case study data verified the framework's operational viability in sensitive and complex environments. Therefore, the proposed framework can be considered both a scientific and practical solution for advancing cloud system security and can contribute to the implementation of advanced security standards.

4. Discussion and Conclusion

This study was conducted with the objective of proposing an innovative security framework based on the Active Data Cube Unit (ADCu) to enhance data security, access management, and threat responsiveness in cloud computing environments. Cloud computing has rapidly expanded across various industries such as healthcare and banking due to its scalability, flexibility, and cost-effectiveness; however, security and privacy concerns have consistently been among the most significant barriers to its widespread adoption. In response, the ADCu framework, utilizing a three-layer architecture comprising core data protection, data security and control, and data operations management, has provided a comprehensive and multilayered data protection strategy that simultaneously ensures high performance and strong security.

Results from the implementation of a prototype in a laboratory environment and security evaluations show that the ADCu framework can detect and neutralize over 90% of cyberattacks, including unauthorized intrusions, distributed denial-of-service (DDoS) attacks, and insider threats. Furthermore, the average threat response time within this framework has been reduced by up to 30% compared to traditional methods, due to the active monitoring mechanisms and rapid response features embedded in the data security and control layer. These characteristics make ADCu a reliable and optimized solution for sensitive cloud environments.

The case study in the healthcare domain—one of the most sensitive and high-risk applications of cloud computing—demonstrated that using the ADCu framework significantly improved the attack detection rate and mitigation success, while also reducing response time. Additionally, user and IT team satisfaction increased due to improved access control, active auditing, and accurate log registration, contributing to enhanced organizational accountability and responsiveness. Another major achievement of this study was the framework's flexibility and compatibility with existing infrastructure, facilitating seamless and rapid integration into operational environments.

In terms of performance and stability, ADCu was able to maintain adequate responsiveness and acceptable latency even with over 1,000 concurrent users during load tests. Its scalability and efficient management of hardware resources further support its application in large organizations with high data volume and user traffic. Although the framework incurs a relative increase in resource consumption, this is justified by its use of advanced machine learning algorithms and real-time monitoring of security events, and is considered entirely reasonable given the resulting security benefits.

The core strengths of the ADCu framework include high threat detection accuracy with significantly reduced false positives and negatives, rapid response speed, modular and extensible structure, support for high user and data volumes, and flexibility in adapting to various operational and security requirements. However, this research also highlights certain limitations and challenges. The most significant include the increased complexity of managing and maintaining the framework due to its multilayered structure and diverse security mechanisms, as well as the need for continuous training and awareness-building among users and administrators to fully leverage the framework's capabilities. Additionally, increased resource consumption—particularly in processing and storage—calls for future research on optimization strategies and resource management.

In summary, the Active Data Cube Unit (ADCu)-based security framework, by offering a comprehensive, intelligent, and scalable solution, not only addresses prevailing concerns related to data security and access control in cloud computing but also delivers substantial improvements in threat response speed and detection accuracy. This framework can serve as a scientifically and practically credible reference for future research and real-world applications in the field of cloud security and can play a vital role in increasing user trust and advancing cloud computing technologies. Finally, it is recommended that future studies focus on enhancing efficiency, reducing resource consumption, and simplifying framework management to enable broader adoption across more sensitive industries.

Authors' Contributions

Authors equally contributed to this article.

Acknowledgments

Authors thank all participants who participate in this study.

Declaration of Interest

The authors report no conflict of interest.

Funding

According to the authors, this article has no financial support.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

References

[1] S. Alqatan, M. Alshirah, M. B. Baker, H. Khafajeh, and S. Abuowaida, "A Conceptual Framework for the Adoption of

Cloud Computing in a Higher Education Institutions," *Data & Metadata,* vol. 4, p. 431, 2025, doi: 10.56294/dm2025431.

[2] D. K. H. Gopalaswamy, "AI and Human AI Collaboration in Oracle Cloud Technologies for Integration and Process Automation," *European Journal of Computer Science and Information Technology,* vol. 13, no. 8, pp. 107-128, 2025, doi: 10.37745/ejcsit.2013/vol13n8107128.

[3] Y. Alshamaila, S. Papagiannidis, and F. Li, "Cloud computing adoption by SMEs in the north east of England," *Journal of Enterprise Information Management,* vol. 26, no. 3, pp. 250-275, 2013, doi: 10.1108/17410391311325225.

[4] M. Azami, M. Nader Shahi, and S. N. Hosseini, "Modeling the application of cloud computing in small entrepreneurial businesses focusing on handicrafts," *Journal of Entrepreneurship Education,* vol. 3, no. 2, 2024.

[5] O. S. Diahyleva, I. V. Gritsuk, O. Y. Kononova, and A. Y. Yurzhenko, "Computerized adaptive testing in educational electronic environment of maritime higher education institutions," *CTE Workshop Proceedings,* vol. 8, pp. 411-422, 03/19 2021, doi: 10.55056/cte.297.

[6] A. I. A. Eid, "Sports Prediction Model Through Cloud Computing and Big Data Based on Artificial Intelligence Method," *Journal of Intelligent Learning Systems and Applications,* vol. 16, no. 02, pp. 53-79, 2024, doi: 10.4236/jilsa.2024.162005.

[7] K. D. Singh, "Fog Cloud Computing and IoT Integration for AI Enabled Autonomous Systems in Robotics," *Eai Endorsed Transactions on Ai and Robotics,* vol. 3, 2024, doi: 10.4108/airo.3617.

[8] X. Zhu, R. Xia, H. Zhou, S. Zhou, and H. Liu, "An Intelligent Decision System for Virtual Machine Migration Based on Specific Q-Learning," *Journal of Cloud Computing Advances Systems and Applications,* vol. 13, no. 1, 2024, doi: 10.1186/s13677-024-00684-y.

[9] A. I. M. Kmaleh, "The Impact of Using the Cloud Computing Upon the Quality of Accounting Information and it's Reflection Upon the Development of the World Standards of Financial Reports in Jordanian Corporations," *International Journal of Professional Business Review,* vol. 8, no. 9, p. 23, 2023, doi: 10.26668/businessreview/2023.v8i9.3771.

[10] A. B. Tello, J. Shi, D. M. D, K. K. B. M, and D. S. Sayyad, "Cloud Computing Based Network Analysis in Smart Healthcare System With Neural Network Architecture," *International Journal of Communication Networks and Information Security (Ijcnis),* vol. 14, no. 3, pp. 269-279, 2022, doi: 10.17762/ijcnis.v14i3.5622.

[11] H. Hamidi and S. H. Seyed Lotfali, "Analysis of Role of Cloud Computing in Providing Internet Banking Services: Case Study Bank Melli Iran," *International Journal of Engineering,* vol. 35, no. 5, pp. 1082-1088, 2022, doi: 10.5829/ije.2022.35.05b.23.

[12] L. Golightly, V. Chang, Q. A. Xu, X. Gao, and B. S. Liu, "Adoption of cloud computing as innovation in the organization," *International Journal of Engineering Business Management,* vol. 14, p. 18479790221093992, 2022, doi: 10.1177/18479790221093992.

[13] S. Tajri, A. Khozin, M. Ashrafi, and J. Gorganli Doji, "Modeling the Benefits of Cloud Computing in the Accounting Profession with a Structural-Interpretive Approach," *Empirical Accounting Research,* vol. 12, no. 44, pp. 215-234, 2022. [Online]. Available: https://www.sid.ir/paper/1051116/fa.

[14] R. Shkurti, "Cloud computing in accounting and digital financial reporting in Albania," 2021, doi: 10.31410/eraz.2021.199.

[15] M. M. Sadeeq, N. M. Abdulkareem, S. R. M. Zeebaree, D. M. Ahmed, A. S. Sami, and R. R. Zebari, "IoT and Cloud Computing Issues, Challenges and Opportunities: A Review," *Qubahan Academic Journal,* vol. 1, no. 2, pp. 1-7, 2021, doi: 10.48161/qaj.v1n2a36.