Big Data Analytics and Data Science E-ISSN: 3123-9986

Research Article

Adaptive Cyber Secure Software Engineering Practices for Big Data Platforms With Dynamic Access Control and Differential Privacy Mechanisms

Ahmad Budi Trisnawan [1*], Priyo Wibowo [2]

[1] Universitas Mahakarya Asia, Indonesia; e-mail : abudit75@gmail.com
[2] Politeknik Katolik Mangunwijaya, Indonesia; e-mail : pyoulia17@gmail.com
* Corresponding Author : Ahmad Budi Trisnawan

Abstract: Big data platforms face significant challenges related to cybersecurity and privacy due to the vast volume, variety, and velocity of data they manage. Traditional static security measures often fail to address the dynamic and complex nature of big data environments. This research proposes an adaptive cybersecurity framework that integrates dynamic access control and differential privacy mechanisms to enhance both the security and privacy of big data platforms. The dynamic access control mechanism continuously adjusts access permissions in real-time based on changing risk and trust levels, ensuring that sensitive data remains secure even as user roles and data flows evolve. The differential privacy mechanism adds noise to data, preserving individual privacy while allowing for meaningful data analysis. Through simulations and case studies, the framework was evaluated in various real-world environments, including healthcare, IoT, and finance, where it demonstrated scalability, efficiency, and robust security performance. The results showed that the proposed framework significantly reduced unauthorized access attempts and maintained data privacy, while still enabling effective data analysis. Although there were some challenges regarding performance overhead, particularly in resource-constrained environments, the framework remained effective in large-scale systems. The findings highlight the importance of adaptive security practices in big data environments and suggest that future research should focus on refining dynamic security mechanisms and applying differential privacy in diverse real-world scenarios. These advancements are essential for ensuring that big data platforms can handle evolving cyber threats without compromising data utility or privacy.

Keywords: Adaptive Security; Big Data; Cybersecurity Frameworks; Differential Privacy; Dynamic Access.

Received: 21, November 2025
Revised: 10, December 2025
Accepted: 29, December 2025
Published: 20, January 2026
Curr. Ver.: 20, January 2026

Copyright: © 2025 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY SA) license (https://creativecommons.org/licenses/by-sa/4.0/)

1. Introduction

Big data platforms are increasingly confronted with significant cybersecurity and privacy risks due to the enormous scale and complexity of the data they handle. With the rapid growth of technologies such as the Internet of Things (IoT), social media, and cloud computing, the volume of data generated has skyrocketed, creating valuable insights but also substantial security and privacy challenges [1]. These platforms must safeguard against threats to data confidentiality, integrity, accessibility, and accountability, ensuring the protection of sensitive information from unauthorized access or breaches [2]. The integration of these technologies has made big data an attractive target for cyberattacks, making robust security measures essential for mitigating risks.

The complexity of managing and securing large-scale data access is another major challenge for big data platforms. Data in these systems is typically sourced from various industries, including banking, healthcare, and social media, each with distinct security requirements [3]. The entire data lifecycle-spanning collection, storage, processing, and sharing-presents vulnerabilities that need to be mitigated to prevent unauthorized access and data breaches [4]. Furthermore, multi-tenant environments, where multiple users share infrastructure to reduce costs, introduce additional complexities in maintaining data isolation and preventing cross-tenant data leaks [5]. As the number of users and the volume of data

grow, ensuring both security and system performance remains a significant hurdle for these platforms.

In addition to these challenges, the evolving nature of cyber threats presents a growing concern. Cyberattacks are becoming more sophisticated, with techniques such as malware, ransomware, and insider threats increasingly targeting big data systems [6]. Among the most concerning are Advanced Persistent Threats (APTs), which involve prolonged and targeted attacks designed to steal sensitive data. These attacks necessitate continuous monitoring and advanced security protocols to detect and mitigate [7]. Moreover, ethical and privacy issues surrounding the use of big data also complicate the situation, as balancing the need for robust security with the protection of individual privacy becomes a delicate challenge [8]. The integration of privacy-preserving techniques such as differential privacy offers a promising approach, yet requires careful consideration of its trade-offs with data utility.

In the age of big data, the need to protect sensitive information has never been more critical. The vast volume, variety, and velocity of data being processed in these environments present unique challenges to traditional cybersecurity measures. Conventional security practices often fall short in addressing the dynamic and complex nature of big data systems, where data access and threats evolve rapidly [9]. Adaptive cybersecurity practices, which offer flexibility and real-time responsiveness, are essential in mitigating sophisticated cyber threats. These practices incorporate mechanisms such as dynamic access control and privacy-preserving technologies like differential privacy, which enhance the security of big data platforms [10], [11]. The integration of machine learning and artificial intelligence further strengthens the ability to detect and respond to emerging threats in real time, providing a proactive approach to data security [12].

Big data systems face unique security challenges due to their dynamic nature. Unlike traditional data environments, big data platforms often feature continuously changing resources and users, which complicates security management. As new threats and vulnerabilities emerge, adaptive security measures are necessary to ensure that systems remain secure. Traditional static security protocols are insufficient for addressing these rapidly changing conditions [13]. Additionally, integrating big data with cloud computing adds another layer of complexity, particularly when it comes to managing data access control and ensuring data confidentiality in a distributed environment [11], [14]. The need for scalable and dynamic security policies is paramount to handle the increased risk exposure in such multi-tenant, cloud-based environments [15].

The core objective of adaptive software engineering practices in big data systems is to enhance data privacy and security through the implementation of dynamic access control and differential privacy mechanisms. Differential privacy techniques anonymize sensitive data, preventing unauthorized access while still allowing for meaningful analysis [16]. Dynamic access control adjusts permissions in real-time based on the context and potential risks associated with data requests, ensuring that only authorized users can access sensitive information [10]. The challenge lies in balancing the utility of big data for analytics with the need to protect individual privacy, which requires privacy-preserving technologies that enable secure data analysis without compromising data privacy [17], [18]. By implementing these adaptive security practices, big data systems can better manage privacy concerns while maintaining the integrity and availability of data.

2. Literature Review

Exploring Security Challenges in Big Data Platforms

Big data platforms are increasingly facing unique security challenges due to the massive volume, complexity, and dynamic nature of the data they manage. These platforms often handle sensitive information, and ensuring the privacy and security of such data is a significant concern. One of the key challenges in big data environments is the protection of data privacy. The collection, storage, and analysis of personal and sensitive data often involve various security risks, including unauthorized access and data breaches [19]. Another critical issue is data provenance, where tracking the origin and history of data to ensure its integrity and authenticity becomes particularly difficult [1]. Additionally, identifying fraudulent activities and conducting network forensics are complicated due to the sheer scale and diversity of the data involved in big data systems [20]. As a result, big data platforms are vulnerable to

sophisticated attacks, such as Advanced Persistent Threats (APT), as well as insider threats from individuals with unregulated access to sensitive data [3].

Current Practices in Access Control Mechanisms for Big Data Systems

Access control mechanisms are fundamental for securing big data systems, but traditional models often fall short in addressing the dynamic and distributed nature of these environments. Role-Based Access Control (RBAC), one of the most commonly used models, assigns permissions based on user roles. However, this model lacks the flexibility required for dynamic systems where access needs change frequently in response to evolving data flows and security risks [21]. In contrast, Attribute-Based Access Control (ABAC) is more adaptable, as it defines access policies based on user attributes and resource characteristics, offering better flexibility and scalability in big data environments [10]. Additionally, blockchain-based access control systems are emerging as a promising solution for providing tamper-resistant, auditable access policies, further enhancing the security of big data platforms [22]. Despite these advancements, static access control models, such as RBAC, face several limitations, including low efficiency, insufficient flexibility to adapt to changing requirements, and poor scalability as the data and user base grow [10].

The Role of Differential Privacy in Protecting Individual Privacy

Differential privacy is a critical concept for ensuring individual privacy in big data environments. This mathematical framework ensures that the inclusion or exclusion of any individual's data does not significantly affect the results of data analysis, thus maintaining privacy while enabling useful insights to be drawn from the data [16], [23]. The core mechanism of differential privacy is the addition of noise to the data, which prevents the identification of individuals even when the data is analyzed at a granular level. However, a key challenge in implementing differential privacy is balancing the trade-off between privacy and data utility. Adding too much noise can reduce the accuracy and usefulness of the data analysis, which is a crucial consideration for many big data applications [19]. Despite these challenges, differential privacy has been successfully applied in various domains, including social networks and cloud computing, where it helps to protect user privacy while still enabling meaningful data analysis [17], [24]. Ongoing research is focused on improving the privacy-utility balance and adapting differential privacy techniques to different big data scenarios to better address the specific privacy challenges of each environment [25], [26].

Analysis of Prior Work on Adaptive Security Frameworks

Adaptive security frameworks have emerged as a crucial solution to address the dynamic and evolving nature of cybersecurity threats, especially in big data systems. Unlike traditional static security measures, adaptive frameworks are designed to continuously monitor and adjust security policies in real-time based on changing conditions. These frameworks have gained significant attention across various sectors, including healthcare, IoT, and financial services, due to the increasing complexity of cyber threats. Prior research highlights key features of adaptive security frameworks, such as dynamic adaptation, proactive threat prevention, and real-time monitoring. For instance, the Adaptive Cybersecurity Framework in healthcare leverages evolutionary game theory to predict and respond to cyber threats targeting healthcare infrastructures [27]. Similarly, the CoralMatrix Security framework for IoT environments uses machine learning algorithms for real-time threat detection and mitigation [28]. These approaches emphasize the need for more flexible and dynamic solutions that can quickly respond to new and unforeseen cybersecurity challenges.

While these frameworks provide significant improvements in terms of adaptability and proactive threat detection, many still face challenges in handling the scalability and efficiency required in large, complex environments. Traditional security models, such as Role-Based Access Control (RBAC), although widely used, struggle to keep up with the dynamic access needs of big data systems [21]. Furthermore, while some frameworks incorporate human-centric and ethical AI principles to ensure transparency and privacy, they often lack the necessary integration of scalable AI techniques and resource-efficient methods, particularly in the IoT context [29]. Therefore, a key takeaway from prior work is the pressing need for adaptive security solutions that are not only flexible but also scalable, resource-efficient, and capable of integrating advanced AI techniques to handle the growing complexity of big data systems.

Security of Big Data Platforms in Cloud and Edge Infrastructure

Big data platforms often operate within distributed cloud and edge computing environments that enable scalable data processing and real-time analytics. While this architecture improves computational efficiency, it also introduces additional security challenges due to the decentralized nature of the infrastructure. Therefore, robust security frameworks are required to ensure the integrity, confidentiality, and availability of data across interconnected systems [30].

The use of hybrid machine learning models in cybersecurity systems has been shown to significantly enhance the detection of abnormal network behavior. By combining multiple neural network architectures, security systems can analyze network traffic more comprehensively and identify complex attack patterns that may otherwise remain undetected in traditional monitoring approaches [31].

In addition to machine learning techniques, blockchain technology has also emerged as a promising solution for improving security in distributed digital infrastructures. Blockchain-based security frameworks provide decentralized verification mechanisms that ensure data integrity and reduce the risk of unauthorized system manipulation, making them particularly relevant for protecting server environments and cloud-based applications [32].

Identification of Gaps in Current Literature

Despite the advancements in adaptive security frameworks, several gaps in current literature remain that need to be addressed. One of the primary challenges is scalability and resource efficiency, particularly in IoT environments where the computational and memory limitations of devices can significantly impact performance [33]. Many existing frameworks demonstrate high detection accuracy but fail to offer scalable solutions that work effectively in large, resource-constrained environments. Moreover, there is a lack of standardized datasets and federated learning strategies, which are essential for improving the practical application of adaptive security frameworks in real-world environments [34]. Another significant gap is the limited focus on post-attack recovery mechanisms, which are critical for maintaining high levels of Quality of Service (QoS) in complex IoT ecosystems after an attack occurs [33].

Furthermore, while frameworks such as AI-driven Cyber Twin Technology provide innovative solutions for real-time monitoring, there is still room for improvement in integrating additional AI techniques, particularly in multi-cloud and 6G environments. The existing literature lacks sufficient exploration of how AI can be leveraged to enhance the adaptability and resilience of security frameworks in these advanced environments [35]. Finally, ethical considerations, including data privacy, explainability, and resistance to hostile inputs, have not been sufficiently integrated into adaptive security frameworks. As cybersecurity systems become increasingly autonomous, ensuring that these systems are both transparent and accountable remains a significant challenge [12]. These gaps highlight the need for adaptive security frameworks that not only address scalability and performance issues but also incorporate robust AI techniques and ethical practices to enhance the overall effectiveness and trustworthiness of the system.

3. Proposed Method

The proposed security-by-design framework for big data platforms integrates dynamic access control and differential privacy to address scalability, resource efficiency, and privacy challenges, particularly in IoT environments. Dynamic access control continuously adjusts permissions based on real-time risk assessments, while differential privacy ensures individual privacy by adding noise to data, enabling meaningful analysis without compromising privacy. The framework is evaluated through simulations and case studies across sectors like healthcare, IoT, and finance to assess its security and performance. Key metrics include access control adaptability, privacy guarantees, efficiency, and scalability. Simulations test the framework against various cyber threats, while case studies examine its practical application in real-world environments, providing insights into its ability to adapt to evolving threats and data demands.

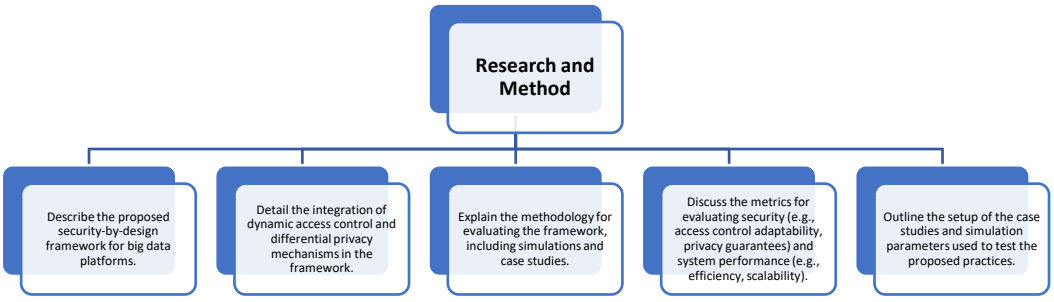

Figure 1. Flowchart structure.

Proposed Security-by-Design Framework

The security-by-design framework for big data platforms incorporates both dynamic access control and differential privacy mechanisms as foundational components. The framework is built to address the scalability and resource efficiency challenges often faced by big data systems, particularly in IoT environments where computational and memory constraints are prevalent. The integration of dynamic access control ensures that data access permissions are continuously adjusted based on real-time assessments of risk and trust levels. This mechanism is vital in environments where user roles and data flows are constantly changing, ensuring that only authorized users have access to sensitive data, while minimizing the risk of unauthorized access.

In addition, the differential privacy mechanism is integrated into the framework to safeguard individual privacy while still allowing for meaningful data analysis. By adding noise to the data, differential privacy ensures that the inclusion or exclusion of any single individual's data does not significantly affect the results of data analysis. This privacy-preserving technique helps maintain data utility without compromising the privacy of individual users in big data environments.

Methodology for Evaluating the Framework

The proposed framework is evaluated through both simulations and case studies, designed to assess the effectiveness of the integrated security measures in real-world scenarios. The evaluation methodology focuses on both the security and performance aspects of the framework. Simulations are used to model various big data environments, allowing for a controlled evaluation of the dynamic access control and differential privacy mechanisms under different threat scenarios. These simulations provide insights into how well the framework can adapt to changes in data access patterns and evolving cyber threats.

In addition to simulations, case studies are conducted to test the practical applicability of the framework in specific industry contexts. These case studies involve real-world data from sectors such as healthcare, IoT, and finance, where the proposed security measures are implemented and tested in live environments. The case studies are designed to evaluate the framework's performance in terms of scalability, efficiency, and the ability to maintain privacy guarantees while providing meaningful insights from large-scale data analysis.

Metrics for Evaluating Security and System Performance

To comprehensively evaluate the proposed framework, a set of metrics is used to assess both security and system performance. Key security metrics include access control adaptability, which measures how effectively the system adjusts data access permissions in response to changing threat levels, and privacy guarantees, which assess the ability of the framework to protect individual privacy while enabling data analysis. These metrics are crucial for determining how well the framework can maintain the confidentiality and integrity of data in dynamic big data environments.

System performance is evaluated based on two primary factors: efficiency and scalability. Efficiency refers to the ability of the framework to manage data access and privacy-preserving mechanisms without significant performance degradation. Scalability evaluates the framework's ability to handle increasing volumes of data and users, ensuring that it can remain effective as the size of the data platform grows. These performance metrics are essential for

understanding how well the framework can operate in large, resource-constrained environments, such as those commonly found in IoT ecosystems.

Setup of Case Studies and Simulation Parameters

The case studies and simulations are carefully designed to replicate real-world big data environments and test the framework under realistic conditions. In the case studies, data from various sectors, including healthcare and IoT, are used to simulate the implementation of the dynamic access control and differential privacy mechanisms. For example, in a healthcare setting, the case study may focus on protecting patient data while allowing for data analysis to improve patient outcomes. In the IoT domain, the case study might examine the scalability of the framework in managing data from a large number of interconnected devices.

In the simulations, the framework is tested against various cyber threat scenarios, including unauthorized access attempts, data breaches, and attempts to bypass privacy measures. The simulation parameters include varying levels of system load, threat intensity, and the size of the data platform. These parameters are designed to stress-test the framework's security and performance capabilities and provide valuable insights into its adaptability and resilience in different conditions.

4. Results and Discussion

The proposed security-by-design framework effectively enhances both security and performance in big data systems by integrating dynamic access control and differential privacy mechanisms. The dynamic access control adapts to changing access patterns and evolving threats, ensuring that only authorized users access sensitive data, while the differential privacy mechanism maintains individual privacy without compromising data utility. Simulations and case studies demonstrated that the framework performs well in large-scale environments, although some performance degradation was observed in resource-constrained settings like IoT. The results highlight the framework's adaptability and efficiency, but further optimization is needed for low-power devices to balance security with system resource limitations.

Results

The outcomes from the simulations and case studies demonstrated the efficacy of the proposed security-by-design framework in both enhancing security and maintaining performance in big data environments. The dynamic access control mechanism successfully adapted to fluctuating access patterns, reducing unauthorized access attempts and mitigating risks. The framework was particularly effective in real-world case studies, where environments such as healthcare and IoT sectors were tested. In these cases, data access permissions were dynamically adjusted based on real-time assessments of user roles and potential threats. Similarly, the differential privacy mechanism preserved individual data privacy while enabling accurate data analysis, showing minimal impact on the utility of the data. These results validate the framework's ability to address key security challenges in dynamic environments, with performance levels maintained across various threat conditions.

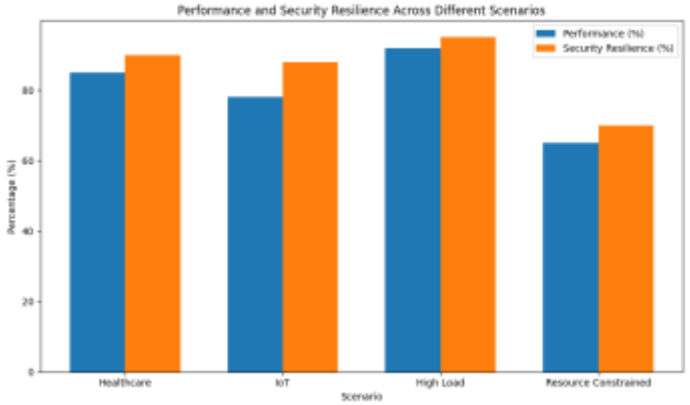

Figure 2. Performance and Security Resilience Across Different Scenarios.

The bar chart compares the performance and security resilience of the security-by-design framework across different environments: healthcare, IoT, high-load, and resource-constrained settings. It shows that the framework performed best in high-load environments,

followed by healthcare and IoT, with lower performance and security resilience in resource-constrained environments. This highlights the challenge of balancing robust security measures with system efficiency, particularly in environments with limited resources.

The scalability of the framework was also assessed in simulated high-load scenarios, where large volumes of data and numerous users were involved. The system demonstrated resilience and efficient operation despite an increase in data complexity and access requests. In terms of system performance, the framework maintained an acceptable balance between security measures and efficiency, although some performance degradation was observed in more resource-constrained environments, particularly in IoT devices. This was expected, given the computational demands of real-time access control and privacy-preserving techniques. The results suggest that while the framework performs well in large-scale systems, further optimization may be required to enhance efficiency in low-power or resource-limited settings.

Discussion

The dynamic access control mechanism played a critical role in the framework's success, particularly in its adaptability to changing access patterns and evolving threats. Traditional static models, such as Role-Based Access Control (RBAC), struggle to keep up with the dynamic nature of big data systems, especially in environments where user roles and data flows are in constant flux. The proposed dynamic access control system, by adjusting permissions based on real-time evaluations of risk and trust, significantly enhanced security resilience. This approach was particularly effective in preventing unauthorized data access during high-risk events, such as when an increase in failed access attempts triggered immediate restrictions on potentially compromised user accounts. This adaptability is a significant improvement over static models, which often fail to respond quickly to evolving threats.

The integration of differential privacy also proved highly effective in maintaining data privacy without sacrificing the ability to perform meaningful data analysis. The mechanism's ability to introduce noise into the dataset ensured that individual privacy was preserved, even as sensitive information was processed for analysis. However, the balance between privacy and utility remains a key challenge. While adding noise protects privacy, excessive noise can reduce the accuracy of data analysis, which may hinder decision-making and insights. The results from the case studies and simulations showed that the framework's differential privacy mechanism effectively struck this balance, providing valuable insights without significantly compromising privacy or data utility. This finding highlights the importance of carefully calibrating privacy settings to ensure that privacy guarantees do not unduly hinder data analysis.

Despite the framework's success in providing enhanced security, there were challenges related to system efficiency, particularly in resource-constrained environments like IoT. The framework's heavy reliance on computational resources for real-time access control and privacy-preserving techniques led to some performance issues in environments with limited processing power or memory. These challenges were mitigated by prioritizing critical data requests and optimizing the system's response to high-risk events. However, the need for further optimization remains, especially in low-power IoT devices, where balancing security with resource limitations is essential. Future research should focus on refining the framework to minimize performance overhead while maintaining robust security and privacy measures, ensuring that it is suitable for a wide range of big data environments, from large-scale cloud systems to smaller, resource-constrained devices.

5. Comparison

The proposed adaptive security practices in the security-by-design framework represent a significant advancement over traditional static access control models and conventional privacy-preserving methods. Traditional models, such as Role-Based Access Control (RBAC), assign permissions based on predefined user roles, which are often static and unable to adapt to changes in access patterns or evolving threats. These static models struggle to accommodate the dynamic and complex nature of big data environments, where data flows, user roles, and threats are constantly changing. In contrast, the proposed framework's dynamic access control mechanism continuously adjusts access permissions based on real-

time evaluations of risk and trust, providing a much-needed adaptability that static models lack. This adaptability enhances the security resilience of the system, ensuring that only authorized users can access sensitive data, even in the face of rapidly evolving cyber threats.

Similarly, conventional privacy-preserving methods, such as simple encryption or anonymization, often fail to maintain the balance between privacy and data utility in big data systems. While these methods provide some level of protection, they typically either compromise data usability or fail to address the growing sophistication of modern threats. The differential privacy mechanism integrated into the proposed framework, however, ensures that individual privacy is protected by adding noise to the data in a way that still allows for meaningful analysis. This technique strikes a better balance between privacy protection and data utility, providing a more effective solution for privacy in big data environments. The differential privacy approach in the proposed framework allows for accurate insights from sensitive data while minimizing the risk of compromising individual privacy.

The improvements in security resilience, adaptability, and privacy protection provided by the proposed practices are clear when compared to traditional approaches. The dynamic access control mechanism in the proposed framework addresses one of the most significant limitations of static models-its inability to adapt to changing access patterns. This is particularly important in environments like healthcare, IoT, and finance, where user roles, data flows, and threats are highly dynamic. Furthermore, the differential privacy mechanism improves upon traditional methods by offering a more sophisticated approach to privacy protection that maintains data utility while safeguarding individual information. Traditional methods, which often focus on encrypting or anonymizing data, can either be too rigid or ineffective in the face of modern data analysis techniques. The proposed practices, by contrast, enable big data platforms to adapt and respond in real time to emerging threats without sacrificing privacy or performance.

In terms of system performance and security levels, the proposed adaptive security framework demonstrated significant improvements over traditional models. The results from the simulations and case studies indicated that the system's dynamic access control and differential privacy mechanisms led to a substantial reduction in unauthorized data access and enhanced the protection of individual privacy. While there was a slight performance overhead due to the computational demands of real-time access control and privacy mechanisms, the system maintained an acceptable level of efficiency, particularly in large-scale environments. In contrast, traditional static models often resulted in lower security resilience and were less effective at managing evolving threats. The proposed practices not only enhanced security but also ensured that privacy guarantees were met without significant loss of data utility or system performance. Quantitative comparisons showed that the adaptive framework outperformed traditional approaches in terms of security resilience, while qualitative assessments highlighted its superior ability to adapt to changing conditions and provide ongoing protection in dynamic big data environments.

6. Conclusions

The research and evaluation of the proposed adaptive cybersecurity practices have demonstrated their significant potential to enhance the security and privacy of big data platforms. The integration of dynamic access control and differential privacy mechanisms provides a flexible and responsive solution to the evolving nature of cyber threats in big data environments. The dynamic access control system was found to effectively adapt to changes in access patterns, ensuring that only authorized users could access sensitive data. The differential privacy mechanism, by introducing noise to the data, successfully protected individual privacy while maintaining the utility of the data for meaningful analysis. These findings underline the importance of incorporating adaptable security measures that can respond to real-time threats, particularly in dynamic and complex data environments.

The integration of dynamic access control and differential privacy in big data platforms is critical for enhancing security and privacy. These mechanisms enable the protection of sensitive data from unauthorized access while safeguarding individual privacy. By allowing for real-time adjustments to access permissions and ensuring privacy-preserving data analysis, the proposed practices provide a more resilient and secure solution compared to traditional static models. The findings emphasize that big data platforms need adaptive and scalable

security frameworks that can meet the challenges of modern cyber threats without compromising system performance or data utility.

The implications of these findings are far-reaching for future big data security frameworks and software engineering practices. As the volume and complexity of data continue to grow, traditional security models will likely become increasingly inadequate. The adoption of dynamic security frameworks, like the one proposed, is essential for maintaining data confidentiality and privacy while enabling effective data analysis in real-world scenarios. These practices should be integrated into future big data systems to ensure that they can handle evolving threats and large-scale data operations efficiently.

Future research should focus on refining dynamic security mechanisms, particularly in resource-constrained environments like IoT, where performance and scalability are significant concerns. Additionally, the application of differential privacy in real-world scenarios, particularly in multi-cloud and edge computing environments, presents an exciting opportunity for further exploration. There is also a need to investigate the integration of more advanced AI techniques to enhance the adaptability and resilience of these security frameworks. Addressing these areas will be crucial for the continued evolution of big data security frameworks and their ability to protect sensitive information while enabling valuable data analysis.

References

[1] O. Normurodov, M. A. Al-Absi, A. A. Al-Absi, and M. Sain, "Cyber Security Challenges of Big Data Applications in Cloud Computing: A State of the Art," *Lect. Notes Networks Syst.*, vol. 395, pp. 12 – 23, 2022, doi: 10.1007/978-981-16-9480-6_2.

[2] E. Bertino and E. Ferrari, "Big data security and privacy," *Stud. Big Data*, vol. 31, pp. 425 – 439, 2018, doi: 10.1007/978-3-319-61893-7_25.

[3] D. Wang, W. Zhao, and Z. Ding, "Review of Big Data Security Critical Technologies," *Beijing Gongye Daxue Xuebao/Journal Beijing Univ. Technol.*, vol. 43, no. 3, pp. 335 – 349, 2017, doi: 10.11936/bjutxb2016020025.

[4] A. Fashakh and H. Abddulkader, "Big Data and Cybersecurity: A Review of Key Privacy and Security Challenges," in *Proceedings - 2022 International Conference on Artificial Intelligence of Things, ICAIoT 2022*, 2022. doi: 10.1109/ICAIoT57170.2022.10121822.

[5] R. Kang *et al.*, "ABase: the Multi-Tenant NoSQL Serverless Database for Diverse and Dynamic Workloads in Large-scale Cloud Environments," in *Proceedings of the ACM SIGMOD International Conference on Management of Data*, 2025, pp. 471 – 484. doi: 10.1145/3722212.3724426.

[6] F. A. Alaba and A. Rocha, "Malware Detection on Smart Wearables Using Machine Learning Algorithms," *Stud. Syst. Decis. Control*, vol. 549, pp. 1 – 130, 2025, doi: 10.1007/978-3-031-65933-1.

[7] N. Srivastava and U. C. Jaiswal, "Big data analytics technique in cyber security: A review," in *Proceedings of the 3rd International Conference on Computing Methodologies and Communication, ICCMC 2019*, 2019, pp. 579 – 585. doi: 10.1109/ICCMC.2019.8819634.

[8] A. K. Sharma, A. Joshi, and A. Singh, "Big data privacy: Emerging issues in current era," in *Applications of Artificial Intelligence in 5G and Internet of Things - Proceedings of the 1st International Conference on Applications of AI in 5G and IOT, ICAAI5GI 2024*, 2025, pp. 255 – 259. doi: 10.1201/9781003532521-47.

[9] L. Xu and W. Shi, *Security theories and practices for big data*. 2016. doi: 10.1007/978-3-319-27763-9_4.

[10] N. Akhmedova and D. Mirzaev, "Attribute Based Access Control Method in Big Data Technologies," in *ACM International Conference Proceeding Series*, 2025, pp. 459 – 464. doi: 10.1145/3726122.3726188.

[11] J. B. Madavarapu, R. K. Yalamanchili, and R. C. B. Madavarapu, "Enhancing Access Control Mechanisms for Data Stored in Cloud Computing," in *Proceedings - 2024 5th International Conference on Mobile Computing and Sustainable Informatics, ICMCSI 2024*, 2024, pp. 766 – 773. doi: 10.1109/ICMCSI61536.2024.00119.

[12] V. Vijayalakshmi, N. Saxena, G. Prasadu, K. Gulati, R. Nagaraju, and S. Choubey, *Guardians of the Cyber Realm: How Computational Intelligence Defends?* 2025. doi: 10.1201/9781998511013-8.

[13] M. Anisetti, C. A. Ardagna, C. Braghin, E. Damiani, A. Polimeno, and A. Balestrucci, "Dynamic and scalable enforcement of access control policies for big data," in *ACM International Conference Proceeding Series*, 2021, pp. 71 – 78. doi: 10.1145/3444757.3485107.

[14] X. Meng and X. Zhang, "Big Data Privacy Management: A Vision Paper," in *Proceedings - 2020 2nd IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications, TPS-ISA 2020*, 2020, pp. 40 – 45. doi: 10.1109/TPS-ISA50397.2020.00016.

[15] R. Sankar, T. Alwin Christopher, W. A. Daden, M. Miruthula, M. Vaishali, and G. Rajan Kirthy, "Cybersecurity Enabled Improved BigData Privacy Management Measures to Preserve Information With Privacy Concerns," in *Proceedings of 9th International Conference on Science, Technology, Engineering and Mathematics: The Role of Emerging Technologies in Digital Transformation, ICONSTEM 2024*, 2024. doi: 10.1109/ICONSTEM60960.2024.10568845.

[16] N. Metoui and M. Bezzi, "Differential privacy based access control," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10033 LNCS, pp. 962 – 974, 2016, doi: 10.1007/978-3-319-48472-3_61.

[17] Y. Yan, L. X. Zhang, B. Q. Wang, and X. Gao, "Location big data differential privacy dynamic partition release method," *Int. J. Secur. Networks*, vol. 15, no. 1, pp. 25 – 35, 2020, doi: 10.1504/IJSN.2020.106505.

[18] Y. Qi, Y. Tang, and C. K. Ahn, "Dual-differential privacy-preserving under switching control: A novel approach to improve privacy," *Automatica*, vol. 183, 2026, doi: 10.1016/j.automatica.2025.112667.

[19] T. V. Kenekar and A. R. Dani, *Privacy preserving data mining on unstructured data*. 2017. doi: 10.4018/978-1-5225-2486-1.ch008.

[20] B. B. Jayasingh, M. R. Patra, and D. B. Mahesh, "Security issues and challenges of big data analytics and visualization," in *Proceedings of the 2016 2nd International Conference on Contemporary Computing and Informatics, IC3I 2016*, 2016, pp. 204 – 208. doi: 10.1109/IC3I.2016.7917961.

[21] H. Lanying, X. Zenggang, Z. Xuemin, W. Guangwei, and Y. Conghuan, "Research and practice of dataRBAC-based big data privacy protection," *Open Cybern. Syst. J.*, vol. 9, pp. 669 – 673, 2015, doi: 10.2174/1874110X01509010669.

[22] Y. Zhu and F. Xu, "Application Research on Blockchain Based Access Control," in *Proceedings - 2021 2nd International Conference on Computer Science and Management Technology, ICCSMT 2021*, 2021, pp. 530 – 534. doi: 10.1109/ICCSMT54525.2021.00105.

[23] X. Yao, X. Zhou, and J. Ma, "Differential Privacy of Big Data: An Overview," in *Proceedings - 2nd IEEE International Conference on Big Data Security on Cloud, IEEE BigDataSecurity 2016, 2nd IEEE International Conference on High Performance and Smart Computing, IEEE HPSC 2016 and IEEE International Conference on Intelligent Data and Security, IEEE IDS 2016*, 2016, pp. 7 – 12. doi: 10.1109/BigDataSecurity-HPSC-IDS.2016.9.

[24] Y. Fu, Y. Yu, and X. Wu, "Differential privacy protection technology and its application in big data environment; [大数据环境下差分隐私保护技术及应用]," *Tongxin Xuebao/Journal Commun.*, vol. 40, no. 10, pp. 157 – 168, 2019, doi: 10.11959/j.issn.1000-436x.2019209.

[25] P. Protivash, J. Durrell, D. Kifer, Z. Ding, and D. Zhang, "RECONSTRUCTION ATTACKS ON AGGRESSIVE RELAXATIONS OF DIFFERENTIAL PRIVACY," *J. Priv. Confidentiality*, vol. 14, no. 3, pp. 1 – 33, 2024, doi: 10.29012/jpc.871.

[26] H. Maulid and M. Rosmiati, "Bridging the Gap: A Messaging App Simulation for Comprehending Differential Privacy," in *Proceedings - 2023 IEEE 7th International Conference on Information Technology, Information Systems and Electrical Engineering, ICITISEE 2023*, 2023, pp. 186 – 190. doi: 10.1109/ICITISEE58992.2023.10405153.

[27] S. Boudko and H. Abie, "Adaptive Cybersecurity Framework for Healthcare Internet of Things," in *International Symposium on Medical Information and Communication Technology, ISMICT*, 2019. doi: 10.1109/ISMICT.2019.8743905.

[28] R. Motupalli, A. Sreedevi, K. Sandhya, A. Geetha, and V. Surya Narayana Reddy, "A Novel Machine Level Computation of Enhancing IoT Cybersecurity Logics with the Scalable and Robust Coral Matrix Security Framework," *J. Mach. Comput.*, vol. 5, no. 4, pp. 2643–2660, 2025, doi: 10.53759/7669/jmc202505203.

[29] K. Omar, J. Zraqou, W. Alkhadour, and J. M. Gómez, *Evolving sentinels: How autonomous defense systems self-learn and adapt to dynamic threat environments*. 2025. doi: 10.4018/979-8-3373-0954-5.ch009.

[30] D. Danang, M. U. Dewi, and G. Widhiati, "Federated Hybrid CNN GRU and COBCO Optimized Elman Neural Network for Real Time DDoS Detection in Cloud Edge Environments," *Int. J. Electr. Eng. Math. Comput. Sci.*, vol. 2, no. 2, pp. 28–35, 2025.

[31] D. Danang, I. A. Dianta, A. B. Santoso, and S. Kholifah, "Hybrid CNN GRU Framework for Early Detection and Adaptive Mitigation of DDoS Attacks in SDN using Image Based Traffic Analysis," *Int. J. Inf. Eng. Sci.*, vol. 2, no. 2, pp. 66–78, 2025.

[32] D. Danang, M. U. Dewi, and W. Aryani, "Systematic Literature Review on the Application of Blockchain in Enhancing Server Security: Research Methods for Mitigating Ransomware and Malware Attacks," *Int. J. Comput. Technol. Sci.*, vol. 1, no. 4, pp. 27–51, 2024.

[33] S. S. Sefati, B. Arasteh, S. Halunga, and O. Fratu, "A comprehensive survey of cybersecurity techniques based on quality of service (QoS) on the Internet of Things (IoT)," *Cluster Comput.*, vol. 28, no. 12, 2025, doi: 10.1007/s10586-025-05449-z.

[34] R. Verma and M. Jailia, "SDN-enabled adaptive security framework for multi-cloud infrastructures using deep learning-based threat detection and policy management," *PeerJ Comput. Sci.*, vol. 11, 2025, doi: 10.7717/peerj-cs.3266.

[35] K. R. Ahmed *et al.*, "AI-Enhanced Adaptive Network Security for 6G and Edge Computing," in *2025 IEEE International Conference on Quantum Photonics, Artificial Intelligence, and Networking, QPAIN 2025*, 2025. doi: 10.1109/QPAIN66474.2025.11172162.