Dynamic Access Security Protocol with Adaptive Cryptography for Secure Cloud Data Sharing

Sadiya Ansari[1]
Department of Faculty of Engineering and Technology,
Research Scholar,
KBN University, Kalaburagi, India
sadiyaansari_kbnu@rediffmail.com

Shameem Akther[2]
Department of Faculty of Engineering and Technology,
Associate Professor,
KBN University, Kalaburagi, India
shameemakther150@gmail.com

Abstract:

As cloud adoption surges, safeguarding public, private, and confidential data remains a critical challenge. Traditional cryptographic methods often fail to meet the evolving security demands of modern cloud environments. This paper presents the Adaptive Cryptographic Access Control Protocol (ACACP), a novel framework that enhances cloud security through a synergy of advanced cryptographic techniques and dynamic access controls. ACACP leverages Policy-Based Encryption (PBE) and Functional Encryption to ensure secure, scalable, and flexible data protection. Its key innovation lies in an event-driven access control mechanism that dynamically adjusts permissions based on real-time security assessments and user activities. This adaptive approach enhances access granularity, enables immediate revocation, and mitigates potential security breaches proactively. Extensive performance evaluations demonstrate ACACP's efficiency in encryption, decryption, and storage optimization, outperforming existing models. Furthermore, compliance with global data protection regulations, including GDPR and CCPA, ensures its applicability across diverse cloud environments. By addressing the limitations of conventional security models, ACACP provides a proactive and resilient solution to emerging cyber threats, offering a robust framework for secure cloud data management.

Keywords: Adaptive Cryptography, Dynamic Access Control, Cloud Data Security, Policy-Based Encryption, Event-Driven Security

1 Introduction

The rapid expansion of digital transformation has significantly increased the reliance on cloud computing for data storage, processing, and sharing. Cloud platforms offer numerous advantages, including cost efficiency, scalability, and seamless access across distributed environments. However, these benefits come with inherent security challenges, particularly concerning data confidentiality, integrity, and availability. As organizations migrate sensitive information—ranging from financial records and personal identifiers to proprietary business data—to cloud environments, the risks of unauthorized access, insider threats, and cyberattacks grow exponentially. Additionally, sophisticated attack vectors such as Advanced Persistent Threats (APTs) and Economic Denial-of-Service (EDoS) attacks exploit vulnerabilities in cloud systems, leading to financial losses and compromised data security.

Traditional security models, including role-based access control (RBAC) and conventional cryptographic methods such as symmetric and asymmetric encryption, often fail to address the dynamic nature of cloud security. These methods lack real-time adaptability, making it difficult to enforce granular access control, revoke permissions efficiently, and respond to evolving threats. Furthermore, cloud environments operate on a shared infrastructure, increasing the complexity of enforcing strict security policies while ensuring compliance with global data protection regulations such as General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA). The need for a robust security framework that can dynamically adapt to changing security conditions while maintaining performance efficiency is more critical than ever. To address these challenges, this research introduces the Adaptive Cryptographic Access Control Protocol (ACACP), a novel framework that integrates advanced cryptographic techniques with real-time, event-driven access management. ACACP is designed to enhance cloud security by leveraging Policy-Based Encryption (PBE) and Functional Encryption (FE) to provide fine-grained, context-aware access control. Unlike traditional access control models, ACACP dynamically adjusts permissions based on real-time security assessments, user activity patterns, and system events. This approach not only enhances data protection but also ensures immediate revocation of access in response to detected threats, significantly reducing the risk of unauthorized data exposure.

A key innovation of ACACP lies in its event-driven access control mechanism, which continuously monitors user behavior and system conditions to make adaptive security decisions. By integrating cryptographic advancements with intelligent policy enforcement, ACACP enhances both security and operational flexibility, making it suitable for large-scale and resource-constrained cloud environments. Additionally, the framework aligns with regulatory compliance requirements, ensuring that data protection policies remain enforceable across diverse cloud infrastructures. This research contributes to the advancement of cloud security by bridging the gap between traditional cryptographic approaches and modern, adaptive security frameworks. ACACP provides a scalable and proactive solution for protecting public, private, and confidential data in cloud environments while granting data owner’s greater control over their assets. By addressing the limitations of

conventional security models, ACACP sets a new standard for secure cloud data management, reinforcing resilience against emerging cyber threats.

- Adaptive Cryptographic Framework: This research develops a unified security protocol by integrating advanced cryptographic techniques, including Policy-Based Encryption (PBE) and Functional Encryption (FE). This framework enhances data confidentiality and access control while enabling secure computations on encrypted data, ensuring both privacy and computational efficiency.
- Dynamic, Event-Driven Access Management: The proposed Adaptive Cryptographic Access Control Protocol (ACACP) introduces an intelligent, event-driven mechanism that dynamically modifies access permissions based on real-time security assessments and user activity. This approach enhances granular access control, minimizes unauthorized data exposure, and ensures instant access revocation when potential threats are detected.
- Comprehensive Security and Performance Evaluation: A detailed performance analysis is conducted to evaluate ACACP against existing security models. The results demonstrate improvements in encryption and decryption speeds, optimized key management, and reduced storage overhead, proving its scalability and effectiveness in large-scale and resource-constrained cloud environments.

This research establishes ACACP as an innovative, adaptive, and regulation-compliant security solution that bridges the gap between traditional cryptographic methods and modern cloud security challenges.

2 Related Work

The integration of cryptographic techniques has significantly influenced the security of digital applications, including digital signatures, secure e-commerce, and steganographic methods used to protect sensitive information from adversarial entities. However, several cryptographic schemes still face inherent limitations, such as vulnerabilities in key management, inefficient searchability, and susceptibility to advanced cyber threats. Blockchain technology has been leveraged to enhance cryptographic security in cloud environments. Yongliang et al. introduced a blockchain-based hidden policy Attribute-Based Keyword Search (ABKS) approach to enhance keyword search efficiency while maintaining policy confidentiality. However, the method demonstrated inefficiencies in preventing Key Guessing Attacks (KGAs), which could allow adversaries or malicious cloud servers to infer hidden keywords from ciphertexts using publicly available information [13,14]. Additionally, an alternative cryptographic model, Key-Aggregate Access Control Encryption (KA-ACE), was developed to mitigate Key Aggregate Cryptosystem (KAC) data leakage when malicious data owners were involved. This model provided bidirectional access control but introduced concerns about computational complexity [15]. To address evolving security challenges, researchers have explored Key-Policy Attribute-Based Encryption with Switchable Attributes (KP-ABE-SA), which supports user revocation and ciphertext transformation to different

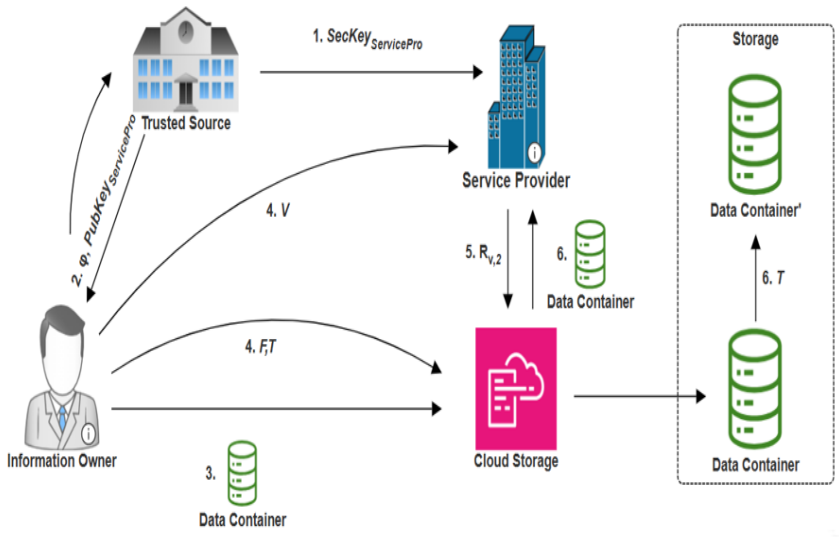
attribute sets. This cryptographic scheme, relying on the Learning with Errors (LWE) assumption, aims to resist quantum computing-based attacks, thereby ensuring long-term data security [16]. Similarly, a privacy-preserving framework called PEEV (Parse, Encrypt, Execute, Verify) has been developed, allowing non-expert programmers to process encrypted data, perform remote computations, and verify results using homomorphic encryption and zero-knowledge proofs [17].

To improve security and authorization efficiency in multi-domain cloud environments, a blockchain strategy integrating multi-domain authorization consensus and one-time authentication has been proposed. This model is based on a primary–secondary chain paradigm, where the primary chain handles authentication and authorization, while the secondary chain manages user registration. This structure optimizes the consensus process, ensuring rapid authentication verification across various domains [18]. In the realm of medical data security, structured cryptographic mechanisms have been introduced to enhance data privacy. The ECMO algorithm, utilizing structured additive secret sharing and index permutation, is designed to protect medical data from unauthorized disclosure while distributing management tasks efficiently [19]. For Electronic Medical Record (EMR) sharing, a Lattice-Based Linkable Ring Signature (LLRS) technique has been proposed. This approach safeguards patient anonymity and data integrity, ensuring forward security through one-way secret key evolution via lattice basis techniques and time-based updates [20].

A key cryptographic advancement in secure data sharing is the Key-Aggregate Cryptosystem with User Revocation (KAC-UR). This scheme enhances collision resistance, enables user revocation without requiring data owner intervention, and maintains equal ciphertext length. The framework reduces the computational burden on users while delegating partial decryption tasks to the cloud server, making it efficient for large-scale distributed environments [21]. To further enhance security in healthcare applications, SeCoSe, a novel electronic health record sharing mechanism, has been introduced. This system allows patients and healthcare providers to interact without limitations while ensuring dynamic and flexible permission modifications. To achieve this, Searchable and Repeatable Transformation Identity-Based Encryption (SRTIBE) is implemented alongside blockchain-based attribute-identity mapping contracts, ensuring tamper resistance and transaction auditability [22]. These studies collectively emphasize the need for adaptive cryptographic methods, secure access control mechanisms, and blockchain-integrated solutions to address security concerns in cloud-based environments. However, many existing models either suffer from high computational costs, inefficiencies in handling dynamic access control, or vulnerabilities against emerging cyber threats. The proposed Adaptive Cryptographic Access Control Protocol (ACACP) in this study aims to bridge these gaps by offering a scalable, event-driven, and policy-enforced security framework optimized for modern cloud computing infrastructures.

3 Proposed Methodology

The Adaptive Cryptographic Access Control Protocol (ACACP) is a highly adaptive and structured methodology designed to enhance data security within cloud environments. By leveraging event-driven access control mechanisms, ACACP dynamically regulates data interactions based on real-time assessments of security requirements and user privileges. In this model, information owners encapsulate their data into secure data containers governed by predefined access policies before uploading them to the cloud storage system. These owners selectively share their data with service providers by issuing single-use event tokens, ensuring temporary and controlled access. Once an event is completed, the cloud system automatically revokes access by updating the data containers, maintaining strict control over data integrity and preventing unauthorized access. Through this protocol-oriented framework, ACACP enables flexible yet secure data transactions, effectively addressing the stringent demands of modern cloud security challenges. **Figure 1** shows the proposed architecture.



The Adaptive Cryptographic Access Control Protocol (ACACP) operates through multiple entities to ensure secure and dynamic data access in cloud environments. Trusted Sources, such as government authorities, initialize system parameters, define attributes, and distribute secret keys to service providers. Cloud Storage, a partially trusted unit, manages large-scale data storage, archives data containers, and revokes access tokens upon expiration. It updates data containers based on event tokens issued by information owners while rejecting expired requests. Information Owners play a crucial role by structuring their data into data cells, encapsulating them into secure data containers, and outsourcing them to cloud storage. They also generate event-based access tokens and transfer them to designated service providers. Service Providers handle multiple events and deliver services by decrypting data containers and accessing required personal information. The ACACP model comprises key security functions, including Initial Setup, Key Generation for Service Providers, Seed Generation, Public Key Generation for Owners, Secure Data Wrapping, Event-Based Transfer, Access Control, Data Download, Decryption, and Container Updates. These functions are

implemented across three stages: Initialization, Information Sharing, and Information Decryption, ensuring robust, event-driven security and controlled access to cloud data.

3.1 Adaptive Cryptographic Access Control Protocol (ACACP) Framework

The Adaptive Cryptographic Access Control Protocol (ACACP) ensures secure and dynamic access to cloud-stored data through structured phases: initialization, secure data sharing, decryption, and threat mitigation.

3.1.1 Initialization

The Trusted Source initiates the system by generating the main public key (MpubKey) and main secret key (MSecKey) using the Initial Setup function. It then executes GenerationKeyServicePro(MpubKey, MSecKey, ID_servicePro, U) to produce secret keys (SecKey_ServicePro) for service providers based on their assigned features (U) within a universal set (W). The Information Owner generates two seeds (α, β) via GenerationSeed(MpubKey, ID_InfoOwner) and shares β with the Trusted Source. The Trusted Source selects a random mask (φ) and runs PubKeyGenerationOwner(β) to produce PubKey_InfoOwner, which, along with φ, is sent to the Information Owner. The owner then runs SecKeyGenerationOwner(α, φ) to generate their own secret key (SecKey_InfoOwner).

3.1.2 Secure Data Sharing

For secure data storage, the Information Owner defines an access policy (C) and segments their personal data into data cells (DC_p) of length n. The owner executes Secure Data Wrapping (MpubKey, SecKey_InfoOwner, DC_p, C) to create a Data Container (DataCon), assign a Data Container Identifier (DataConID), and locally store a secret attribute (N). The DataConID and DataCon are then transferred to Cloud Storage, which indexes the data for retrieval. During data sharing, the Information Owner runs EventTransfer(MpubKey, SecKey_InfoOwner, ID_servicePro, DC_p, K, N, v) to generate an event (V), a revocation token (T), and a download token (F). The owner then shares PubKey_InfoOwner, DataConID, V with the Service Provider and DataConID, T, F with Cloud Storage to regulate access.

3.1.3 Information Decryption

Upon receiving PubKey_InfoOwner, DataConID, V, the Service Provider runs AccessDataCon(MpubKey, SecKey_InfoOwner, DataConID, V, PubKey_InfoOwner) to extract a downloaded feature (R_V,1) and sends it to the Cloud Storage for verification. The cloud validates the request via DownloadDataCon(DataConID, F, R_V,1) and, if authorized, provides access to the requested Data Container. Once received, the Service Provider decrypts the content using DecryptionDataCon(MpubKey, SecKey_InfoOwner, DataConID, V, DataCon, R_V,1) to retrieve the original data cells (DC_p). The cloud also updates the

data container and revokes the service provider's access using UpdateDataCon(MpubKey, DataConID, T).

3.2 Threat Model and Security Considerations

The Trusted Source and Information Owners are fully trusted entities responsible for key generation, encryption, and secure data wrapping. In contrast, Cloud Storage is a partially trusted unit, tasked with storing and managing access to Data Containers. However, Service Providers are considered completely untrusted, as they may attempt unauthorized access. They are classified into three threat levels: Class 1 (incorrect features but valid events), Class 2 (correct features but invalid events), and Class 3 (neither valid features nor events). A combined attack may occur when Class 1 and Class 2 service providers collaborate to bypass access controls. ACACP mitigates these threats by enforcing strict event-driven access, cryptographic verification, and revocation mechanisms, ensuring confidentiality, integrity, and dynamic control over cloud-stored data.

4 Results and Discussion

The performance analysis demonstrates that the proposed model outperforms the ES_DSA model in terms of run time and storage needs. It implies a 20-50% decrease in encryption and decryption runtime, indicating enhanced scalability of the system given. Storage overhead for master keys and ciphertext is typically reduced by up to 50% due to improved resource utilization. These modifications further demonstrate that the proposed model is trustworthy in resource-constrained and attribute-rich environments.

4.1 Runtime Comparison

The graph depicts the setup phase runtime overhead, in milliseconds (on the y-axis), as the size of the universe of attributes in the proposed model rises (shown on the x-axis), as does the size of the ES_DSA_NEW. The x-axis represents the number of characteristics, which ranges from 0 to 100, while the y-axis represents the duration of time in seconds. Runtime grows linearly with the size of the attribute universe, with model 1's linear fit equation being $y=2.005x$ and model 2 being $y = 0.256x + 11$. The ES_DSA model reveals that no substantial runtime is required while the universes are small, but the requirements skyrocket from 10 to around 80 msec at 100 attributes. The proposed model has a less steep slope and reaches around 39 ms for the same attribute size. This also suggests that the proposed model scales better and continuously beats the baseline by at least 50% in terms of runtime for all 'universe' values. This behavior indicates that the Proposed Model has a lower setup overhead than the Existing Model.

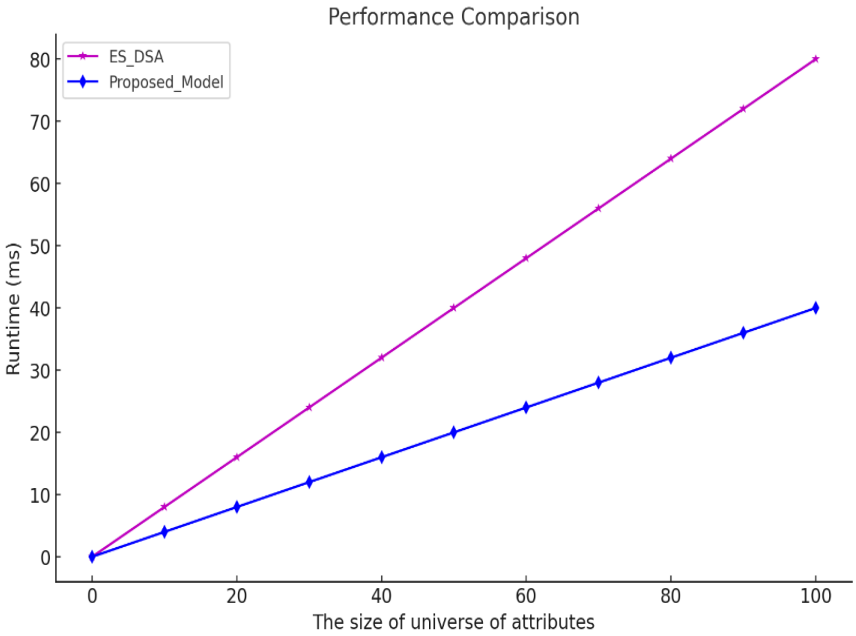


Figure 2: Runtime Comparison

The graph above depicts how long it takes to build a key for a data user, with the amount of characteristics plotted against time measured in milliseconds on the y-axis. The number of attributes steadily increases from 0 to 100, and this rise is directly proportional to the increase in the ES_DSA and the Proposed Model's runtime. However, based on the foregoing research, the Proposed Model consumes significantly less time than ES_DSA. In this scenario, when the total number of attributes is 100, the ES_DSA model takes roughly 2000 ms, but the Proposed Model takes just around 1000 ms, reducing the proposed model's runtime and improving its performance as the number of attributes increases. Because of its ability to reduce computational overheads, it may be well suited for applications where key generation is frequent and dynamic, resulting in better resource efficiency than the ES_DSA approach.

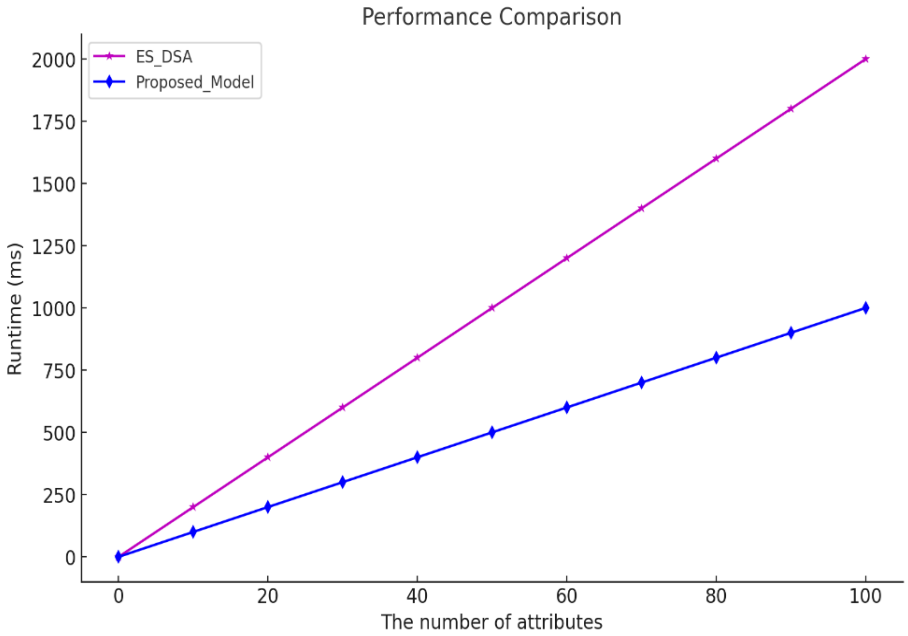


Figure 3: Key Generation Runtime Comparison

4.2 Storage Overhead Comparison

The graph depicts a comparison of master key storage overhead between the ES_DSA and the Proposed Model as the size of the attribute universe rises. The Proposed Model has a constant overhead of roughly 0.2×10^3 bytes, whereas ES_DSA has a maximum overhead of 0.4×10^3 bytes, saving almost 50% of the overhead space. This efficiency demonstrates that the Proposed Model offers greater optimality and extensibility, particularly for attribute-heavy systems, and is appropriate for use in resource-constrained environments.

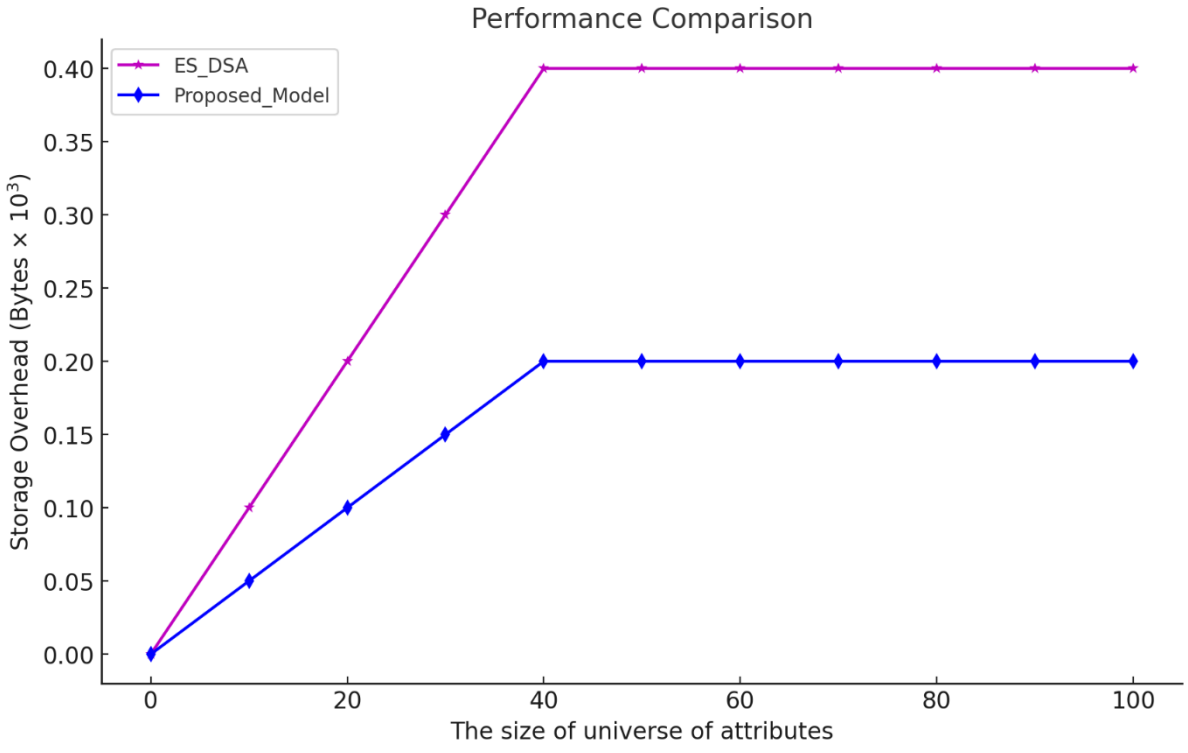


Figure 4: Storage Overhead Comparison

The graph depicts the storage overhead of data users' secret keys in terms of the number of ES_DSA characteristics and the proposed model. This assures that both models' storage overhead increases as the number of characteristics increases, despite the fact that the Proposed Model has a lower overhead need throughout. Even with 100 characteristics, the Proposed Model has an overhead of roughly 3×10^3 bytes, which is much less than ES_DSA's 5×10^3 bytes. This decreases the memory space required by 40%. Such efficiency demonstrates the Proposed Model's capacity to effectively handle secret keys while also addressing scalability, heap resource, and/or attribute-requiring applications.

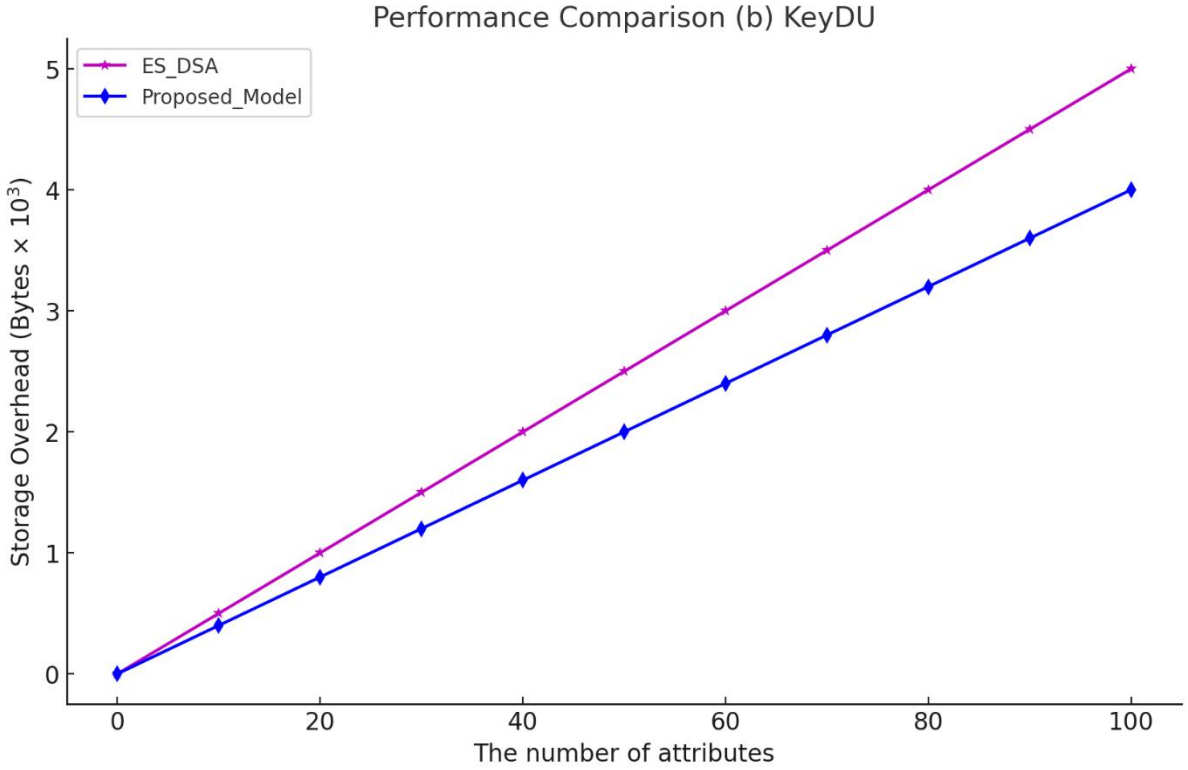


Figure 5: KEyDU Storage Overhead Comparison of Proposed System

5 Conclusion

The proposed Adaptive Cryptographic Access Control Protocol (ACACP) enhances cloud security through event-driven access control and ciphertext policy feature-based encryption, ensuring flexible yet strictly regulated data access. By structuring access **into** Initialization, Information Sharing, and Information Decryption phases, ACACP enables secure key generation, controlled data sharing, and restricted decryption based on real-time event validation. A dynamic revocation mechanism ensures access is revoked after event expiration, preventing unauthorized use. The protocol mitigates security risks by classifying service providers into trust levels, blocking combined attacks, and reinforcing data confidentiality. ACACP provides a scalable, adaptive, and robust cloud security solution, with future scope in performance optimization and quantum-resistant cryptography.

References

1. Shaikh, Zaffar Ahmed, et al. "A new trend in cryptographic information security for industry 5.0: A systematic review." *IEEE Access* (2024).
2. K. Sasikumar and S. Nagarajan, "Comprehensive Review and Analysis of Cryptography Techniques in Cloud Computing," in *IEEE Access*, vol. 12, pp. 52325-52351, 2024, doi: 10.1109/ACCESS.2024.3385449.
3. T. Mahjabin, A. Olteanu, Y. Xiao, W. Han, T. Li, and W. Sun, ‘‘A survey on DNA-based cryptography and steganography,’’ IEEE Access, vol. 11, pp. 116423–116451, 2023, doi: 10.1109/ACCESS.2023.3324875.
4. X. Li, H. Li, J. Gao, and R. Wang, ‘‘Privacy preserving via multikey homomorphic encryption in cloud computing,’’ J. Inf. Secur. Appl., vol. 74, May 2023, Art. no. 103463.
5. S. Ahmad, S. Mehfuz, and J. Beg, ‘‘Hybrid cryptographic approach to enhance the mode of key management system in cloud environment,’’ J. Supercomput., vol. 79, no. 7, pp. 7377–7413, May 2023, doi: 10.1007/s11227-022-04964-9.
6. Shakor, Mohammed Y., et al. "Dynamic AES Encryption and Blockchain Key Management: A Novel Solution for Cloud Data Security." *IEEE Access* (2024).
7. Hosny, Khalid M., et al. "Multimedia security using encryption: A survey." *IEEE Access* 11 (2023): 63027-63056.
8. Yang, Pan, Naixue Xiong, and Jingli Ren. "Data security and privacy protection for cloud storage: A survey." *Ieee Access* 8 (2020): 131723-131740.
9. Sahi, Aqeel, David Lai, and Yan Li. "A Review of the State of the Art in Privacy and Security in the eHealth Cloud." *Ieee Access* 9 (2021): 104127-104141.
10. Hua Deng, Zheng Qin, Qianhong Wu, Zhenyu Guan, and Yunya Zhou. 2020. Flexible attribute-based proxy re-encryption for efficient data sharing. Inf. Sci. 511, C (Feb 2020), 94–113. https://doi.org/10.1016/j.ins.2019.09.052.
11. Q. Zhang, Y. Fu, J. Cui, D. He and H. Zhong, "Efficient Fine-Grained Data Sharing Based on Proxy Re-Encryption in IIoT" in IEEE Transactions on Dependable and Secure Computing, vol. 21, no. 06, pp. 5797-5809, Nov.-Dec. 2024, doi: 10.1109/TDSC.2024.3386690.
12. Feng, T.; Wang, D.; Gong, R. A Blockchain-Based Efficient and Verifiable Attribute-Based Proxy Re-Encryption Cloud Sharing Scheme. *Information* **2023**, *14*, 281. https://doi.org/10.3390/info14050281.
13. K. Zhang, Y. Zhang, Y. Li, X. Liu, and L. Lu, “A blockchain-based anonymous attribute-based searchable encryption scheme for data sharing,” IEEE Internet Things J., vol. 11, no. 1, pp. 1685–1687, 2024.
14. H. Wang, J. Ning, X. Huang, G. Wei, G. S. Poh, and X. Liu, “Secure fine-grained encrypted keyword search for e-healthcare cloud,” IEEE Trans. Dependable Secur. Comput., vol. 18, no. 3, pp. 1307–1319, 2021.
15. J. Liu, J. Qin, W. Wang, L. Mei, and H. Wang, “Key-aggregate based access control encryption for flexible cloud data sharing,” Comput. Standards Interfaces, vol. 88, 2024, Art. no. 103800.

16. F. Luo, H. Wang, X. Yan and J. Wu, "Key-Policy Attribute-Based Encryption With Switchable Attributes for Fine-Grained Access Control of Encrypted Data," in *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 7245-7258, 2024, doi: 10.1109/TIFS.2024.3432279
17. O. Ahmed, C. Gouert and N. Georgios Tsoutsos, "PEEV: Parse Encrypt Execute Verify—A Verifiable FHE Framework," in *IEEE Access*, vol. 12, pp. 94673-94689, 2024, doi: 10.1109/ACCESS.2024.3424420.