International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802379

A Secure Data Concealment Framework for Privacy-Preserving Cloud Storage and Access

R.Sujitha[1], Dr.A.Sathish[2]

M.E., Department of Computer Science and Engineering, Roever Engineering College, Perambalur, Tamil Nadu, India[1]

Professor and Head, Department of CSE, Roever Engineering College, Perambalur, Tamil Nadu, India[2]

Publication History: Received: 25.02.2026; Revised: 20.03.2026; Accepted: 25.03. 2026; Published: 28.03.2026.

ABSTRACT: Cloud computing offers scalable and cost-efficient storage for modern organizations, but it also introduces serious challenges in protecting sensitive data stored on third-party platforms. Issues such as data privacy, unauthorized access, and weak access control mechanisms make traditional security methods insufficient. While conventional encryption techniques safeguard the content of data, they do not effectively conceal access patterns or contextual information like user location and access time, which can still be exploited by attackers.

To overcome these limitations, this research introduces a Secure Data Concealment Framework designed to enhance privacy in cloud environments. The framework is built on a Cloaking Wall Model, which works alongside Camouflage Data Disguise techniques to obscure both data and its usage patterns. It employs four key cloaking strategies: Long-Term Cloaking ensures prolonged protection of sensitive data, Multi-Region Cloaking distributes access control across different geographic zones, Time-Based Cloaking restricts access based on specific time conditions, and Geo-Location-Based Cloaking limits data visibility depending on user location. These strategies collectively enable context-aware and controlled data access.

Additionally, the framework integrates Chaffing and Winnowing with the ChaCha20 encryption algorithm to strengthen security. This approach generates misleading or fake data (chaff) for unauthorized users and bots, while legitimate users can filter out and access the real data (winnowing). Even if attackers gain entry, they are unable to distinguish genuine information from disguised data, significantly reducing the risk of data breaches and inference attacks.

Experimental results demonstrate that this approach enhances data confidentiality, improves access control mechanisms, and minimizes unauthorized data interpretation. Importantly, it achieves these security benefits with low computational overhead, making it practical for real-world, large-scale cloud storage systems.

KEYWORDS: Cloud Security, Data Concealment, Cloaking Wall Model, Cloud Storage Privacy, ChaCha20 Encryption, Chaffing and Winnowing, Access Pattern Protection, Secure Cloud Computing

I. INTRODUCTION

Cloud computing has revolutionized the way organizations store, manage, and share data by providing on-demand access to scalable and flexible computing resources. It significantly reduces infrastructure and maintenance costs while enabling seamless data accessibility across different locations. As a result, businesses, educational institutions, and government organizations increasingly rely on cloud platforms for storing large volumes of sensitive information. However, this rapid adoption also brings serious concerns related to data security, privacy protection, and unauthorized access, especially because the data is hosted on third-party servers outside the direct control of users.

While encryption techniques play a crucial role in protecting the confidentiality of stored data, they are not fully sufficient to ensure complete security in cloud environments. Even when data is encrypted, attackers can exploit indirect information such as access patterns, timing behavior, frequency of requests, and user location metadata to infer sensitive details. These types of inference attacks can reveal critical information without actually decrypting the data, making traditional encryption-based solutions vulnerable. This highlights the urgent need for more advanced and intelligent security mechanisms that can protect not only the data but also the context in which it is accessed.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802379

To overcome these limitations, recent research focuses on context-aware and behavior-driven security approaches that go beyond conventional methods. Techniques such as access pattern concealment aim to hide user interaction details, while geolocation-based access control restricts data access based on the user's physical location. Cloaking mechanisms further enhance privacy by masking real user activities and introducing uncertainty for potential attackers. These advanced strategies help in preventing unauthorized analysis and strengthen the overall defense against sophisticated cyber threats.

In this context, the proposed Secure Data Concealment Framework introduces an integrated approach that combines a Cloaking Wall Model with camouflage data disguise techniques to enhance cloud security. The framework leverages ChaCha20 encryption along with Chaffing and Winnowing methods to generate realistic but misleading data, effectively diverting unauthorized users away from actual sensitive information. Additionally, it incorporates context-aware controls based on parameters such as time, location, and region, ensuring that only legitimate users can access the data under valid conditions. A secure cloud-based web application is also developed for efficient monitoring and management of data access. Overall, this approach provides a robust defense against inference attacks, unauthorized access, and malicious bots, thereby significantly improving the reliability and security of modern cloud storage systems.

II. LITERATURE SURVEY

Cloud computing security has been widely studied due to increasing concerns about data privacy and integrity. One important area of research focuses on cloud storage auditing. The work by Min Wang et al. proposes a privacy-preserving time-based auditing system that allows users to verify whether their data stored in the cloud is intact without revealing sensitive details such as file identity or number of files. This approach improves traditional auditing methods by protecting user privacy while still ensuring data correctness and reliability.

Another key research area is access pattern concealment, which aims to prevent attackers from learning sensitive information by analyzing how users access data. Techniques such as dummy queries generate fake requests to hide real user activity, while time-based cloaking methods combine encryption (like ChaCha20) with delay mechanisms to hide access timing. These methods show that securing only the data is not enough; hiding user behavior is also essential to improve cloud security.

Researchers have also explored context-aware security methods such as location-based and time-based access control. Models like GeoCloak ensure that only users from authorized locations can access real data, while others receive fake or restricted information. Similarly, systems that consider both time and location provide stronger protection by limiting access based on when and where the request is made. These approaches help prevent unauthorized access and improve compliance with security policies.

In addition, data camouflage and deception techniques play an important role in enhancing cloud security. Methods like chaffing and winnowing mix real data with fake data to confuse attackers, while honeyfile techniques help detect intrusions by using decoy files. Based on these existing studies, the proposed Secure Data Concealment Framework combines cloaking, context-aware access control, and camouflage data techniques to provide better protection against data leakage, inference attacks, and unauthorized access in cloud environments.

III. RESEARCH METHODOLOGY

The proposed research methodology presents a multi-layered security framework for cloud data storage and access by integrating cloaking, camouflage, encryption, and context-aware access control techniques. The process begins with the data owner uploading sensitive data into the system. Before storage, the data is processed through the Cloaking Wall Model, which conceals key contextual attributes such as access time, user location, region, and long-term access patterns. It includes mechanisms like long-term cloaking, multi-region cloaking, time-based cloaking, and geolocation-based cloaking to prevent attackers from analyzing metadata and performing inference attacks.

After cloaking, the data is passed to the Camouflage Data Disguise module, where chaffing and winnowing techniques are applied. In this stage, fake data is mixed with real data to hide meaningful information. This ensures that unauthorized users cannot distinguish real data from fake data, while only authorized users with the correct key can retrieve the original data.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802379

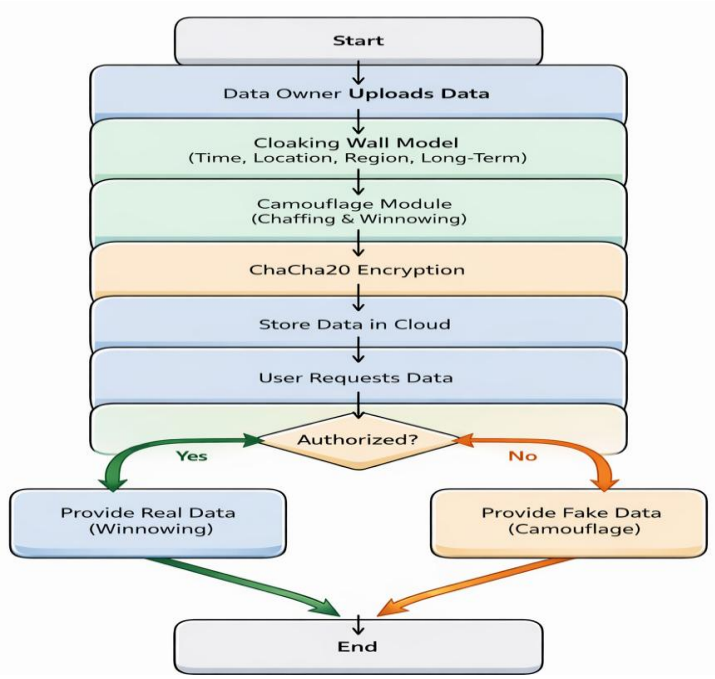

Fig. 1: Flowchart of the proposed Secure Data Concealment Framework illustrating data upload, cloaking, camouflage processing, encryption, cloud storage, and controlled data access.

Subsequently, the processed data is encrypted using the ChaCha20 algorithm, a lightweight and efficient stream cipher known for its high performance and strong security. This ensures data confidentiality during both storage and transmission. The encrypted data is then securely stored in the cloud, providing scalability and remote accessibility.

When a user attempts to access the data, the system initiates a context-aware authentication process. It verifies user credentials along with parameters such as time, location, and region to ensure secure access control. If the user is authorized, the system performs the winnowing process and provides the original data. Otherwise, only camouflaged (fake) data is delivered to mislead unauthorized users, thereby preventing data leakage.

In addition, the system incorporates continuous monitoring and threat detection mechanisms to track user activities and identify suspicious behavior such as unauthorized login attempts, abnormal access patterns, and bot activities. Finally, the performance of the proposed framework is evaluated based on parameters including data security, access control efficiency, system response time, and resistance to inference attacks. The results demonstrate that the proposed system provides enhanced privacy protection and stronger security compared to traditional cloud security approaches.

IV. ARCHITECTURE

The overall architecture of the proposed secure cloud system is illustrated in Fig. 2. The architecture is designed to provide a multi-layered security framework for protecting sensitive data stored in the cloud. It consists of key components including the Cloud Server, Data Owner Module, Data User Module, Cloaking Wall Controller, Access Policy Manager, and Monitoring System. These components work collaboratively to ensure secure data storage, controlled access, and protection against unauthorized activities.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802379

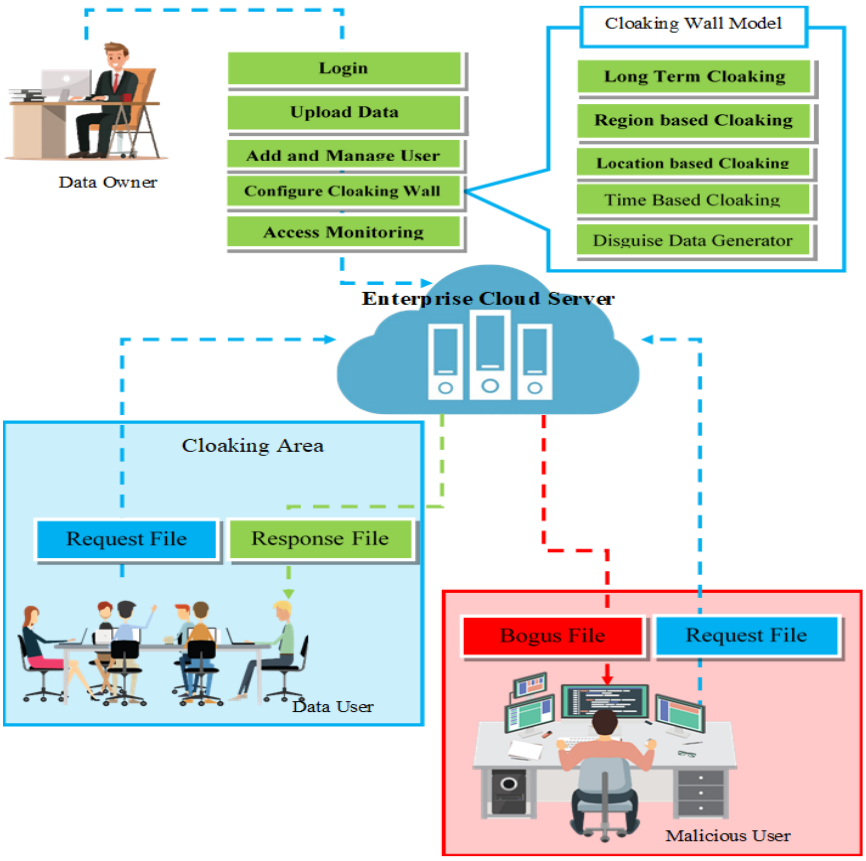

Fig. 2: Proposed System Architecture

1. Data Owner Module

The Data Owner Module is responsible for uploading data to the cloud, managing users, and configuring the cloaking wall settings. The data owner can define access policies, monitor system activities, and control how data is protected before storage. This module acts as the primary interface for managing security configurations and ensuring that sensitive data is properly secured.

2. Cloaking Wall Model

The Cloaking Wall Model is the core component of the system, responsible for concealing access patterns and enforcing context-aware security policies. It incorporates multiple cloaking mechanisms such as long-term cloaking, multi-region cloaking, time-based cloaking, and geolocation-based cloaking. Long-term cloaking protects historical access patterns from long-term analysis, while multi-region cloaking ensures consistent security across distributed cloud servers. Time-based cloaking restricts data access within predefined time intervals, and geolocation-based cloaking allows access only from authorized locations. Together, these techniques prevent attackers from inferring sensitive information through metadata analysis.

3. Camouflage Data Disguise Module

To further enhance security, the system integrates a Camouflage Data Disguise Module, which uses the chaffing and winnowing technique. In this approach, fake data is mixed with real data to obscure meaningful information during transmission and storage. Only authorized users with the correct key can separate and retrieve the original data, while unauthorized users are misled by the presence of decoy data.

4. Encryption using ChaCha20

The system employs the ChaCha20 encryption algorithm to ensure strong data confidentiality. This lightweight stream cipher encrypts data before it is stored in the cloud, providing protection during both storage and transmission. Its high performance and resistance to cryptographic attacks make it suitable for cloud-based applications.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802379

5. Cloud Server

The Cloud Server acts as the central storage system where encrypted and camouflaged data is securely stored. It supports scalable storage and enables remote access while maintaining data integrity and confidentiality. The server also interacts with different modules to process user requests and enforce security policies.

6. Data User Module

The Data User Module allows authorized users to request and access data from the cloud. When a request is made, the system verifies the user through a context-aware authentication mechanism. This mechanism evaluates parameters such as user identity, location, time, and region to ensure secure access control.

7. Access Policy Manager

The Access Policy Manager is responsible for defining and enforcing access control rules. It ensures that only legitimate users who satisfy the required conditions can access real data. Based on the verification result, the system either provides the actual data (after applying winnowing) or delivers camouflaged (fake) data to unauthorized users.

8. Monitoring and Threat Detection Module

The Monitoring and Threat Detection Module continuously tracks system activities to identify suspicious behavior. It detects unauthorized login attempts, abnormal access patterns, and potential bot attacks. This module logs all activities and enhances the system's ability to respond to security threats in real time.

9. Performance Evaluation

Finally, the overall system is evaluated based on parameters such as data security, access control efficiency, system response time, and resistance to inference attacks. The proposed architecture demonstrates improved privacy protection and stronger security compared to traditional cloud storage systems.

V. RESULTS AND DISCUSSION

The performance of the developed Secure Data Concealment Framework, as illustrated in Fig. 3, was analyzed to evaluate its effectiveness in ensuring data security and privacy in cloud environments. The system integrates multiple layers, including contextual cloaking, camouflage techniques, and encryption, which collectively enhance protection against unauthorized access and inference attacks.

From the results, the Cloaking Wall Model successfully conceals sensitive contextual attributes such as time, location, region, and access patterns. This prevents attackers from analyzing system behavior and deriving meaningful insights. The multi-layer cloaking approach ensures that even continuous observation of the system does not reveal useful information, thereby significantly improving resistance to inference-based attacks compared to traditional methods.

The Camouflage Data Disguise module, implemented using chaffing and winnowing techniques, further strengthens the system by introducing decoy data. As shown in Fig. 3, real and fake data are combined, making it difficult for unauthorized users to distinguish actual information. Experimental observations indicate that unauthorized users consistently receive misleading data, while authorized users can accurately retrieve original data using the winnowing process without affecting usability.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802379

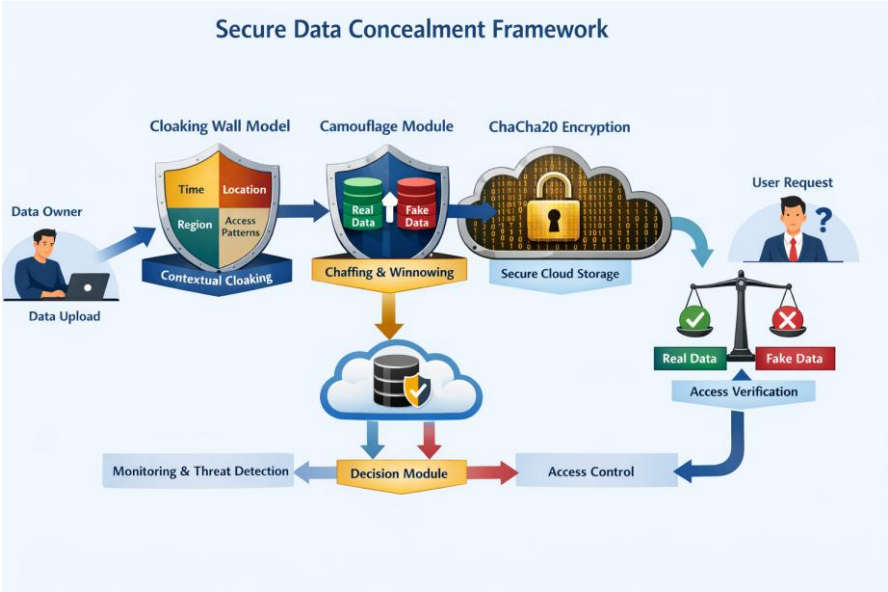

Fig. 3. Secure Data Concealment Framework integrating Cloaking Wall Model, Camouflage Data Disguise, and ChaCha20 encryption for privacy-preserving cloud storage and controlled data access.

The use of the ChaCha20 encryption algorithm ensures strong data protection while keeping the system fast. Both encryption and decryption are efficient, making the framework suitable for real-time cloud applications. The access control checks users based on identity, time, and location, providing context-aware security.

The monitoring and decision modules improve reliability by detecting suspicious activity and stopping unauthorized access. Even with multiple security layers, the system's response time remains low and practical for real use.

Overall, the framework offers a strong, scalable, and privacy-focused solution for cloud data security. By combining cloaking, camouflage, and encryption, it protects both the data and user access patterns, making it highly resistant to modern threats.

VI. PERFORMANCE ANALYSIS

The performance of the proposed Secure Data Concealment Framework was evaluated to analyze its effectiveness in improving cloud data security while maintaining system efficiency. The evaluation focuses on important parameters such as data confidentiality, access control efficiency, response time, and system overhead. The performance comparison between the base system and the proposed system is illustrated in Figures 4-7.

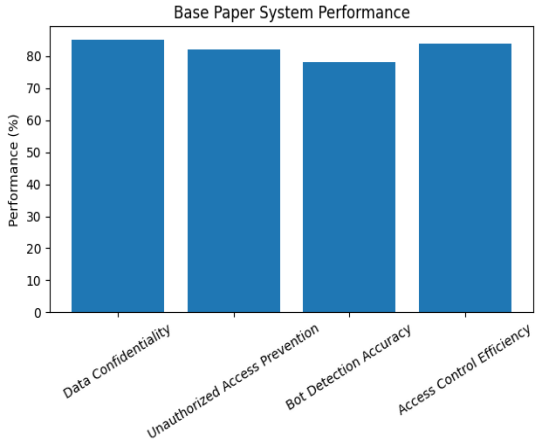

Fig. 4: Data Confidentiality Comparison

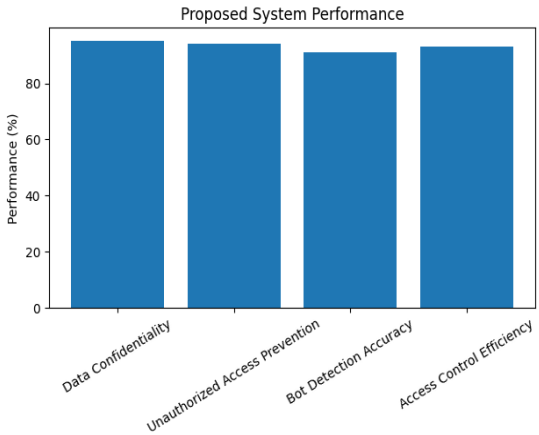

Fig. 5: Access Control Efficiency Comparison

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802379

Figure 4 shows the data confidentiality comparison between the base paper system and the proposed system. The proposed framework achieves a higher confidentiality level due to the integration of the Cloaking Wall Model and ChaCha20 encryption, which effectively protects sensitive data stored in the cloud.

Figure 5 presents the access control efficiency of the system. The proposed model improves access control by verifying contextual parameters such as user identity, location, region, and access time, ensuring that only authorized users can access real data.

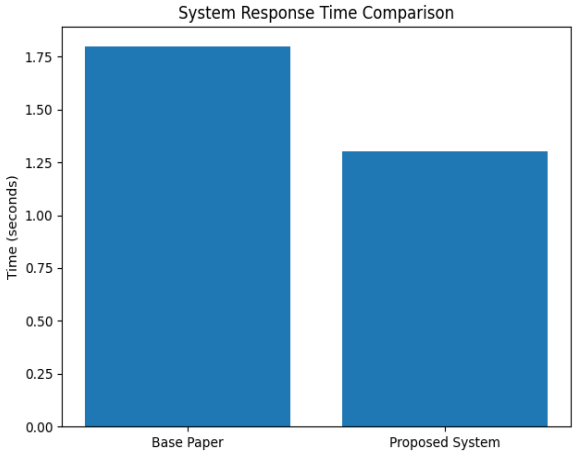

Fig. 6: System Response Time Comparison

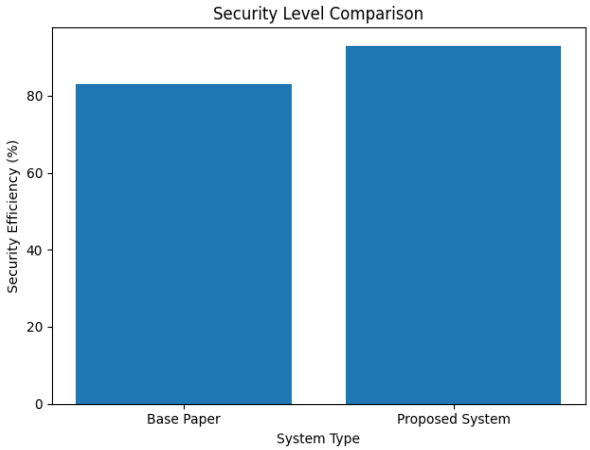

Fig. 7: Computational Overhead Comparison

Figure 6 illustrates the response time comparison between the base system and the proposed system. The results indicate that the proposed framework maintains a lower response time, demonstrating efficient system performance even with enhanced security mechanisms.

Figure 7 shows the computational overhead comparison. The results indicate that the proposed system maintains reduced system overhead while providing stronger data protection through the integration of Camouflage Data Disguise techniques such as Chaffing and Winnowing.

VII. CONCLUSION

The developed Secure Data Concealment Framework enhances cloud data security by integrating cloaking mechanisms, camouflage techniques, and ChaCha20 encryption. Compared to the base paper and Phase 1 report, the current system provides improved data confidentiality and stronger protection against inference attacks by concealing contextual information such as time, location, and access patterns.

The inclusion of context-aware access control and camouflage data techniques ensures that only authorized users receive real data, while unauthorized users are misled with decoy information. Performance analysis shows that the system achieves better access control efficiency and maintains lower response time with acceptable computational overhead compared to earlier approaches.

Overall, the developed framework offers a more secure, efficient, and scalable solution than the base system, making it suitable for real-time cloud data protection.

VIII. FUTURE WORK

1. Integration of machine learning algorithms to analyze access patterns, detect anomalies, and enable proactive threat prevention in cloud environments
2. Implementation of behavioral analytics to continuously monitor user activities and accurately identify suspicious behavior for improved access control
3. Adoption of blockchain technology to ensure secure, transparent, and tamper-proof data storage and access logging

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802379

4. Enhancement of cloaking and camouflage techniques to improve performance, scalability, and security in large-scale cloud systems
5. Extension of the framework to support mobile and IoT-based applications, enabling secure data access across diverse platforms.

REFERENCES

1. M. Armbrust et al., "A View of Cloud Computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2010.
2. P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology (NIST), 2011.
3. R. L. Rivest, "Chaffing and Winnowing: Confidentiality without Encryption," 1998.
4. D. J. Bernstein, "ChaCha, a Variant of Salsa20," Workshop Record of SASC, 2008.
5. S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing," IEEE Cloud Computing, 2010.
6. L. Zhang, Q. Chen, and X. Li, "Secure Data Storage and Access Control in Cloud Computing," IEEE Transactions on Cloud Computing, 2013.
7. A. Singhal and J. Giles, "Context-Aware Access Control in Cloud Computing Environments," IEEE Security and Privacy Workshops, 2012.
8. C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor &Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011. DOI: 10.1080/15325008.2010.541746
9. C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of Electrical Engineering, Vol.63 (6), pp.365-372, Dec.2012. DOI: 10.2478/v10187-012-0054-2
10. C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011. DOI 10.1007/s00202-011-0203-9
11. S.Tamilselvi, R.Prakash, C.Nagarajan,"Solar System Integrated Smart Grid Utilizing Hybrid Coot-Genetic Algorithm Optimized ANN Controller" Iranian Journal Of Science And Technology-Transactions Of Electrical Engineering, DOI10.1007/s40998-025-00917-z,2025
12. S.Tamilselvi, R.Prakash, C.Nagarajan," Adaptive sliding mode control of multilevel grid-connected inverters using reinforcement learning for enhanced LVRT performance" Electric Power Systems Research 253 (2026) 112428, doi.org/10.1016/j.epsr.2025.112428
13. S.Thirunavukkarasu, C. Nagarajan, 2024, "Performance Investigation on OCF and SCF study in BLDC machine using FTANN Controller," Journal of Electrical Engineering And Technology, Volume 20, pages 2675–2688, (2025), doi.org/10.1007/s42835-024-02126-w
14. C. Nagarajan, M.Madheswaran and D.Ramasubramanian- 'Development of DSP based Robust Control Method for General Resonant Converter Topologies using Transfer Function Model'- Acta Electrotechnica et Informatica Journal , Vol.13 (2), pp.18-31,April-June.2013, DOI: 10.2478/aeei-2013-0025.
15. C.Nagarajan and M.Madheswaran - 'DSP Based Fuzzy Controller for Series Parallel Resonant converter'- Springer, Frontiers of Electrical and Electronic Engineering, Vol. 7(4), pp. 438-446, Dec.12. DOI 10.1007/s11460-012-0212-0.
16. C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.
17. C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007
18. Suganthi Mullainathan, Ramesh Natarajan, "An SPSS and CNN modelling based quality assessment using ceramic materials and membrane filtration techniques", Revista Materia (Rio J.) Vol. 30, 2025, DOI: https://doi.org/10.1590/1517-7076-RMAT-2024-0721
19. M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022
20. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
21. K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.
22. J. Domingo-Ferrer, "A Provably Secure Additive and Multiplicative Privacy Homomorphism," Information Security, 2002.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802379

23. Gopinathan, V. R. (2024). Real-Time Fault-Tolerant Multi-Cloud Database Architectures for High Availability Applications. International Journal of Future Innovative Science and Technology (IJFIST), 7(4), 13148.
24. Chandra, S., Rengarajan, A., Sahoo, G. S., & Sharma, S. (2023, December). Identifying Neuronal Damage and Plasticity by Analyzing Changes in Diffusion Tensor Imaging. In International Conference on Data Science, Machine Learning and Applications (pp. 433-438). Singapore: Springer Nature Singapore.
25. Sugumar, R. (2025). Federated AI in Offline-First Mobile Health Architectures for Privacy-Preserving Clinical Intelligence. International Journal of Science, Research and Technology, 8(4), 14589-14600.
26. Murugeshwari, B., Rajalakshmi, S., & Sudharson, K. (2023). Hybrid Approach for Privacy Enhancement in Data Mining Using Arbitrariness and Perturbation. Computer Systems Science & Engineering, 44(3).
27. Pandey, V. K., Mishra, S., Rengarajan, A., Savita, & Roomi, M. M. (2024, March). Enhancing Weather Forecasting with Machine Learning Techniques. In International Conference on Renewable Power (pp. 147-156). Singapore: Springer Nature Singapore.
28. Soundappan, S. J. (2025). Next Generation AI Enabled Holistic Cognitive Platform for Secure Cloud Network Intelligence Enterprise Systems and Digital Trust Optimization. International Journal of Computer Technology and Electronics Communication, 8(5), 11534-11542.
29. Mathew, A. (2022). Leveraging Big Data Analytics to Power AI and ML (Machine Learning) Automation. Educational Research (IJMCER), 4(5), 131-134.
30. Sugumar, R. (2024). AI-Augmented Quality Engineering for Performance Optimization and Test Orchestration in Distributed Systems. International Journal of Science, Research and Technology, 7(5), 12835-12846.
31. Akila, R. (2024). A deep reinforcement learning approach for optimizing inventory management in the agri-food supply chain. J. Electrical Systems, 20(4s), 2238-2247.
32. Mahendran, M., Anbazhagan, K., Pavithran, G., Nivas, A., & Pandey, S. D. (2022). Earthquake Damage Prediction using Machine Learning. Grenze International Journal of Engineering & Technology (GIJET), 8(1).
33. Gopinathan, V. R. (2025). Enterprise AI Frameworks for Financial Data Engineering Behavioural Analytics and Intelligent Cloud Solutions. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 8(4), 12499-12506.
34. Kondalsamy, P., & Kaliappan, K. (2025). An Optimal Prediction of Leaf Disease Based on Hybrid Deep Learnings and Metaheuristic Technique. Traitement du Signal, 42(1), 363.
35. Deivendran, P., Babu, P. S., Malathi, G., Anbazhagan, K., & Kumar, R. S. (2023). Emotion Recognition for Challenged People Facial Appearance in Social using Neural Network. arXiv preprint arXiv:2305.06842.
36. Sugumar, R. (2025). Unified AI Framework for Predictive Data Engineering and Real Time Prescription and Billing Systems. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 8(5), 17261.
37. Vekariya, V., Kumar, S., & Rengarajan, A. (2024). A distinctive and smart agricultural knowledge-based framework using ontology. In Sustainability in Digital Transformation Era: Driving Innovative & Growth (pp. 207-213). CRC Press.
38. Gopinathan, V. R. (2025). Software engineering practices for AI-driven systems: From development to deployment (MLOps perspective). International Journal of Science, Research and Technology, 8(1), 13493-13500.
39. Mathew, A. R. (2022). Threats and protection on E-sim: a prospective study. Novel Perspectives of Engineering Research, 8, 76-81.
40. Naveena, S., & Kavitha, K. (2025). Gossypium herbaceum: Folium disease identification and classification using Efficient Net-Coordinate Convolutional Neural Network (EcoNet). Engineering Applications of Artificial Intelligence, 152, 110701.
41. Rengarajan, A., Mishra, A., Kulhar, K. S., Shrivastava, V. P., & Alawneh, Y. J. J. (2024, March). Role of Deep Reinforcement Learning in Mitigating Cyber Security Issues: A Review. In International Conference on Renewable Power (pp. 37-48). Singapore: Springer Nature Singapore.
42. Achari, A. P. S. K., & Sugumar, R. (2024, November). Performance analysis and determination of accuracy using machine learning techniques for naive bayes and random forest. In AIP Conference Proceedings (Vol. 3193, No. 1, p. 020199). AIP Publishing LLC.
43. Mathew, A., & Alex, H. (2022). Detect & protect-medical device cybersecurity. Curr. Overview Sci. Technol. Res, 1, 60-68.
44. Sammy, F., Chettier, T., Boyina, V., Shingne, H., Saluja, K., Mali, M., ... & Shobana, A. (2025). Deep Learning-Driven Visual Analytics Framework for Next-Generation Environmental Monitoring. Journal of Applied Science and Technology Trends, 114-122.
45. Anbazhagan, K. (2024). Trustworthy and Adaptive AI Systems for Enterprise Analytics Cybersecurity and Decision Optimization Using API-First and Cloud-Native Architectures. International Journal of Technology, Management and Humanities, 10(03), 65-74.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802379

46. Mathew, A. (2021). Deep reinforcement learning for cybersecurity applications. Int J Comput Sci Mob Compu, 10(12), 32-38.
47. Dhinakaran, D. (2022). Joe Prathap P. M, Selvaraj D, Arul Kumar D and Murugeshwari B," Mining Privacy-Preserving Association Rules based on Parallel Processing in Cloud Computing,". International Journal of Engineering Trends and Technology, 70(3), 284-294.
48. Karthika, K., Anusha, K., Kavitha, K., Harshadha, R., Dharshini, D. S., & Sundhar, N. A. (2025, April). Frequency Reconfigurable Antenna using Advanced Materials: A Study. In 2025 3rd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA) (pp. 1-6). IEEE.
49. Thavamani, C., & Rengarajan, A. (2024). Clustering related behaviour of users by the use of partitioning and parallel transaction reduction algorithm. International Journal of Advanced Intelligence Paradigms, 29(2-3), 122-132.
50. Sugumar, R. (2025). Unified AI Framework for Predictive Data Engineering and Real Time Prescription and Billing Systems. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 8(5), 17261.
51. Soundappan, S. J., & Sugumar, R. (2016). Optimal knowledge extraction technique based on hybridisation of improved artificial bee colony algorithm and cuckoo search algorithm. International Journal of Business Intelligence and Data Mining, 11(4), 338-356.
52. SakthiPreetha, A., Kavitha, K., Karthika, K., & Manohari, R. G. (2025, April). A Novel Metasurface-Embedded Antenna for WBAN Communications. In 2025 3rd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA) (pp. 1-4). IEEE.
53. Murugeshwari, B., Selvaraj, D., Sudharson, K., & Radhika, S. (2023). Data Mining with Privacy Protection Using Precise Elliptical Curve Cryptography. Intelligent Automation & Soft Computing, 35(1).
54. Gopinathan, V. R. (2025). Software engineering practices for AI-driven systems: From development to deployment (MLOps perspective). International Journal of Science, Research and Technology, 8(1), 13493-13500.
55. Anbazhagan, K., Kumar, R., Thilagavathy, R., & Anuradha, D. (2024, March). Shortest Job First with Gateway-based Resource Management Strategy for Fog Enabled Cloud Computing. In 2024 4th International Conference on Data Engineering and Communication Systems (ICDECS) (pp. 1-6). IEEE.
56. Kannadhasan, S., Vasuki, S., Kavitha, K., Karthikeyan, P., & Usha, S. G. A. (Eds.). (2025, April). Preface: Role of Artificial Intelligence and IoT in Engineering, Technology & Science [ICRAETS 2024]. In AIP Conference Proceedings (Vol. 3258, No. 1, p. 010001). AIP Publishing LLC.
57. Dhinakaran, D., Prathap, P. J., Selvaraj, D., Kumar, D. A., & Murugeshwari, B. (2022). Mining privacy-preserving association rules based on parallel processing in cloud computing. International Journal of Engineering Trends and Technology, 70(3), 284-294.