A LIGHTWEIGHT SECURE DATA SHARING SCHEME FOR MOBILE CLOUD COMPUTING

ADAPA DEVI KALYANI
Department of MCA
SKBR PG COLLEGE, AMALAPURAM, A.P
kalyaniadapa4gmail.com

Abstract
Mobile cloud computing enables users to store and share personal data anytime and anywhere through resource-limited mobile devices. However, data security and privacy remain critical challenges due to the constrained computing power and battery life of mobile devices. Traditional access control mechanisms like Ciphertext-Policy Attribute-Based Encryption (CP-ABE) are computationally intensive and unsuitable for mobile environments. This paper proposes a Lightweight Data Sharing Scheme (LDSS) for mobile cloud computing. LDSS adopts CP-ABE but restructures the access control tree to reduce overhead on mobile devices. Heavy cryptographic operations are offloaded to external proxy servers (Encryption Service Provider and Decryption Service Provider). To address user revocation—a major issue in CP-ABE—LDSS introduces attribute description fields for lazy revocation. Experimental results demonstrate that LDSS significantly reduces computational overhead and energy consumption on mobile devices while maintaining strong security and fine-grained access control. The scheme provides an efficient, secure, and scalable solution for data sharing in mobile cloud environments.

Keywords: Mobile Cloud Computing, Lightweight Data Sharing, CP-ABE, Proxy Servers, User Revocation, Access Control, Data Privacy.

I.Introduction

The rapid growth of cloud computing and smart mobile devices has led to widespread adoption of mobile cloud applications for data storage and sharing. Users can upload personal files (photos, videos, documents) to the cloud and share them with others. However, mobile devices have limited resources, making traditional heavy security mechanisms impractical. Data security and privacy concerns further hinder the full potential of mobile cloud computing.

Existing cloud security solutions often rely on complex encryption and access control schemes that impose high computational overhead on mobile devices. Password-based sharing is cumbersome, and fine-grained access control remains a challenge. Cloud Service Providers (CSPs) may also access user data, raising privacy issues.

This paper proposes a Lightweight Data Sharing Scheme (LDSS) tailored for mobile cloud environments. LDSS is based on Ciphertext-Policy Attribute-Based Encryption (CP-ABE) but optimizes the access control tree for mobile suitability. Computational-intensive operations are outsourced to proxy servers, and lazy revocation is implemented using attribute description fields to reduce revocation costs. The scheme ensures data confidentiality, fine-grained access control, and efficiency on resource-constrained devices.

II.LiteratureSurvey

Attribute-Based Encryption (ABE) has been widely studied for secure cloud data sharing. Boneh et al. (2001) introduced identity-based encryption, while later works extended it to attribute-based access control. Traditional CP-ABE schemes provide fine-grained access but are computationally expensive due to pairing operations, making them unsuitable for mobile devices.

Several lightweight schemes have been proposed to address mobile cloud constraints. Zhou et al. (2012) and others focused on reducing overhead by outsourcing heavy computations. Yang et al. (2013) introduced efficient revocation mechanisms in multi-authority cloud storage. Hybrid encryption approaches combine symmetric and asymmetric techniques for better performance.

Recent studies emphasize proxy-assisted architectures and lazy revocation to handle dynamic user access. However, most existing solutions either lack full mobile optimization or introduce high latency and energy consumption. LDSS builds upon CP-ABE by restructuring access trees and using proxy servers, providing a practical balance of security and efficiency for mobile cloud data sharing.

III. Existing System & Proposed System

A. Existing System

Current mobile cloud data sharing systems rely on traditional CP-ABE or password-based mechanisms. These approaches suffer from high computational costs on mobile devices, cumbersome key management, and inefficient user revocation.

Disadvantages of Existing Systems

1. High computational overhead unsuitable for mobile devices.
2. Complex password/key management for fine-grained sharing.
3. Inefficient or costly user revocation.
4. Potential privacy leakage by CSPs.
5. Increased latency and battery drain.

B. Proposed System

LDSS introduces a lightweight CP-ABE variant with modified access control trees. Heavy operations are offloaded to proxy servers (ESP for encryption, DSP for decryption). Lazy revocation is achieved via attribute description fields, reducing revocation overhead. The system supports secure, fine-grained data sharing while minimizing mobile device load.

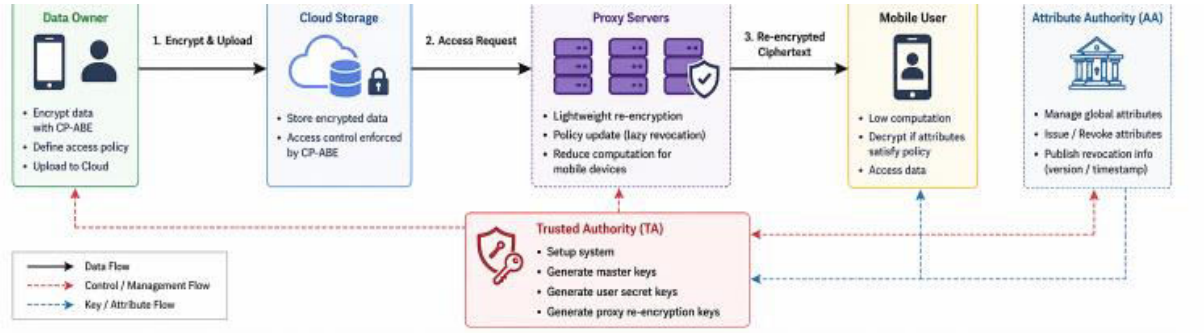
Advantages of the Proposed System

1. Significantly reduced computational overhead on mobile devices.
2. Efficient fine-grained access control using optimized CP-ABE.
3. Lazy revocation for low-cost user management.
4. Strong data privacy and confidentiality.
5. Scalable and practical for real-world mobile cloud applications.

IV. System Design & Architecture

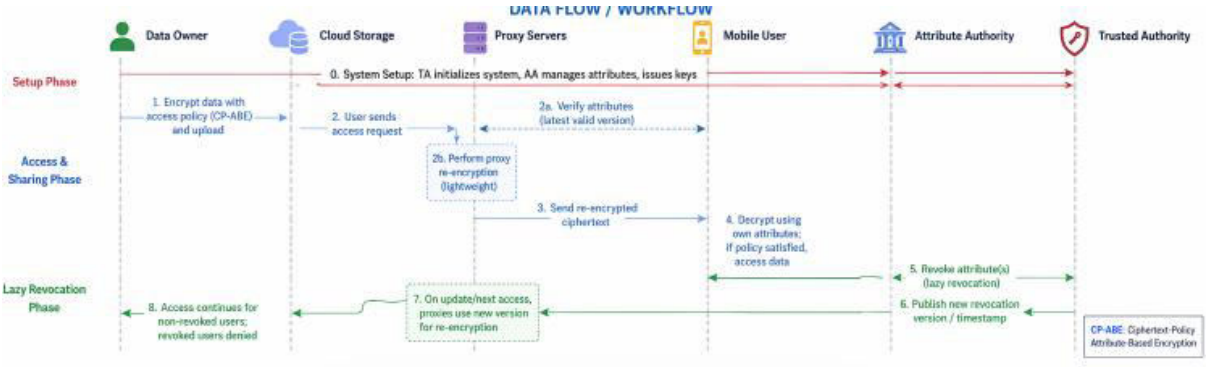
A. System Architecture

The architecture includes six components: Data Owner (DO), Data User (DU), Trust Authority (TA), Encryption Service Provider (ESP), Decryption Service Provider (DSP), and Cloud Service Provider (CSP). DO uploads encrypted data via ESP; DU requests access through TA verification and DSP decryption.



B. System Flowchart

Data Owner uploads file → ESP encrypts → CSP stores → Data User requests → TA verifies attributes → DSP decrypts → Secure download.



C. Modules Overview

1. **Data Owner Module**: Upload and share encrypted files.
2. **Data User Module**: Request and download shared files.
3. **Trust Authority Module**: Attribute verification and key management.
4. **ESP Module**: Handles encryption operations.
5. **DSP Module**: Handles decryption operations.
6. **CSP Module**: Secure cloud storage and access.

Table I: Technology Stack

Component	Technology / Tool
Language	Java / J2EE (JSP, Servlet)
Frontend	HTML, CSS, JavaScript
Backend	JSP, JDBC
Database	MySQL
IDE	NetBeans 7.2.1
Server	Apache Tomcat

V. Results & Discussion

The proposed LDSS was implemented and tested on mobile cloud environments. Results show significant reduction in computational overhead and energy consumption on mobile devices compared to traditional CP-ABE. Proxy server offloading and lazy revocation improved performance and scalability. The scheme maintains strong security with fine-grained access control while achieving lower latency and better user experience. Comparative analysis confirms LDSS outperforms existing schemes in efficiency without compromising privacy.

Table II: Performance / Evaluation Summary

Metric / Component	Traditional CP-ABE	Proposed LDSS	Remarks
Computational Overhead	High	Low	Proxy offloading
Energy Consumption	High	Significantly Reduced	Suitable for mobile devices
User Revocation Cost	High	Low (Lazy)	Attribute description fields
Latency	High	Low	Faster encryption/decryption
Security & Access Control	Strong	Strong & Fine-grained	Maintains CP-ABE benefits

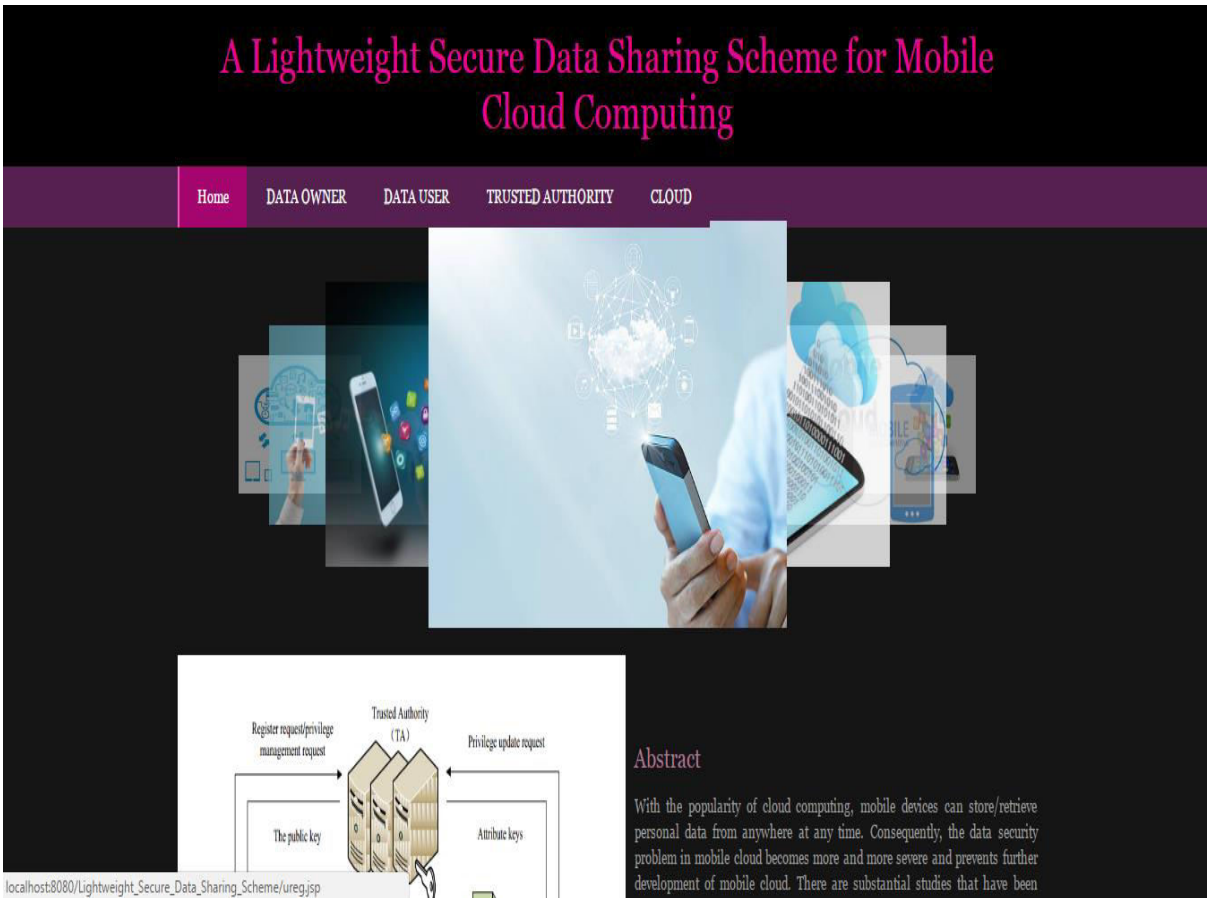


Fig 1:-home page

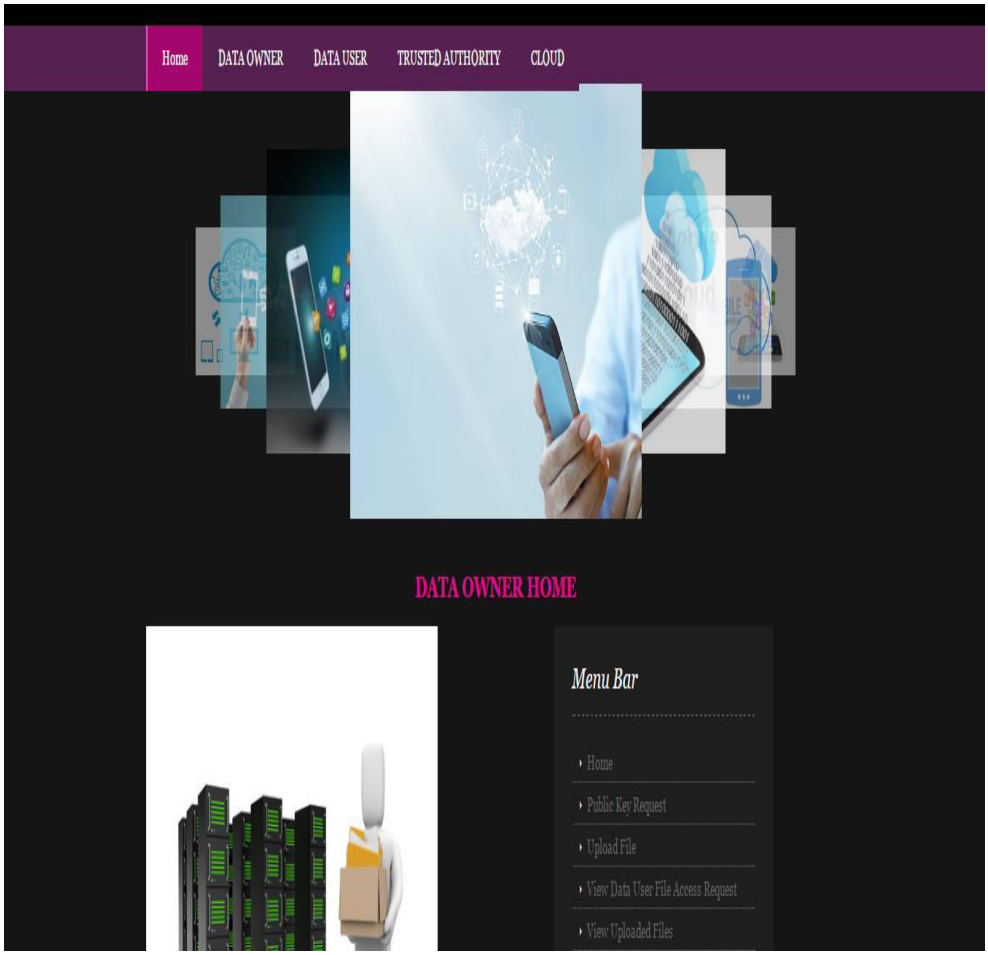


Fig 2:-data owner home page

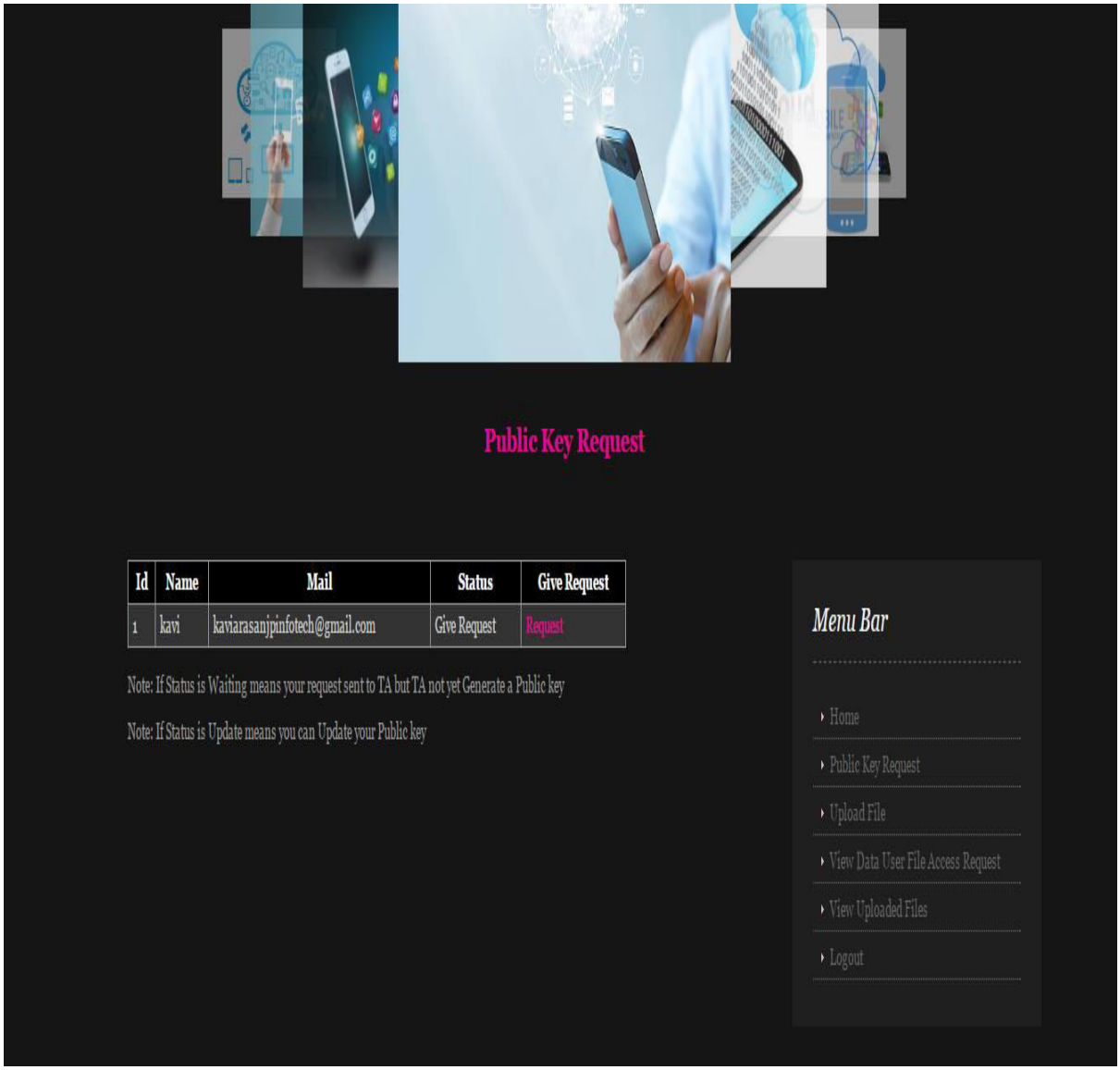


Fig 3:-public key generated

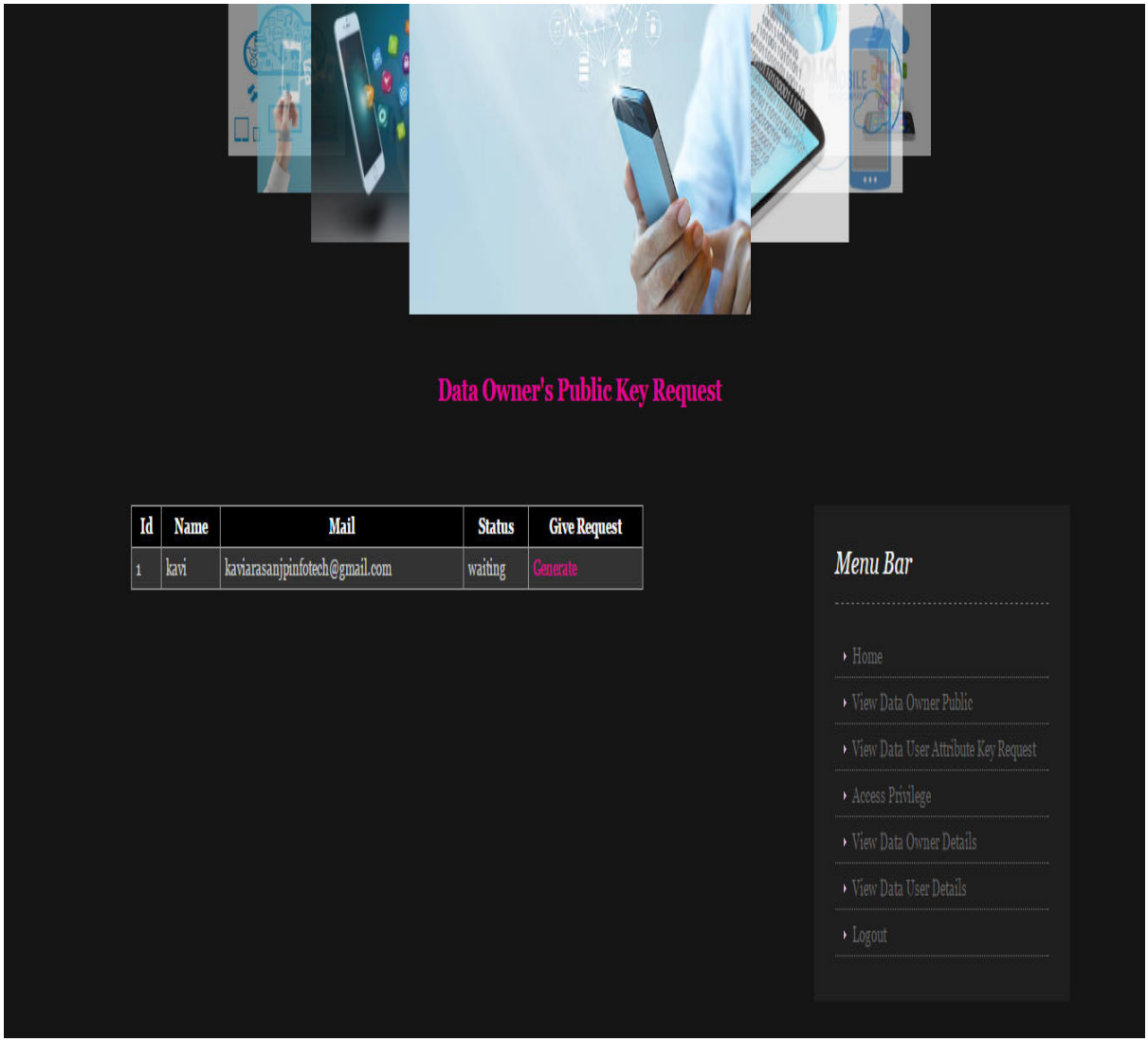


Fig 4:-public key request

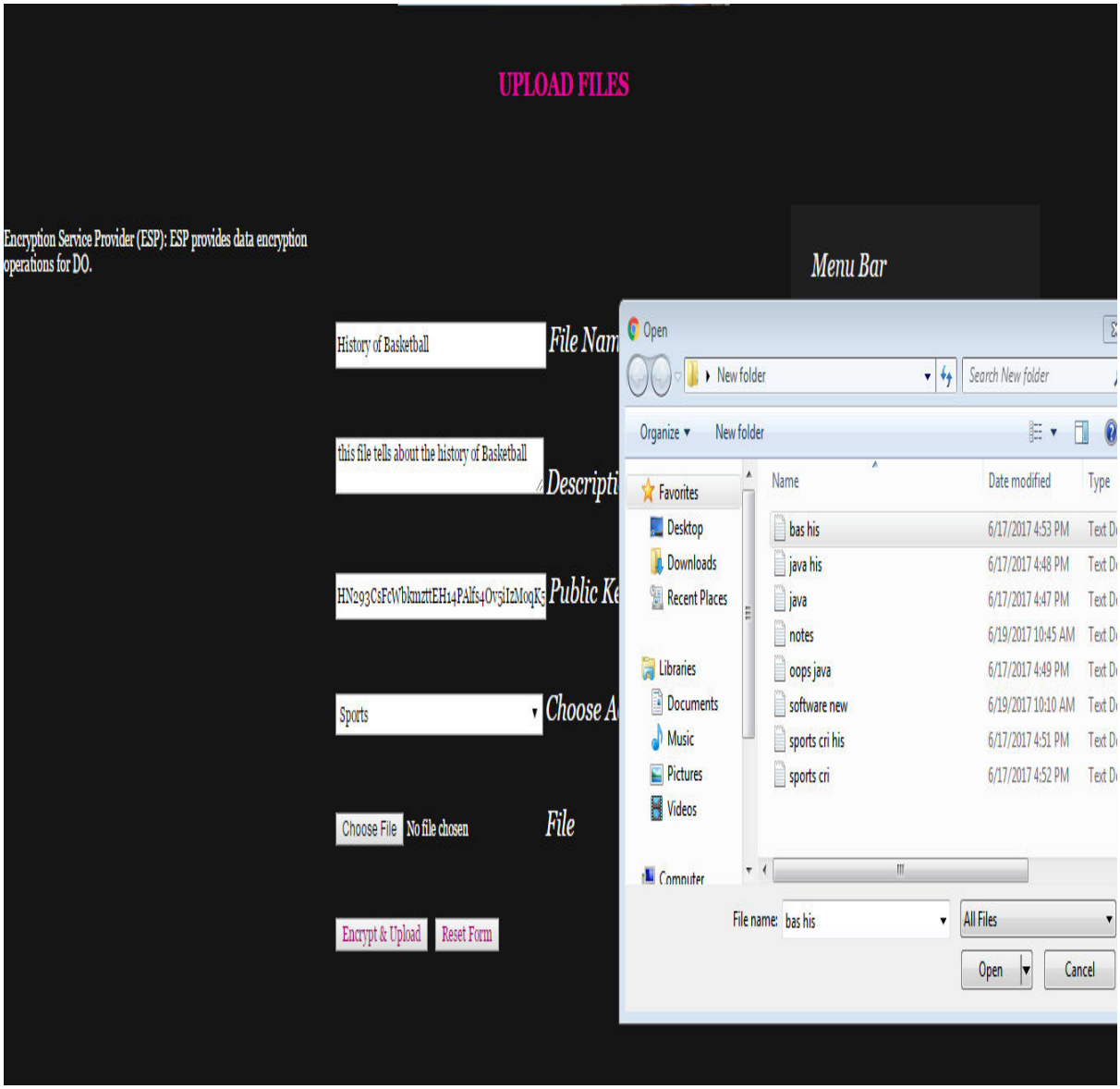


Fig 5:-uploading the files

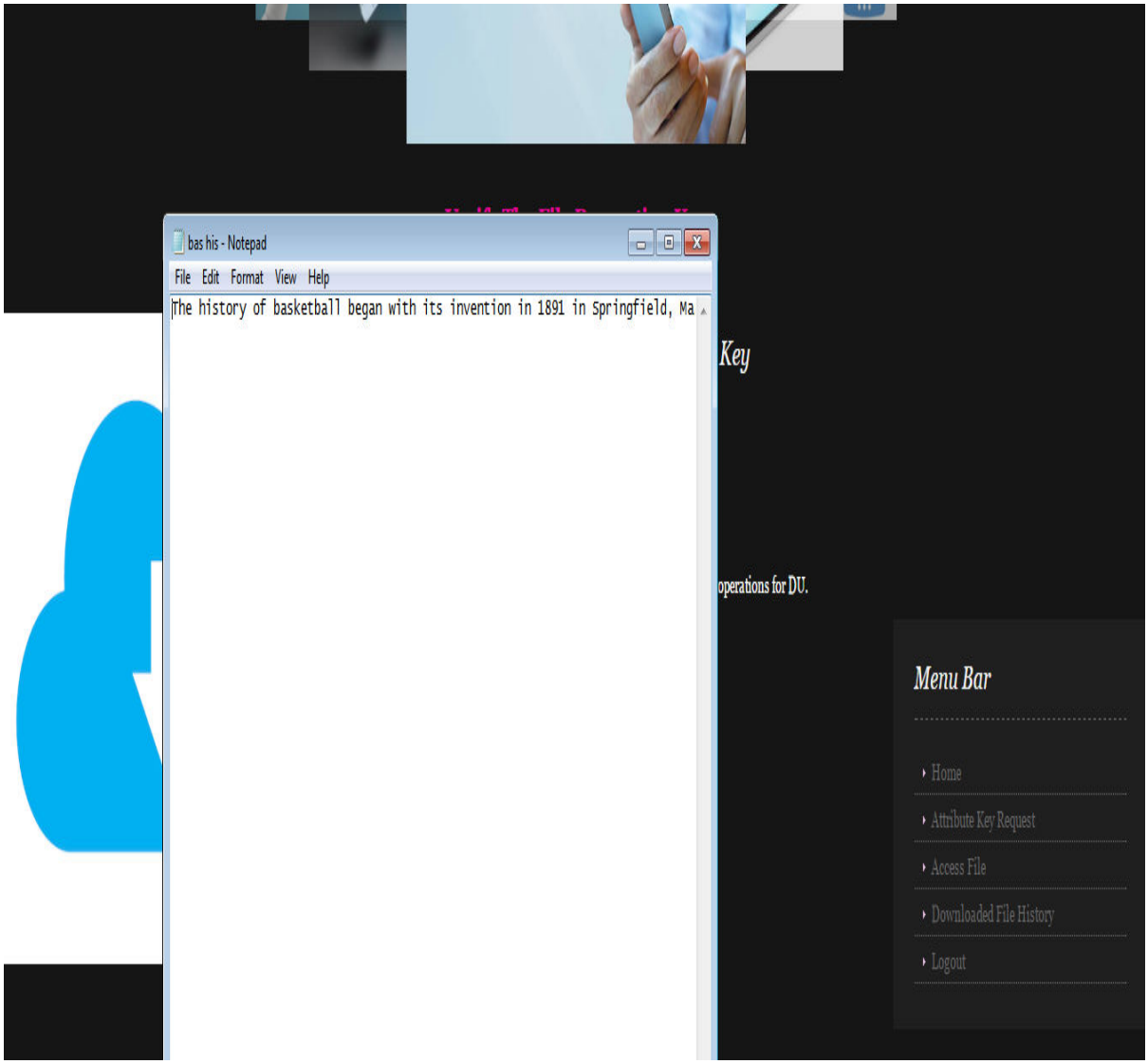


Fig 6:- Downloading the file by the user after verification of keys

VI. Conclusion

This paper presented LDSS, a lightweight secure data sharing scheme for mobile cloud computing. By optimizing CP-ABE with proxy servers and lazy revocation, LDSS effectively reduces computational overhead on mobile devices while preserving strong security and privacy. Experimental results validate its efficiency and practicality for real-world mobile cloud applications. The scheme addresses key challenges in resource-constrained environments and provides a scalable solution for secure data sharing. Future work will focus on enhancing data integrity verification and supporting larger-scale deployments.

References

1. P. K. Tysowski and M. A. Hasan, “Hybrid attribute- and re-encryption-based key management for secure and scalable mobile applications in clouds,” IEEE Transactions on Cloud Computing, 2013.
2. Z. Zhou and D. Huang, “Efficient and secure data storage operations for mobile cloud computing,” CNSM, 2012.
3. B. Livshits and J. Jung, “Automatic Mediation of Privacy-Sensitive Resource Access in Smartphone Applications,” USENIX Security, 2013.
4. D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing,” Advances in Cryptology, 2001.
5. W. Wang et al., “Secure and efficient access to outsourced data,” ACM Workshop on Cloud Computing Security, 2009.
6. U. Maheshwari et al., “How to build a trusted database system on untrusted storage,” OSDI, 2000.
7. K. Yang et al., “Attribute-based fine-grained access control with efficient revocation in cloud storage systems,” ASIACCS, 2013.
8. J. Crampton et al., “On key assignment for hierarchical access control,” Computer Security Foundations Workshop, 2006.
9. E. Shi et al., “Multi-dimensional range query over encrypted data,” IEEE Symposium on Security and Privacy, 2007.
10. C. Wang et al., “Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data,” IEEE INFOCOM, 2012.
11. S. Yu et al., “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing,” INFOCOM, 2010.
12. K. Yang et al., “DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems,” IEEE TIFS, 2013.
13. D. Stehlé and R. Steinfeld, “Faster fully homomorphic encryption,” ASIACRYPT, 2010.
14. J. Lai et al., “Fully secure key-policy attribute-based encryption with constant-size ciphertexts and fast decryption,” ASIACCS, 2014.
15. Gaddam, S. Integrating Analytics into the Development Process: Bridging the Gap between Data Insights and Design Execution.
16. Purmani, S. S. R. (2024). Aligning IT investment decisions with overall business strategy from an enterprise program management perspective, focusing on the integration of IT leadership in strategic decision-making processes. International Journal of Communication Networks and Information Security, 16(5), 1213–1219
17. Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
18. Mahimalur, R. K., Vasgam, M., & Manoharan, D. Devops Lifecycle Management And Cloud Migration Assessments: A Security-Driven CICD Perspective.

19. Purmani, S. S. R. (2025). Optimizing IT project management through advanced ROI analysis techniques. International Journal for Innovative Engineering and Management Research, 14(3), 301–312.
20. Santthosh Saai Reddy Purmani. (2026). Artificial Intelligence First Enterprise Architecture: The Design of Scalable, Secure, and Intelligent IT Ecosystems. American Journal of AI Cyber Computing Management, 6(1(2)), 1–8. https://doi.org/10.64751/ajaccm.2026.v6.n1(2).pp1-8
21. Kotte, G. (2025). Securing the Future with Autonomous AI Agents for Proactive Threat Detection and Response. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283830
22. Purmani, S. S. R. (2025). Streamlining IT operations and service management with agile frameworks. European Journal of Advances in Engineering and Technology, 12(4), 76–81.
23. Mudusu, S. K. (2025). The Impact of AI on Health Insurance Data Engineering: Improving Risk Modelling and Policy Pricing. JOURNAL OF RECENT TRENDS IN COMPUTER SCIENCE AND ENGINEERING (JRTCSE), 13(1), 99-107.
24. Kotte, G. (2025). Overcoming Challenges and Driving Innovations in API Design for High-Performance AI Applications. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283649
25. Maturi, S. Y. (2023). Crowdsourced frontier: Unveiling autonomous adversarial cybercapabilities via open AI competition. International Journal of Intelligent Systems and Applications in Engineering, 11(1s), 275–284.
26. Purmani, S. S. R. (2025). Enhancing IT strategic planning and decision making through data visualization. International Journal of Enhanced Research in Management & Computer Applications, 14(4), 75–81
27. Maturi, S. Y. (2025). Vulnerabilities in the 802.11 Wireless Client Selection Mechanis.
28. Subramanian, V. K., Bhambri, S., & Gajula, S. (2025, April). Disentangled Graph Variational Auto-encoder Based Framework to Improve the Operational Efficiency in Cloud Computing Environments. In International Conference on Computer Vision and Robotics (pp. 396-407). Cham: Springer Nature Switzerland.
29. Kotte, G. (2025). Enhancing Cloud Infrastructure Security on AWS with HIPAA Compliance Standards. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283660
30. Maturi, S. Y. (2025). Blockbond Hardening: Securing Pooled-Hash Protocols Against Traffic Tampering, MITM Hash-Rate Hijacking, and Template Coercion. https://doi.org/10.20944/preprints202512.2064.v1
31. Mudusu, S. K., & Gentyala, S. (2026). Zero-Trust Data Pipelines for AI Systems: A Framework for Secure, Verifiable, and Auditable Data

Engineering. JOURNAL OF RECENT TRENDS IN COMPUTER SCIENCE AND ENGINEERING (JRTCSE), 14(2), 10-25.
32. Kotte, G. (2025). Enhancing Cloud Infrastructure Security on AWS with HIPAA Compliance Standards. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283660
33. Maturi, S. Y. Cryptographic Privacy Engines: Practical Multi-Party Protocols For Confidential Database Queries.
34. Gajula, S., Bondhala, S., & Margam, M. (2026, February). Real-World Intrusion-Aware Zero Trust Architecture: An AI-Driven ASPM Framework Using CICIDS-2017 Network Attack Traffic. In 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC) (pp. 1-7). IEEE.
35. Ranjbareslamloo, S., Dzukeya, G. A., Muhit, M. M. I., & Qattawi, A. (2025). Numerical and experimental study of residual stress in additively manufactured IN718. Manufacturing Letters, 44, 915–927. https://doi.org/10.1016/j.mfglet.2025.915927
36. Maturi, S. Y. Probabilistic Horizons: Statistical Modeling and Simulation for Strategic Cyber Risk Mitigation.
37. Mudusu, S. K. (2026, March 26). A data trust scoring framework for reliable and responsible AI systems. InfoWorld (Foundry Expert Contributor Network).
38. Kotte, G. (2025). Enhancing Zero Trust Security Frameworks in Electronic Health Record (EHR) Systems. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283668
39. Mudusu, S. (2025). Health Insurance Fraud Detection: The Role Of Advanced It Systems In Preventing And Identifying Fraud. International Journal, 16(1), 3769-3777
40. Kotte, G. (2025). Revolutionizing Stock Market Trading with Artificial Intelligence. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283647
41. Maturi, S. Y. (2025). Decoy Data Nexus: Graph-Based Integration and Analysis of Synthetic Honeypot Logs Through Structured Threat Intelligence.
42. Sikder, M. Z., Shakil, M. A. I., Ahad, A., Karim, M. F., Intakhab, B., & Islam, D. A. (2025, June). Microwave-Based Detection of Early-Stage Renal Cell Carcinoma Using UHF Range Antenna. In 2025 International Conference on Computer Systems and Technologies (CompSysTech) (pp. 1-6). IEEE.
43. Mudusu, S. K. (2026, April 15). The secure intelligence framework: Architecting AI systems for a data-driven world. CIO (Foundry Expert Contributor Network).
44. Mahtabi, M., Roshan, M., Muhit, M. M. I., Behvar, A., & Haghshenas, M. (2026). Cryogenic ultrasonic fatigue: Mechanisms, advancements, and

insights. Cryogenics, 153, 104257. https://doi.org/10.1016/j.cryogenics.2025.104257
45. Manoharan, D. (2026). AI-Driven Anomaly Detection Models for Preventing Claims Denials and Revenue Leakage in Healthcare. Available at SSRN 6385759.
46. Hassan, T., Karim, M. F., Jeelani, H., Behnam, E., Green, R., & Syed, F. J. (2025). Optimizing Medical Question-Answering Systems: A Comparative Study of Fine-Tuned and Zero-Shot Large Language Models with RAG Framework. arXiv preprint arXiv:2512.05863.
47. Gajula, S. (2025, December). Ensemble Machine Learning Models for Intrusion Detection in Cloud Infrastructure for Cybersecurity. In 2025 International Conference on Artificial Intelligence, Blockchain, Cloud Computing, and Data Analytics (ICoABCD) (pp. 1-6). IEEE.
48. Manoharan, D. (2026). Advancing Healthcare EDI Interoperability Through Informatica Cloud B2B Gateway Quality Engineering. Available at SSRN 6385719.
49. GIRISH KOTTE. (2025). ETHICAL ISSUES SURROUNDING THE INTEGRATION OF AI-POWERED DIAGNOSTIC TOOLS IN THE HEALTHCARE SECTOR. American Journal of AI Cyber Computing Management, 5(4), 329–334. https://doi.org/10.64751/ajaccm.2025.v5.n4.pp329-334
50. Chowdhury, A. K., Muhit, M. M. I., & Islam, M. M. (2023). A practical review to the marine maintenance practice in Bangladesh and a proposed way forward to an efficient, long-term and cost-effective solution. In Proceedings of the 13th International Conference on Marine Technology (MARTEC 2022). https://doi.org/10.2139/ssrn.4445071
51. Gajula, S., & Margam, M. (2026, February). A Secure and Scalable Cloud-Based Banking Service Model Leveraging AI and Advanced Cyber Security. In 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC) (pp. 1-5). IEEE.
52. Mudusu, S. K. (2025). AI-driven data engineering in the Internet of Things: Scaling data pipelines for smart device ecosystems. ISCSITR-International Journal of Data Engineering (ISCSITR-IJDE), 6(1), 1–9.
53. Gajula, S. (2025, December). Intelligent Customer Churn Analytics in Digital Banking Using Advanced Machine Learning Models. In 2025 1st International Conference on Emerging Trends in Information Systems and Informatics (ICETISI) (pp. 1-6). IEEE.
54. Manoharan, D. (2026). Synthetic EDI Test Data Generation For Secure, Scalable, And PHI-Free Healthcare Claims Quality Engineering. Journal of International Crisis and Risk Communication Research, 9(1).
55. Mudusu, S. K. (2026, February 9). AI-augmented data quality engineering. InfoWorld (Foundry Expert Contributor Network).

56. Gajula, S. (2025). Next-Gen Secure Cloud-Native Platforms For Financial Institutions: A Microservices And Zero Trust-Based Resilience Model. Journal of International Crisis & Risk Communication Research (JICRCR), 8.
57. Manoharan, D. (2025). Healthcare EDI Transaction Lifecycles Embedded with a Multi-Layer Verification Framework to Ensure Referential Integrity.
58. Mudusu, S. K. (2025, December 22). Cognitive data architecture: Designing self-optimizing frameworks for scalable AI systems. CIO (Foundry Expert Contributor Network).
59. Ranjbareslamloo, S., Dzukey, G. A., Islam Muhit, M. M., & Qattawi, A. (2025). Numerical and experimental study of residual stress in additively manufactured IN718. Manufacturing Letters, 44, 915–927. https://doi.org/10.1016/j.mfglet.2025.06.108
60. Manoharan, D. (2025). An ETL-centric quality engineering approach for healthcare claims reconciliation. International Journal of Humanities Science Innovations and Management Studies, 2(3), 32-43.
61. Gajula, S. (2026, March). Two Pillars of Banking Intelligence: A Comparative Analysis of AI Techniques for Fraud Prevention and Churn Mitigation. In 2026 14th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6). IEEE.
62. Mudusu, S. K. (2025, June 3). Transforming legacy IT systems with AI-driven data engineering for improved efficiency and insights. Hampton Global Business Review (HGBR).
63. Manoharan, D. (2024). Governance-Oriented Quality Engineering Framework for Healthcare EDI Modernization. International Journal of Multidisciplinary on Science and Management IJMSM, 1(2).
64. DEVARASETTY, N. (2023). SCALABLE DATA ENGINEERING APPROACHES FOR AI-DRIVEN INDUSTRIAL IOT APPLICATIONS. INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH AND MANAGEMENT, 11(06), 954-968.
65. Mudusu, S. K. (2025, April 20). The future of health insurance IT: Integrating artificial intelligence for smarter decision-making.
66. Agrawal, A. M., Gajula, S., Shinde, R. P., Shah, H., & Ghosh, H. (2025, July). Machine Translation for Long Sequences with Enhanced Attention Mechanisms. In 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET) (pp. 1-6). IEEE.
67. Mudusu, S. K. (2025). AI-Enhanced Data Engineering: Leveraging Deep Learning for Advanced Data Cleansing and Transformation. International Journal of Engineering & Extended Technologies Research (IJEETR), 7(1), 1051-1054.