

Portable Blind Cloud Storage System for Secure Multi-Device Data Access Using AI-Based Threat Detection

Aishwarya B Nateekar¹, Aishwarya s², K P Usha³, Bhoomika M Y⁴, Prof. Deepti⁵

¹Department of Computer Science and Engineering & RGIT

²Department of Computer Science and Engineering & RGIT

³Department of Computer Science and Engineering & RGIT

⁴Department of Computer Science and Engineering & RGIT

⁵Department of Computer Science and Engineering & RGIT

Abstract – Cloud computing has become a widely adopted technology for storing and managing large-scale digital data. However, conventional cloud storage systems face significant challenges related to data privacy, unauthorized access, insider threats, and lack of intelligent security monitoring. Users often have limited control over their data once it is uploaded to cloud servers, leading to potential security and trust issues.

*This paper proposes a **Portable Blind Cloud Storage System for Secure Multi-Device Data Access** integrated with **Artificial Intelligence-based threat detection**. The system ensures data privacy by implementing client-side encryption using advanced cryptographic techniques such as AES and RSA, preventing cloud providers from accessing original user data. A blind storage architecture is adopted where only encrypted data is stored in the cloud.*

Additionally, the system incorporates AI and machine learning algorithms to monitor user behaviour and detect anomalies such as unauthorized login attempts and suspicious access patterns. This enhances real-time security and proactive threat prevention. The proposed system also supports secure multi-device synchronization, enabling users to access data safely across different devices.

Overall, the system improves data confidentiality, integrity, scalability, and intelligent security management, making it suitable for modern cloud environments and future AI-driven secure storage applications.

Key Words: Cloud Computing, Blind Cloud Storage, Data Security, Multi-Device Access, Artificial Intelligence, Machine Learning, AES Encryption, RSA Algorithm, Cybersecurity, Anomaly Detection, Data Privacy, Secure Authentication.

I. Introduction

Cloud computing has emerged as one of the most important technologies for storing, processing, and managing large volumes of data in modern digital systems. It provides users with scalable storage, remote accessibility, and cost-effective data management solutions. Due to these advantages, cloud services are widely used in personal, academic, and industrial applications.

Despite its benefits, cloud computing introduces several security and privacy concerns. When users upload data to cloud servers, they often lose direct control over their information. This creates risks such as unauthorized access, data breaches, insider attacks, and misuse of sensitive information by cloud service providers or external attackers. In addition, traditional cloud systems lack intelligent monitoring mechanisms to detect abnormal or malicious user activities in real time.

Another major challenge is ensuring secure and seamless multi-device access. Users today access cloud data from multiple devices such as smartphones, laptops, and tablets, which increases the attack surface and security vulnerabilities. Maintaining consistent security across all devices while ensuring data integrity and confidentiality remains a significant issue.

To address these challenges, this paper proposes a **Portable Blind Cloud Storage System for Secure Multi-Device Data Access** integrated with **Artificial Intelligence-based threat detection**. The proposed system focuses on protecting user data through client-side encryption, ensuring that cloud providers cannot access raw data. It also incorporates AI-based anomaly detection to monitor user behaviour and identify suspicious activities.

By combining cloud security, cryptographic techniques, and artificial intelligence, the proposed system aims to provide a secure, intelligent, and privacy-preserving cloud storage solution suitable for modern distributed environments.

II. RELATED WORK

A. Existing Cloud Storage Security Systems

Traditional cloud storage systems mainly use encryption and authentication techniques to protect user data. Algorithms such as AES and RSA are widely used to ensure confidentiality and secure communication between users and cloud servers. These systems provide scalability, remote accessibility, and efficient storage management. However, they still suffer from several limitations such as insider attacks, unauthorized access, and privacy risks because cloud providers may access stored user data.

Blind cloud storage techniques were later introduced to improve privacy protection. In blind storage systems, files are encrypted before uploading to the cloud so that only authorized users can access the original data. Although these systems improve confidentiality, many existing implementations lack intelligent threat monitoring and efficient multi-device synchronization mechanisms.

B. AI-Based Threat Detection in Cloud Computing

Recent advancements in Artificial Intelligence and Machine Learning have improved cybersecurity solutions in cloud environments. AI-based intrusion detection systems analyse user behaviour and access patterns to identify suspicious activities and abnormal login attempts. Machine learning algorithms such as Random Forest, Isolation Forest, and Logistic Regression are commonly used for anomaly detection and threat prediction.

AI-driven monitoring systems provide proactive security by continuously learning user behaviour and detecting deviations from normal activities. These techniques help reduce cyber-attacks, unauthorized access, and false security alerts. However, most existing research focuses either on cloud security or AI-based detection separately, with limited integration of blind cloud storage and intelligent threat monitoring.

Therefore, the proposed system combines blind cloud storage architecture with AI-based anomaly detection to provide a secure, intelligent, and privacy-preserving cloud storage solution for multi-device environments.

C. Recent Advancements and Research Challenges

A. Recent Advancements

Recent advancements in cloud computing security have significantly improved data protection, privacy preservation, and intelligent threat detection mechanisms. Modern cloud storage systems now integrate advanced encryption techniques, Artificial Intelligence (AI), Machine Learning (ML), and anomaly detection methods to improve overall cloud security and reliability.

Blind cloud storage architectures have emerged as an effective solution for preserving user privacy. In these systems, data is encrypted before being uploaded to cloud servers, ensuring that cloud providers cannot access the original information. Advanced encryption algorithms such as AES-256 and RSA are widely used to provide confidentiality, secure key exchange, and integrity protection.

AI-driven cybersecurity systems have also shown significant progress in recent years. Machine learning algorithms such as Random Forest, Isolation Forest, Neural Networks, and Deep Learning models are increasingly used for anomaly detection and intrusion prevention in cloud environments. These techniques help identify suspicious login attempts, abnormal access behaviour, and malicious activities in real time.

Recent research also focuses on scalable anomaly detection systems, Edge AI-based monitoring, and intelligent threat prediction frameworks. Advanced AI models can continuously learn user behaviour patterns and adapt to evolving cyber threats, improving proactive cloud security. AI-powered security monitoring and automated incident response systems are becoming important components of modern cloud infrastructures.

Furthermore, emerging technologies such as blockchain, Zero Trust Architecture, federated learning, and hybrid

cloud security frameworks are being integrated with AI-driven cloud security systems to enhance scalability, privacy, and resilience against advanced cyber-attacks.

B. Research Challenges

Despite significant advancements, several research challenges still exist in secure cloud storage and AI-based threat detection systems.

One major challenge is maintaining data privacy while performing intelligent monitoring and threat analysis. AI systems often require access to large amounts of user data for training and analysis, which may conflict with privacy-preserving cloud storage models.

Another challenge is the increasing complexity of cloud infrastructures. Multi-cloud and hybrid cloud environments introduce issues related to interoperability, distributed security management, and consistent access control mechanisms. Managing security policies across heterogeneous cloud platforms remains difficult.

AI-based intrusion detection systems also face limitations such as false positives, adversarial attacks, high computational cost, and scalability issues. Traditional anomaly detection models may fail to handle dynamic cloud environments and evolving attack patterns efficiently.

The rapid growth of AI-powered applications has also increased cloud attack surfaces. Misconfigured cloud resources, insecure APIs, identity-based attacks, and excessive permissions create additional security vulnerabilities in modern cloud systems.

Another important challenge is detecting sophisticated cyber threats in real time while maintaining system performance and low latency. Modern cloud systems generate massive volumes of access logs and network data, making efficient anomaly detection computationally demanding.

Therefore, future research should focus on developing scalable, privacy-preserving, AI-driven cloud security frameworks capable of providing intelligent threat detection, efficient multi-device synchronization, and secure data access in dynamic cloud environments.

III. SYSTEM ARCHITECTURE

The proposed Portable Blind Cloud Storage System is designed to provide secure, privacy-preserving, and intelligent cloud storage for multi-device environments. The architecture integrates authentication mechanisms, encryption techniques, cloud storage services, and AI-based threat detection to ensure secure data access and monitoring.

The system consists of six major components: User Devices, Authentication Layer, Encryption Layer, Cloud Storage Layer, AI Monitoring Engine, and Secure Retrieval Module.

Users access the system through multiple devices such as mobile phones, laptops, tablets, and desktop systems. The Authentication Layer verifies user identity using secure login credentials and password hashing mechanisms before granting access to the system.

After successful authentication, files are encrypted at the client side using AES-256 encryption. RSA algorithm is used for secure key exchange between users and the cloud environment. The encrypted files are then uploaded to the Cloud Storage Layer, where only encrypted data is stored. This blind storage architecture prevents cloud providers from accessing the original file contents.

The AI Monitoring Engine continuously analyses user behaviour, login patterns, access frequency, and device activities to detect suspicious actions and abnormal access patterns. Machine learning algorithms such as Random Forest and Isolation Forest are used for anomaly detection and intelligent threat analysis.

During file retrieval, authorized users securely download encrypted files from the cloud and decrypt them using valid encryption keys. The Secure Retrieval Module ensures safe multi-device synchronization and protected data access.

The overall workflow of the system includes secure authentication, client-side encryption, secure cloud upload, AI-based monitoring, anomaly detection, secure retrieval, and decryption. The proposed architecture enhances confidentiality, integrity, intelligent threat

detection, scalability, and privacy preservation in modern cloud environments.

III.I. Proposed Integrated Framework

The proposed integrated framework combines cloud computing, encryption techniques, secure authentication, and AI-based threat detection to provide secure multi-device cloud storage. Users are authenticated using secure login mechanisms, and files are encrypted using AES-256 before being uploaded to the cloud. RSA algorithm is used for secure key exchange.

The cloud server stores only encrypted data through a blind storage architecture, preventing unauthorized access by cloud providers. An AI monitoring module continuously analyses user behaviour and access patterns using machine learning algorithms such as Random Forest and Isolation Forest to detect suspicious activities and anomalies.

Authorized users can securely retrieve and decrypt files across multiple devices. The framework enhances data confidentiality, privacy preservation, intelligent threat detection, and secure cloud accessibility.

IV. IMPLEMENTATION

A. Technology Stack

The proposed system is developed using modern web, cloud, security, and Artificial Intelligence technologies. HTML, CSS, and JavaScript are used for designing the frontend user interface. Python with Flask framework is used for backend development and server-side processing. MongoDB/MySQL is used for database management. AWS S3 or Firebase is used as the cloud storage platform for storing encrypted files. AES-256 and RSA algorithms are implemented for encryption and secure key exchange. Machine learning libraries such as Scikit-learn are used for AI-based anomaly detection and threat monitoring.

B. Database Schema Design

The database is designed to securely manage user information, encrypted files, authentication details, and monitoring logs. The main tables/collections include:

❑ User Table

- User ID
- Username
- Email
- Password Hash
- Device Information

❑ File Storage Table

- File ID
- User ID
- Encrypted File Name
- Upload Timestamp
- Cloud Storage Path

❑ Access Log Table

- Log ID
- User ID
- Login Time
- Device Used
- Access Location
- Activity Status

❑ AI Monitoring Table

- Activity ID
- Suspicious Activity Score
- Detected Anomaly
- Threat Status

C. System Process Flowchart

The system workflow begins with user authentication. After successful login, the selected file is encrypted using AES-256 encryption. The encrypted file is uploaded to the cloud server through secure communication channels. The AI monitoring engine continuously analyzes user behavior and access patterns to identify suspicious activities. During retrieval, authorized users

download encrypted files and decrypt them using valid keys for secure access across multiple devices.



Fig 4.1.C: Flowchart of Proposed Portable Blind Cloud Storage System

D. Security Implementation

The proposed system uses multiple security mechanisms to protect user data and ensure secure cloud access. AES-256 encryption is used to encrypt files before uploading them to the cloud, while RSA algorithm provides secure key exchange. Password hashing and authentication mechanisms are implemented to prevent unauthorized access.

The blind cloud storage architecture ensures that cloud providers cannot access original user data. AI-based anomaly detection continuously monitors login behaviour and access patterns to identify suspicious activities. The system also supports secure multi-device synchronization and real-time threat alerts for enhanced cloud security.

Table 4.1: Sample User Records

User_ID	Username	Email	Device Type
U101	Aishwarya b	aish@gmail.com	Laptop
U102	Usha k p	Usha@gmail.com	mobile

Table 4.2: Sample File Storage Records

File_ID	User_ID	File_Name	Encryption
F201	U102	report.pdf	AES-255
F202	U102	project.docx	AES-256
F203	U103	project.docx	AES-257

V. CONCLUSIONS

The proposed Portable Blind Cloud Storage System provides a secure and privacy-preserving solution for multi-device cloud data access. The system combines cloud computing, encryption techniques, secure authentication, and Artificial Intelligence-based threat detection to enhance cloud security and user privacy.

AES-256 encryption and RSA key exchange ensure confidentiality and secure communication, while the blind storage architecture prevents cloud providers from accessing original user data. The integration of AI-based anomaly detection improves intelligent monitoring by identifying suspicious login attempts and abnormal access patterns in real time.

The proposed system enhances secure multi-device synchronization, scalability, and overall protection against cyber threats. This work provides a strong foundation for future AI-driven secure cloud applications and advanced cybersecurity solutions.

Furthermore, the proposed framework improves user trust and reliability in cloud environments by providing intelligent security monitoring and secure data accessibility across multiple platforms. The combination of cloud computing, cybersecurity, and AI technologies makes the system suitable for modern digital applications such as enterprise storage, healthcare systems, banking services, and secure personal cloud management. Future enhancements can further strengthen the system through advanced AI models, blockchain integration, and privacy-preserving intelligent computing techniques.

VI. ACKNOWLEDGEMENT

We express our sincere gratitude to our guide, **Mrs. Deepti N N**, Assistant Professor, Department of Computer Science and Engineering, for her valuable guidance, continuous support, and encouragement throughout the development of this project and journal paper.

We would also like to thank the faculty members of the Department of Computer Science and Engineering for providing the necessary support and technical knowledge required for completing this work successfully.

Finally, we extend our heartfelt thanks to our family members and friends for their motivation and support during the completion of this project.

VII. REFERENCES

13. References

1. M. Armbrust et al., "A View of Cloud Computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.
2. NIST, "Guidelines on Security and Privacy in Public Cloud Computing," NIST Special Publication 800-144, 2011.
3. W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th Edition, Pearson Education, 2017.
4. A. Patcha and J. M. Park, "An Overview of Anomaly Detection Techniques," *Computer Networks*, vol. 51, no. 12, pp. 3448–3470, 2007.
5. I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, MIT Press, 2016.
6. AWS Documentation, "AWS Cloud Security," Amazon Web Services.
7. Scikit -learn Documentation, "Machine Learning in Python."
8. IEEE Research Papers on Cloud Security and AI-Based Intrusion Detection Systems.

VIII. FUTURE SCOPE

The proposed Portable Blind Cloud Storage System can be further enhanced by integrating advanced Artificial Intelligence and modern cybersecurity technologies to improve security, scalability, and intelligent cloud management. Future developments can focus on building more efficient and privacy-preserving cloud storage solutions capable of handling large-scale real-world applications.

The system can be extended using advanced AI models for intelligent threat analytics and real-time cyber-attack prediction. Emerging technologies such as blockchain and federated learning can also be integrated to provide decentralized security and improved privacy preservation. In addition, the framework can support intelligent AI assistants and automated cloud security monitoring systems for enhanced user experience and system reliability.

FUTURE ENHANCEMENTS

- Integration of blockchain-based cloud security
- Federated learning for privacy-preserving AI models
- Advanced AI-based intrusion detection systems
- Secure AI assistants with encrypted memory
- Intelligent threat prediction and automated response systems
- Privacy-preserving recommendation systems
- Encrypted AI model storage and secure data sharing
- Real-time cloud security analytics and monitoring systems.

BIOGRAPHIES

Prof. Deepti N

Prof. Deepti N is a faculty member in the Department of Computer Science and Engineering at Rajiv Gandhi Institute of Technology. She has expertise in the fields of Artificial Intelligence, Machine Learning, and Data Science. Her research interests include Natural Language Processing, intelligent systems, and data-driven applications. She has guided several student projects in emerging technologies and contributed to academic research and development.

Aishwarya B Nateekar



Aishwarya B Nateekar is pursuing Bachelor of Technology in Computer Science and Engineering. The author is a Smile Foundation student and a Quest Global Scholar, reflecting strong academic excellence, technical competence, and social engagement. Her areas of interest include Artificial Intelligence, Machine Learning, Cybersecurity, and Cloud Computing. The current work focuses on secure cloud storage systems integrated with AI-based threat detection for intelligent and privacy-preserving data access.

K P Usha



K P Usha is an undergraduate student in Computer Science and Engineering with interests in software development, cloud computing, data analytics, and Artificial Intelligence. The author actively explores machine learning techniques and AI-based system design. Her current work involves secure multi-device cloud storage systems and intelligent monitoring frameworks for enhanced cybersecurity applications.

Bhoomika M Y



Bhoomika M Y is pursuing Bachelor of Technology in Computer Science and Engineering. Her interests include web technologies, database systems, cloud security, and Artificial Intelligence applications. She is involved in projects related to intelligent cloud storage, AI-based automation tools, and secure data management systems aimed at improving efficiency and scalability in modern computing environments.

Aishwarya S



Aishwarya S is a Computer Science and Engineering student with interests in cybersecurity, cloud computing, and machine learning. The author focuses on developing secure and efficient AI-based systems. Her current work includes AI-integrated cloud storage frameworks with emphasis on intelligent threat detection, secure data handling, and privacy-preserving cloud computing solutions.