JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

KEY-POLICY ATTRIBUTE-BASED ENCRYPTION WITH KEYWORD SEARCH IN VIRTUALIZED ENVIRONMENTS

Mr. A. Yovel, Dr. T. Geetha

PG- Student, Head of the Department,

Master of Computer Applications,

Gnanamani College of Technology (Autonomous), Namakkal-637003, India.

Abstract: In cloud computing environments, ensuring secure data sharing while maintaining efficient data retrieval remains a significant challenge. Traditional encryption methods, while offering confidentiality, often fall short in providing flexible access control and efficient search mechanisms. To address these limitations, this project proposes the integration of **Key-Policy Attribute-Based Encryption with Keyword Search (KP-ABE-KS)**, a privacy-preserving cryptographic scheme that combines fine-grained access control with secure and efficient keyword-based search capabilities. The KP-ABE component enables data owners to define access policies based on user attributes, ensuring that only authorized users with matching credentials can decrypt and access the data. This eliminates the need for constant oversight by the data owner and enforces policy-based access dynamically. Simultaneously, the keyword search functionality allows users to query encrypted data without revealing the content of the data or the search keywords to the cloud service provider, thereby preserving user privacy and enhancing system usability. By integrating KP-ABE with keyword search, the system allows secure and scalable data sharing in virtualized cloud environments such as public or hybrid clouds. The architecture supports dynamic user access, reduces overhead on the data owner, and enables secure retrieval of data without compromising sensitive information. Additionally, the proposed solution is designed to be resistant to various attacks, including keyword guessing and collusion attacks, ensuring robust security for sensitive information stored in the cloud. This project demonstrates the feasibility and effectiveness of the KP-ABE-KS scheme through a prototype implementation, highlighting its potential for secure data sharing in domains such as e-healthcare, financial systems, and enterprise data management where privacy and access control are paramount.

Keywords: Data Owner, Data User, Cloud Server, Key Management Centre (KMC)

I. INTRODUCTION

With the rapid growth of cloud computing and virtualization technologies, organizations and individuals increasingly rely on third-party cloud service providers to store, manage, and access vast amounts of data remotely. While cloud platforms offer scalability, cost-efficiency, and on-demand resource availability, they also raise significant concerns regarding data privacy, unauthorized access, and secure information retrieval. As sensitive information such as personal records, business documents, and healthcare data is outsourced to the cloud, ensuring its confidentiality and controlled accessibility becomes a top priority. Traditional encryption techniques, such as symmetric or public-key encryption, are effective in securing data but fall short in providing fine-grained access control and flexible search capabilities. Once data is encrypted, it becomes difficult for users to search and retrieve specific content without decrypting everything, which is inefficient and potentially insecure. Moreover, these conventional methods often require the data owner to manage user access directly, making the system less scalable and more prone to human error or delays. To overcome these limitations, this project proposes the integration of **Key-Policy Attribute-Based Encryption (KP-ABE)** with **Keyword Search** functionality in virtualized cloud environments. KP-ABE enables data owners to define access policies based on a set of attributes, such as user role, department, or clearance level. Only users whose attributes satisfy the embedded policy can decrypt the data, thereby providing **fine-grained and scalable access control**. This removes the burden of direct access management from the data owner and supports dynamic, policy-driven authorization. In addition, the incorporation of **secure keyword search** allows authorized users to perform encrypted searches over the cloud-stored data without revealing the content of their queries or the data itself to the cloud service provider. This enhances usability without compromising security, ensuring both **data privacy** and **efficient retrieval**. By combining these two powerful techniques, the proposed system addresses the dual challenges of secure access and searchable encryption, making it highly suitable for application in modern cloud-based systems

II.METHODOLOGY

1. DATA OWNER

In today's data-driven environment, organizations rely heavily on accurate, secure, and well-managed data to support business operations and decision-making. As data becomes more critical to success, the concept of data ownership has emerged as a cornerstone of data governance. A data owner is an individual or a role responsible for the quality, integrity, security, and access of specific data assets within an organization. A data owner is typically a senior-level individual within a department or business unit who is accountable for a specific set of data. They ensure that data under their control is: accurate and reliable, Secure from unauthorized access, Compliant with legal and regulatory standards, Accessible to the right people for the right purposes. Data owners are not necessarily the ones managing the data on a day-to-day basis (that's usually the data steward or data custodian), but they are accountable for how data is used and maintained. The Data Owner is typically the individual or organization responsible for generating, classifying, and encrypting sensitive data before it is stored in a cloud environment. Their responsibilities include protecting the confidentiality, integrity, and access policies associated with their data. With the emergence of KP-ABE, Data Owners can enforce fine-grained access control by embedding attribute-based policies into the encryption process. The addition of keyword search capabilities further enhances data usability, allowing authorized users to efficiently locate relevant files without compromising security. Data owners play a crucial role in ensuring that data is trustworthy, secure, and aligned with organizational goals. As organizations continue to grow and manage vast amounts of information, assigning clear data ownership becomes a strategic necessity—not just a technical detail. With strong data ownership in place, businesses can enhance compliance, boost efficiency, and drive more confident, data-informed decisions. The **Data Owner Module** is responsible for enabling secure and controlled sharing of sensitive data in the cloud environment. The primary function of the data owner is to upload encrypted files along with metadata such as keywords for search purposes. The encryption follows **Key-Policy Attribute-Based Encryption (KP-ABE)** to ensure fine-grained access control. After registration and verification by the **Key Management Center (KMC)**, the data owner can access the system. The owner uses a user-friendly interface to upload files that are encrypted using AES and tagged with searchable keywords. These files are stored securely on the cloud server, while the access control policies are embedded within the encryption. Owners can view all uploaded files, check user requests, and manage them efficiently. If a user requests access to a file, the data owner is notified and can approve or reject the request. Upon approval, a notification is sent to the KMC, which handles the generation and transmission of the appropriate decryption key to the user. This module plays a crucial role in ensuring **data confidentiality**, **access accountability**, and **controlled data distribution**. It empowers the data owner with full control over their data and who accesses it, contributing to a trustworthy cloud data-sharing ecosystem.

2. DATA USER

In any organization that depends on data, there are different roles involved in managing and interacting with it. While data owners are responsible for maintaining and protecting data assets, data users are the individuals who consume and use this data for operational, analytical, or strategic purposes. A data user is anyone who accesses data to perform a task, make decisions, or gain insights. A data user is an individual who uses data for analysis, reporting, operations, or decision-making. They are not responsible for owning or managing the data at the structural level, but they rely on data to perform their job functions. Data users span across all departments—marketing, finance, operations, HR, IT, and more. Data users work with the data that is provided, curated, and maintained by data owners and data stewards. Their role is critical in ensuring that data delivers real value to the organization. Data users form the backbone of a data-driven organization. They use data to fulfill daily operations, conduct analyses, and make informed decisions. Although they may not have ownership or custodial responsibilities, their role is critical in ensuring that data delivers value. Empowering data users with the right tools, access, and training helps organizations thrive in a competitive, data-centric world. In a KP-ABE (Key-Policy Attribute-Based Encryption) system with keyword search, the Data User is a legitimate recipient of encrypted data stored in virtualized cloud environments. These users do not have universal access but instead are granted decryption capabilities based on specific attributes assigned to them by a trusted authority. Data Users play a crucial role in retrieving and interpreting encrypted data using keyword-based search mechanisms. Their access is regulated by the structure embedded in their private keys, which reflects their roles, responsibilities, or credentials within the organization. The **Data User Module** allows registered and authorized users to securely search and retrieve encrypted data from the cloud server. This module emphasizes **privacy-preserving access**, where users can perform keyword-based search operations over encrypted data without revealing the keywords or data content. Once a user registers, the KMC verifies their identity and attributes before granting access. After logging in, users can input keywords to search for encrypted files. The system uses **searchable encryption** to match keywords without decrypting the files. If matching files are found, users can view a list of results. To access a particular file, the user must submit a request to the corresponding data owner. If the owner approves, the request is forwarded to the KMC, which verifies the user's attributes and sends a **trapdoor-secured decryption key**. The user can then use this key to decrypt and download the file. This module provides **confidential access** to data without compromising the privacy of the search terms or content. It supports scalable usage and ensures that only **authorized users with matching attributes** can access the required files, preserving both data security and user privacy.

3. CLOUD SERVER

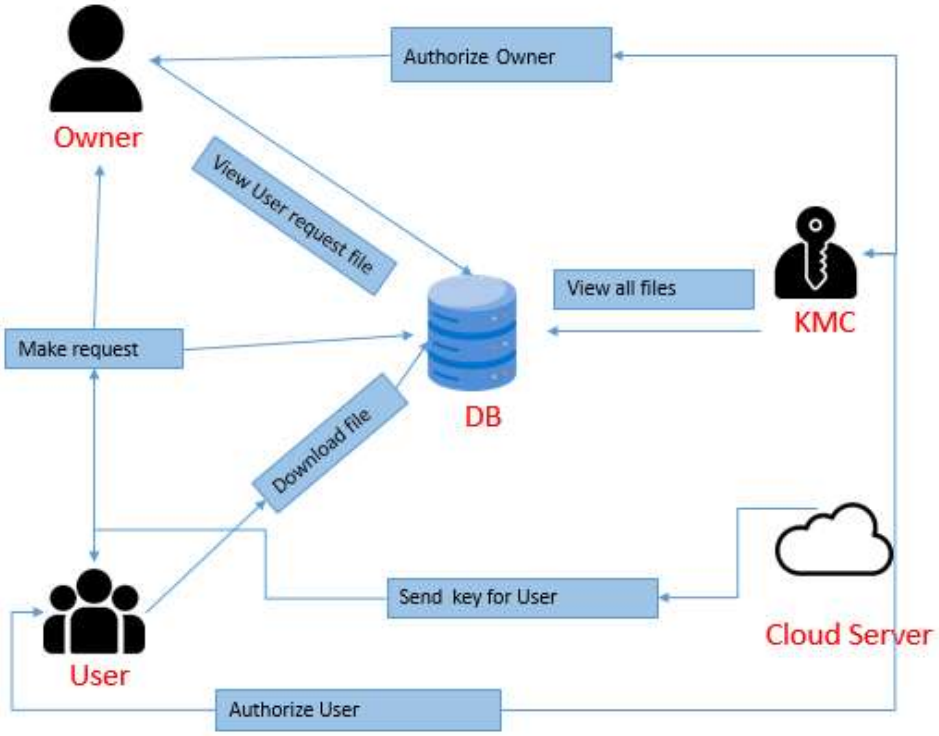
The Cloud Server Module is the backbone of the data storage and retrieval system. It acts as a secure intermediary that stores encrypted files uploaded by data owners and facilitates keyword-based searches by data users. cloud server is a virtual server (rather than a physical server) that runs in a cloud computing environment. It provides computing resources such as storage, processing power, memory, and networking over the internet. Cloud servers are hosted and maintained by cloud service providers like Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and others. Unlike traditional on-premises servers that require

physical hardware and infrastructure, cloud servers are virtualized and scalable, making them cost-effective, flexible, and efficient for businesses of all sizesThe server does not decrypt or view any file contents, maintaining strong confidentiality. After logging in with administrative credentials, cloud server operators can view and authorize user and owner accounts. The system keeps track of all uploaded files and their associated encrypted metadata for efficient keyword search processing. When users submit a search request, the server compares the encrypted keyword trapdoor against stored indices to find matching files. The cloud server also offers graphical data visualizations (powered by JFreeChart) for monitoring file activity, system usage, and data access patterns. This feature assists in system maintenance and audit operations. The Cloud Server Module ensures data integrity, search functionality, and authorized file access routing while remaining agnostic to the actual content. It forms a privacy-preserving infrastructure suitable for large-scale, secure cloud storage systems. Cloud servers have revolutionized the way organizations manage and deploy computing resources. Their scalability, affordability, and accessibility make them ideal for businesses seeking agility and growth. Whether it's for website hosting, software development, or big data analysis, cloud servers provide the flexibility and power required in the modern digital age. As technology continues to advance, the reliance on cloud infrastructure will only increase, making it an essential component of digital transformation

4.Key Management Center (KMC)

A Key Management Centre (KMC) is a centralized facility that securely generates, distributes, and manages cryptographic keys for various applications. The KMC plays a crucial role in ensuring the security and integrity of sensitive data. The **Key Management Center (KMC)** is a trusted authority responsible for handling identity verification, key generation, and secure key distribution in the system. It is the **central control point** for maintaining access policies and ensuring that only authorized users receive decryption keys. Upon registration, both data owners and data users must be approved by the KMC based on pre-defined attribute sets such as department, role, or access level. The KMC then issues keys derived from **Key-Policy Attribute-Based Encryption (KP-ABE)**, binding users to specific access policies. When a user requests access to an encrypted file and the data owner approves it, the KMC receives this request and checks the user's attributes. If the attributes satisfy the access policy embedded in the file's ciphertext, the KMC generates a secure decryption key (trapdoor) and transmits it to the user. In addition, the KMC provides analytics and system monitoring through graphs and logs. It plays a critical role in enforcing security policies, preventing **collusion attacks**, and enabling **dynamic user and access management**. This module enhances system **scalability**, **reliability**, and **security enforcement**, making it essential for regulated environments such as healthcare, enterprise, and academia.

III.SYSTEM ARCHITECTURE



IV.RESULT AND DISCUSSION:

The proposed Plant Leaf Disease Detection System using a Vision Transformer (ViT)-based Multi-Class Classifier achieves higher accuracy and better generalization compared to traditional methods. By analyzing plant leaf images through self-attention mechanisms, the model improves disease identification across multiple classes. This system enables early detection, helping farmers take timely actions to minimize crop losses and promote sustainable agriculture. The integration of KP-ABE with keyword search

has proven to be both **technically feasible** and **practically effective**. The prototype demonstrates how secure, fine-grained, and privacy-preserving data access can be achieved in cloud environments. The use of attribute-based policies ensures that only users with appropriate credentials can decrypt data, while the keyword search mechanism adds practical usability without compromising security.

V. CONCLUSION

Virtualized Environments" project presents a secure and scalable solution to the growing demand for privacy-preserving data sharing in cloud computing. By combining attribute-based encryption with secure keyword search capabilities, the system addresses two critical challenges in cloud security: ensuring that only authorized users can access sensitive data and allowing users to efficiently retrieve specific information without compromising data confidentiality. The integration of KP-ABE enables fine-grained access control, where access rights are defined through access policies associated with attributes rather than fixed user identities. This ensures greater flexibility and scalability, particularly in dynamic environments where user roles and permissions frequently change. Only users whose attribute set satisfies the embedded access policy are granted access to the encrypted data, thereby eliminating unauthorized data exposure. In parallel, the keyword search mechanism allows users to search encrypted data using specific terms without the need for decryption or revealing sensitive information to the cloud provider. This enhances data usability and efficiency, making it feasible to retrieve relevant information quickly, even when stored in encrypted form. The system maintains a strong balance between security and functionality, offering an effective solution for applications that handle confidential or sensitive information, such as in healthcare, finance, education, and government sectors.In conclusion, this project demonstrates the practical implementation and potential impact of integrating KP-ABE with keyword search in cloud environments. It lays the groundwork for more advanced privacy-preserving data sharing systems and opens up opportunities for future enhancements, including support for complex queries, real-time access monitoring, and integration with emerging technologies like blockchain and AI-based threat detection. The proposed model serves as a significant step forward in building secure, intelligent, and user-centric cloud computing ecosystems.

VI. REFERENCES:

[1] Z. Xia, N. N. Xiong, A. V. Vasilakos, and X. Sun, “EPCBIR: An efficient and privacy-preserving content-based image retrieval scheme in cloud computing,” Inf. Sci., vol. 387, pp. 195–204, 2017.

[2] L. Rao, H. Zhang, and T. Tu, “Dynamic outsourced auditing services for cloud storage based on batch-leaves-authenticated merkle hash tree,” IEEE Trans. Services Comput., vol. 13, no. 3, pp. 451–463, May/Jun. 2020

[3] Miao, R. Deng, X. Liu, K.-K. R. Choo, H. Wu, and H. Li, “Multiauthority attribute-based keyword search over encrypted cloud data,” IEEE Trans. Dependable Secure Comput., vol. 18, no. 4, pp. 1667–1680, Jul./Aug. 2021

[4] G. Xu, H. Li, Y. Dai, K. Yang and X. Lin, "Enabling efficient and geometric range query with access control over encrypted spatial data", *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 4, pp. 870-885, Apr. 2019.

[5] S. ManjuNair and M.S. Rajasree, "Fine-grained search and access control in multi-user searchable encryption without shared keys", J. Inf. Secur. Appl., vol. 41, pp. 124-133, 2018.