

Identity based encryption

Accountable Privacy Preserving with Attribute-Based Encryption for Cloud Storage

A Project Report

submitted in partial fulfilment of the requirements

of

Applied Cloud Computing for Securing data

By

DUDDELA MUKESH

20AK1A0583

BOGGALA NAVEEN KUMAR REDDY

20AK1A0593

BADDULA SURESH

21AK5A0513

VOODI NARENDRA

20AK1A0591

KAMMARI LALITH KUMAR

21AK5A0515

Under the Esteemed Guidance of
UMAMAHESWARI R

ACKNOWLEDGEMENT

We wish to express our deep appreciation to everyone who played a vital role in the triumphant culmination of this project.

Primarily, our heartfelt gratitude goes out to **Umamaheswari R.** Her profound expertise and guidance were instrumental in steering us through challenges and aiding us in making well-informed decisions throughout the project journey.

A special acknowledgment is extended to the **Techsakshyam team**, whose dedicated time and efforts proved invaluable. Your insightful advice greatly aided us in reaching the successful completion of the project. To you, we owe a debt of eternal gratitude.

Our sincere thanks extend to the **Edunet Foundation**, for their mentorship and constructive feedback, which significantly enhanced the project. Their wealth of wisdom and experience provided invaluable perspectives, guiding the project towards the pinnacle of excellence.

Recognition is due to the unwavering efforts of our team members who committed their time and expertise to various facets of the project. Everyone's distinctive contribution has left an indelible mark, transforming this initiative into a collaborative and meaningful endeavor.

In conclusion, heartfelt thanks to all contributors who played a pivotal role in making the Weather Master App project a resounding success. To each one of you, we express our deepest appreciation for being an integral part of this endeavor.

ABSTRACT

In the current cloud storage, Issues with access control and data security must be resolved immediately. Since it enables dynamic access control over encrypted data, multi-authority attribute-based encryption (MA-ABE) is viewed as a viable remedy for data access control security issues in the dynamic Internet of things.

But the current issue with key abuse is seriously undermining MA-ABE's security access control. Only a single authority and a small universe of attributes (users) are supported by the current accountable attribute-based encryption systems. Furthermore, they oppose revocation. Because they are built in the composite order bilinear group, some techniques are inefficient. The author of this paper suggests the first vast universe decentralized accountability system. Multi-authority attribute-based encryption scheme with outsourcing decryption based on prime order bilinear groups.

The proposed scheme allows for the dynamic capacity expansion of attributes, users, and authorities. An audit mechanism is given to judge if the suspicious key was leaked by a malicious user or by authorities and to determine the identity of the leaker. The malicious user who divulges key can be punished by user-attribute revocation. The revocation mechanism is resistant to collusion attacks undertaken by revoked users and non-revoked users. Meanwhile, it satisfies the requirements of forward and backward security. To save resources, the outsourced decryption module is optional for users with restricted resources. According to the results of the performance analysis, it is suited for large-scale cross-domain cooperation in the dynamic cloud storage.

we extend the offer mentioned proposed system with a Ciphertext Policy Attribute Based Encryption (CP-ABE) scheme with accountability to address the security and privacy issues

Key Features:

Identity-Based Encryption (IBE):

IBE is a cryptographic scheme where a user's public key can be derived from some unique information associated with the user, such as an email address or username. This simplifies key management as there's no need for a complex public key infrastructure (PKI) and certificate management.

Fine-Grained Access Control:

With IBE, fine-grained access control can be achieved. Administrators can define access policies based on users' identities or attributes, allowing for precise control over who can access what data.

Group-Based Access Control:

Group data sharing allows users to be organized into groups, and access policies can be applied at the group level. This simplifies access management, as permissions can be assigned to entire groups rather than individual users.

TABLE OF CONTENTS

Abstract	iii
List of Figures	v
Chapter 1. Introduction	01
1.1 Problem Statement	01
1.2 Problem Definition	01
1.3 Expected Outcomes	012
Chapter 4. Implementation and Results	13
4.1 System Implementation	13
4.2 Testing and Validation	14
4.3 Results and Findings.....	17
Chapter 5. Conclusion	20
GitHub Link.....	20
Video Link	20
References.....	Error! Bookmark not defined.
1.4. Organization of the Report	02
Chapter 2. Literature Survey	03
2.1 Paper- 1	03
Chapter 3. Proposed Methodology	05 3.1
System Design	05
3.2 Modules used	06
3.3 Data Flow Diagrams (DFD)	07
3.4 Advantages	09
3.5 Requirement Specifications	09

LIST OF FIGURES

Sl. No.	Name	Page No.
Figure 1	System Design	6
Figure 2	DFD: Level 0	7
Figure 3	DFD: Level 1	8
Figure 4	Registration Page	14
Figure 5	Login Page	15

CHAPTER 1 INTRODUCTION

1.1. Problem Statement:

In the real world of cloud computing, data sharing among groups demands robust security mechanisms to safeguard sensitive information. Multi Authority Attribute Based Encryption presents a promising approach for securing data in cloud environments, offering convenience and flexibility in key management and for reducing the storage cost.

1.2. Problem Definition:

The Internet of Things (IoT) is a new paradigm that integrates more and more physical things in the real world across different areas into communication networks by ubiquitous enabling device technologies such as near field communication (NFC) devices, RFID tags and readers, and embedded sensor and actuator nodes. It collects, analytics, stores, shares, and access data across different platforms, then provides intelligent services in the form of smart cities, smart grids, smart homes, smart transportation, smart healthcare with the help of other technologies such as cloud computing and artificial intelligence.

Since the data is mostly confidential and privacy-sensitive, IoT security and access control issues urgently need to be addressed. Encryption is an ideal way to protect data confidentiality. Attribute-based encryption (ABE) is considered an ideal technology to realize fine-grained access control on encrypted data which is introduced by Sahai and Waters [4]. In 2006, Goyal et al. distinguished ABE into key-policy attribute based encryption (KP-ABE) and ciphertext-policy attribute based encryption (CP-ABE). In KP-ABE, secret keys are associated with access policies, and ciphertexts are associated with attributes, while in CP-ABE the ciphertexts are associated with access policies, and secret keys are associated with attributes.

A user can decrypt the ciphertext (i.e. access data) if and only if her/his attributes (i.e. access privileges) satisfy the ciphertext access policy. Therefore, ABE is often used to solve the challenging issue in secure data storage. However, in the Internet of things, data are shared and applied across different domains and organizations, which means that the attributes of users are authorized by different authorities in the same system. So multi-authority attribute based encryption is more practical than single-authority attribute-based encryption for the Internet of things. Moreover, the dynamic capacity expansion of attributes and users is necessary for the Internet of things. So large universe

ABE is more practical than small universe ABE. In small universe ABE, all the attributes are fixed and enumerated when the system is initialized. After that, even adding only one attribute will lead to rebuilding the system and possibly re-encrypting all the data. Conversely, in the large universe ABE, any string can be used as an attribute, and the attributes do not need to be enumerated during system setting, which is more flexible and practical for the dynamic Cloud.

1.3. Expected Outcomes:

Group data sharing in Advanced encryption algorithm (AES) can yield several expected outcomes, which are advantageous for organizations and users engaging in collaborative activities. Here are some of the expected outcomes:

1. **Improved Data Security:** Enhanced security measures implemented within the cloud environment to safeguard sensitive data against unauthorized access, data breaches, and cyber threats. This may include the implementation of encryption, access control mechanisms, authentication protocols, and intrusion detection/prevention systems.
2. **Reduced Storage Costs:** Implementation of efficient storage management techniques, such as data deduplication, compression, and tiered storage, to optimize resource utilization and reduce storage overheads. This leads to cost savings for organizations hosting data in the cloud.
3. **Enhanced Data Availability and Accessibility:** Implementation of redundancy and failover mechanisms to ensure high availability of data and services in the cloud. This includes strategies such as data replication, load balancing, and disaster recovery planning to minimize downtime and ensure business continuity.
4. **Scalability and Performance Optimization:** Implementation of scalable architectures and performance optimization techniques to handle increasing data volumes and user loads in the cloud. This may involve resource provisioning, load balancing, caching, and optimization of network and storage infrastructures.
5. **Compliance and Regulatory Adherence:** Implementation of security and privacy measures to ensure compliance with industry regulations and data protection laws (e.g., GDPR, HIPAA, PCI DSS). This includes implementing security controls, conducting regular audits, and maintaining proper documentation to demonstrate compliance.
6. **Streamlined Data Management Processes:** Implementation of automation and orchestration tools to streamline data management processes, such as data backup, replication, synchronization, and archival. This improves operational efficiency and reduces the risk of human error.
7. **Improved User Experience:** Implementation of user-friendly interfaces and self-service portals for managing and accessing data in the cloud. This enhances user experience and productivity while maintaining security and compliance requirements.
8. **Effective Incident Response and Recovery:** Implementation of incident response plans and procedures to detect, respond to, and recover from security incidents and data breaches in the cloud. This includes incident detection tools, incident response teams, and incident recovery strategies to minimize the impact of security incidents on business operations.

Overall, the expected outcomes of cloud storage and security projects aim to improve the overall security, efficiency, and reliability of data storage and management in the cloud while meeting regulatory requirements and business objectives.

1.4. Organization of the Report:

This report explores the implementation of group data sharing based on AES, It is a cryptographic primitive that allows users to encrypt data for a group based on their identities, rather than public keys. We have meticulously organized the project report for " Accountable Privacy Preserving with Attribute-Based Encryption for Cloud Storage

" to provide readers with comprehensive insights into the initiative's objectives, methodologies, findings, and outcomes. The report begins with a detailed Project Description, outlining the overarching goals, scope, and significance of the " Accountable Privacy Preserving with Attribute-Based Encryption for Cloud Storage" project.

CHAPTER 2 LITERATURE SURVEY

1. **2.1. Paper – 1:** N. Chen, J. Li, Y. Zhang, and Y. Guo, “Efficient CP-ABE scheme with shared decryption in cloud storage,” IEEE Trans. Comput., early access, Dec. 14, 2022

2.1.1. Brief Introduction of Paper:

Attribute based encryption (ABE) is a preferred technology used to access control the data stored in the cloud servers. However, in many cases, the authorized decryption user may be unable to decrypt the ciphertext in time for some reason. To be on the safe side, several alternate users are delegated to cooperate to decrypt the ciphertext, instead of one user doing that. We provide a ciphertext-policy ABE scheme with shared decryption in this paper. An authorized user can recover the messages independently. At the same time, these alternate users (semi-authorized users) can work together to get the messages. We also improve the basic scheme to ensure that the semi-authorized users perform the decryption tasks honestly. An integrated access tree is used to improve the efficiency for our scheme. The new scheme is proved CPA-secure in the standard model. The experimental result shows that our scheme is very efficient on both computational overhead and storage cost.

2.1.2. Techniques used in Paper:

The techniques used in the paper for improving the group data sharing in cloud computing on identity based encryption can be categorized into several key areas, including software development, data analysis, user experience design, and project management. Here's a breakdown of some of the techniques employed:

- **HTML (Hypertext Markup Language):** HTML is the standard markup language used for creating web pages. PHP-based websites typically generate HTML dynamically, allowing content to be generated on-the-fly based on user input or other factors.
- **CSS (Cascading Style Sheets):** CSS is a stylesheet language used to control the presentation and styling of HTML elements on a web page. PHP-based websites often use CSS to define the colors, fonts, spacing, and other visual aspects of the site's design.
- **JS(JavaScript):** JavaScript is a client-side scripting language used to add interactivity and dynamic functionality to web pages. While PHP handles server-side tasks, JavaScript is used to enhance the user experience by enabling features such as form validation, interactive menus etc.
- **JSP (JavaServer Pages):** JSP allows you to create dynamic web pages by embedding Java code within HTML. You would use JSP to generate the dynamic

Content of your cloud application.

Performance Optimization Techniques: This includes techniques such as code optimization, caching mechanisms, asynchronous loading, and image optimization to improve the app's performance, reduce loading times, and enhance responsiveness.

Data Validation and Accuracy: Methods for validating and ensuring the accuracy

- of data, including rigorous testing against ground truth observations and implementing predictive algorithms to improve forecast accuracy.

Cross-Browser Compatibility and Mobile Responsiveness: Testing the project

- across various web browsers and devices to ensure consistent performance and user experience, and applying responsive design principles to adapt the system layout and functionality to different screen sizes and resolutions.

- **Comprehensive Documentation and Coding Standards:** Maintaining detailed documentation covering system architecture, API specifications, codebase structure, and development guidelines, as well as enforcing coding standards and best practices to ensure code maintainability, readability, and extensibility.

- **User-Centric Design Principles:** Incorporating user feedback and conducting user research to refine the software user interface design, navigation, and presentation of cloud data to ensure an intuitive and seamless user experience.

.

CHAPTER 3

PROPOSED METHODOLOGY

3.1 System Design:

- The traceable multi-authority ABE and accountable multi-authority ABE is proposed as MA-CP-ABE scheme, which allows tracing the identity of a misbehaving user who leaked the decryption key to others.
- proposed the first accountable authority CP-ABE with white-box traceability that provides an auditor to judge publicly whether a suspected user is guilty.
- The proposed scheme supports the dynamic capacity expansion of attributes, users, and authorities.
- It is suitable for large-scale multi-domain collaboration in the dynamic cloud.
- The proposed scheme provides an audit mechanism to judge whether a malicious user or authorities leak the suspicious key, and to determine the integrity of the content.
- The revocation mechanism is secure against the collusion attack launched by revoked users and non-revoked users. Meanwhile, it meets the requirements of forward and backward security.
- De-duplication identifies the repeated content and compress the storage system, which leads to consume less storage.
- The limited-resource user can choose to outsource decryption for saving resources. The performance analysis results indicate that the proposed scheme is more efficient and suitable for the cloud

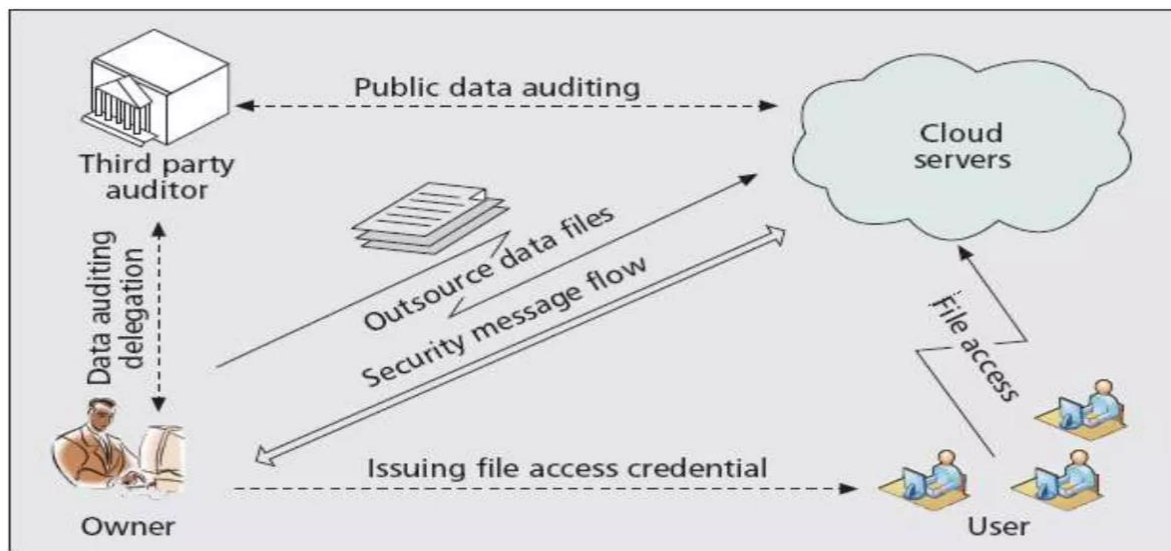


Figure 1: System Design

3.2 Modules Used:

1. The Central Trusted Authority (CTA)

is responsible for generating the global public parameters and the inspection authority's secret key. CTA is considered as a trusted entity in our model.

2. The Attribute Authorities (AA)

are a group of authorities responsible for managing attributes and issuing related secret keys. Unlike state of the art multi-authorities ABE schemes where each authority issues only one attribute, in Ins-PAbAC, each AA may manage a whole set of attributes. These authorities are considered as a trusted entities as they have access to users secret keys as well as their identities.

3. The Inspection Authority (IA)

is an independent authority able to revoke the anonymity of a malicious user when an attack occurs. IA is considered as a trusted entity.

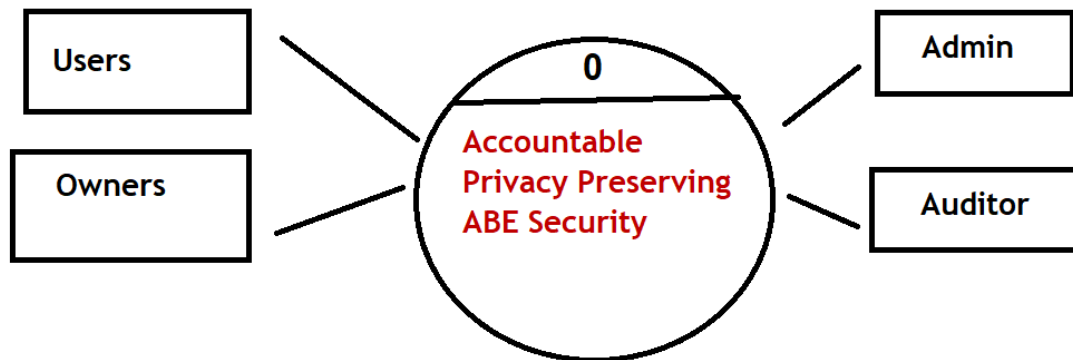
4. The Cloud Service Provider (CSP)

is a remote cloud server who stores and shares data among authorised users. CSP is also responsible for authenticating users before downloading data. CSP is a honest but curious entity

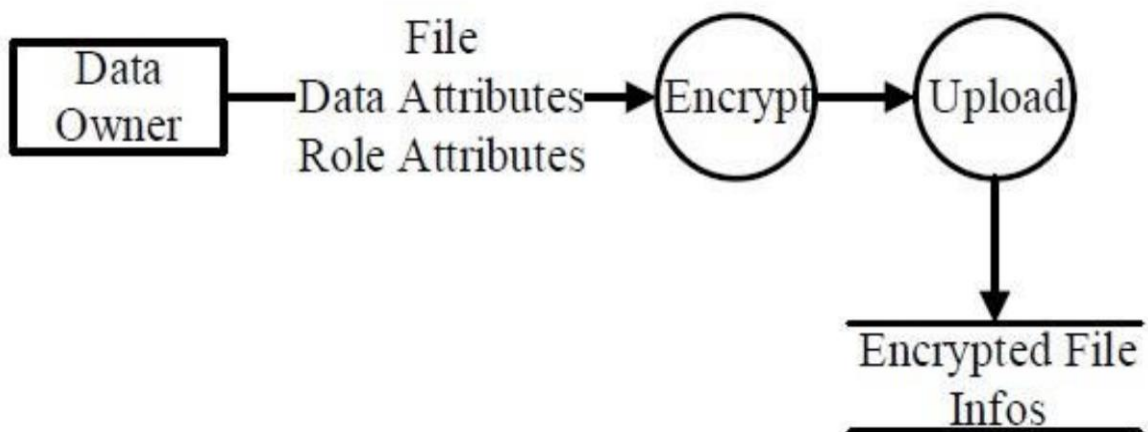
3.3 Data Flow Diagram:

A Data Flow Diagram (DFD) is a graphical representation of the "flow" of data through an information system, modeling its process aspects. A DFD is often used as a preliminary step to create an overview of the system, which can later be elaborated. DFDs can also be used for the visualization of data processing (structured design).

3.3.1. DFD Level 0



3.3.2. DFD Level 1 –



3.4 Advantages:

The identity based encryption offers several advantages:

Some of them are as follows:

- **Simplified Key Management:** IBE eliminates the need for a complex Public Key Infrastructure (PKI) by allowing keys to be generated based on users' identities. This simplifies key management, reducing administrative overhead and complexity.
- **Fine-Grained Access Control:** IBE enables fine-grained access control, allowing administrators to define access policies based on users' identities or attributes. This ensures that only authorized users have access to specific data, enhancing security and privacy.
- **Scalability:** Cloud computing platforms offer scalable resources, making it easy to accommodate growing numbers of users and increasing amounts of data. IBE can leverage this scalability to support dynamic group data sharing environments without sacrificing performance.

3.5 Requirement Specification:

3.5.1 Hardware Requirements:

1. Processor Requirement:

- Intel Core i5/i7 or AMD equivalent

2. RAM Requirement:

- Minimum: 4 GB
- Recommended: 8 GB (especially for heavier workloads)

3. Storage Requirement:

- At least 20 GB of free space for the operating system (Windows/macOS)
- Additional space for Tomcat installation, website files, databases, development tools, code files, and temporary files.

3.5.2 Software Requirements:

○ Operating System:

Windows or macOS for development environments. For Mobiles Android or IOS.

○ Web Server:

Tomcat Server.

○ Database:

Optimize database queries for efficiency.

- **Back-End Technology:**

Java, Servlets, JSP for dynamic content generation.

- **Front-End Technology:**

HTML, CSS, JavaScript, responsive design principles.

CHAPTER 4

IMPLEMENTATION AND RESULT

4.1 System Implementation:

Establishes foundational concepts of cloud computing, group data sharing, and Identity-Based Encryption (IBE). Discusses theoretical principles of cryptography relevant to IBE.

Explores theoretical models of access control, key management, data confidentiality, integrity, authentication, trust, security analysis, privacy, legal and ethical considerations, and future directions and challenges. Improved early quality

1) Requirement Analysis:

Requirement analysis is a crucial phase in the implementation process of group data sharing in cloud computing with Identity-Based Encryption (IBE). In this phase, the organization identifies and documents its needs, objectives, and constraints to ensure that the implemented system meets its expectations.

Functional Requirements:

- User Authentication
- Key Management
- Access Control

Non-Functional Requirements:

- Performance
- Reliability
- Scalability
- Usability

2) Design Phase:

The design page for the implementation of group data sharing in cloud computing with IdentityBased Encryption (IBE) would outline the high-level architectural design and components of the system. This design page provides a high-level overview of the system architecture and components involved in implementing group data sharing in cloud computing with Identity-Based Encryption. It serves as a blueprint for the development and deployment of the system, guiding the implementation process.

User Interface Design:

User interface design is a critical aspect of implementing group data sharing in cloud computing with Identity-Based Encryption (IBE). A well-designed user interface enhances user experience, promotes usability, and facilitates efficient interaction with the system. By incorporating these elements into the user interface design, the system can provide a user-friendly and intuitive experience for users interacting with the group data sharing platform in the cloud.

Functional Design:

Functional design focuses on outlining the specific functionalities and features of the system, detailing how users will interact with it to achieve their objectives. By defining these functionalities in the functional design, the system can be developed and implemented to meet the organization's requirements for secure and efficient group data sharing in the cloud with Identity-Based Encryption.

3) Development Phase:

During the development phase of implementing group data sharing in cloud computing with Identity-Based Encryption (IBE), the focus is on translating the design specifications into functional software components.

Coding and Implementation:

- Developers begin by translating the design specifications and requirements into code using programming languages and frameworks selected for the project. They follow coding standards, best practices, and design patterns to ensure the codebase is maintainable, scalable, and efficient.
- The development process encompasses building the backend infrastructure, such as databases, servers, as well as the frontend components, including user interfaces, forms, and interactive elements.

4.2 Testing and Validation:

- The process of executing a system with the intent of finding an error.
- Testing is defined as the process in which defects are identified, isolated, subjected for rectification and ensured that product is defect free in order to produce the quality product and hence customer satisfaction.
- Quality is defined as justification of the requirements
- Defect is nothing but deviation from the requirements
- Defect is nothing but bug.
- Testing --- The presence of bugs
- Testing can demonstrate the presence of bugs, but not their absence
- Debugging and Testing are not the same thing!
- Testing is a systematic attempt to break a program or the AUT
- Debugging is the art or method of uncovering why the script /program did not execute properly.

Testing Methodologies:

- **Black box Testing:** is the testing process in which tester can perform testing on an application without having any internal structural knowledge of application.
Usually Test Engineers are involved in the black box testing.

-
- **White box Testing:** is the testing process in which tester can perform testing on an application with having internal structural knowledge. Usually The Developers are involved in white box testing.
 - **Gray Box Testing:** is the process in which the combination of black box and white box tonics' are used.

5.2 TCD (Test Case Document):

Test Case Document Contains

- Test Scope (or) Test objective
- Test Scenario
- Test Procedure
- Test case

This is the sample test case document for the Case Investigate details of Client project:

Test scope:

- Test coverage is provided for the screen “ Login check” form of a Administration module of Forensic Manager application
- Areas of the application to be tested

Test Scenario:

When the office personals use this screen for the data entry, adding sections, courts, grades and Case Registration information on s basis and quit the form.

Test Procedure:

- The procedure for testing this screen is planned in such a way that the data entry, status calculation functionality, saving and quitting operations are tested in terms of GUI testing, Positive testing, Negative testing using the corresponding GUI test cases, Positive test cases, Negative test cases respectively.

Example for Gui Test cases:

T.C.No	Description	Expected value	Actual value	Result
1	Check for all the features in the screen	The screen must contain all feature		
2	Check for the alignment of the objects as per the validations	The alignment should be proper way		

Positive Test Cases:

- The positive flow of the functionality must be considered
- Valid inputs must be used for testing
- Must have the positive perception to verify whether the requirements are justified.

Example for Positive Test cases:

T.C.No	Description	Expected value	Actual value	Result
1	Input UserName and Password	Redirect to HomePage	Redirect to Home Page	Redirect to Home Page

Negative Test Cases:

- Must have negative perception.
- Invalid inputs must be used for test.

Example for Negative Test cases:

T.C.No	Description	Expected value	Actual value	Result
1	Input username and password	Login Page	Login Page	Login Page

4.3 Results and Findings:

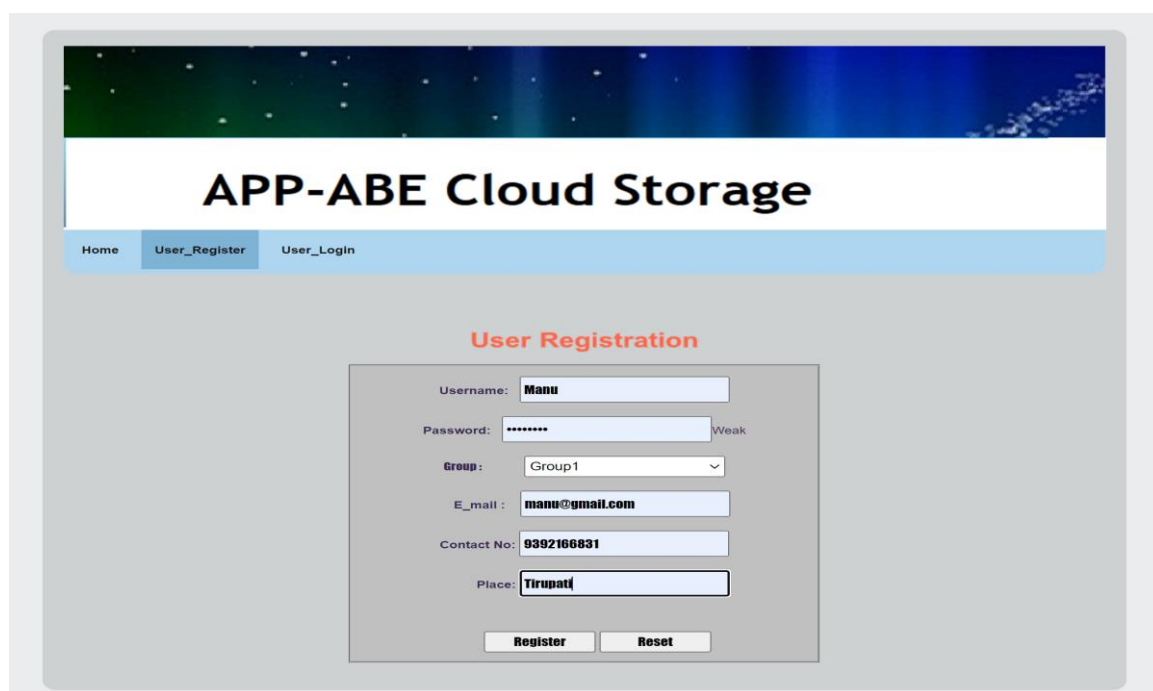
4.3.1 Results:

Enhanced Security: IBE eliminates the need for pre-distributed public keys, reducing the risk of unauthorized access due to key management issues.

Granular Access Control: Data can be encrypted for specific groups or users within a group, ensuring only authorized members can access it. This is particularly beneficial for sensitive data.

Scalability: IBE allows for efficient data sharing with a large number of users within a group without managing individual public/private key pairs for each member. This simplifies administration for large groups.

Efficient Revocation: Revoking access for compromised or departed members becomes easier as keys are tied to identities, not public keys. This ensures data security even when user credentials are compromised.



The screenshot displays the 'APP-ABE Cloud Storage' user registration interface. At the top, a navigation bar includes 'Home', 'User_Register' (the active page), and 'User_Login'. The main heading is 'APP-ABE Cloud Storage'. Below this, the 'User Registration' section is highlighted in red. The registration form contains the following fields and values:

- Username:
- Password: (Weak)
- Group:
- E_mail:
- Contact No:
- Place:

At the bottom of the form are two buttons: 'Register' and 'Reset'.

Figure 1: Registrartion page

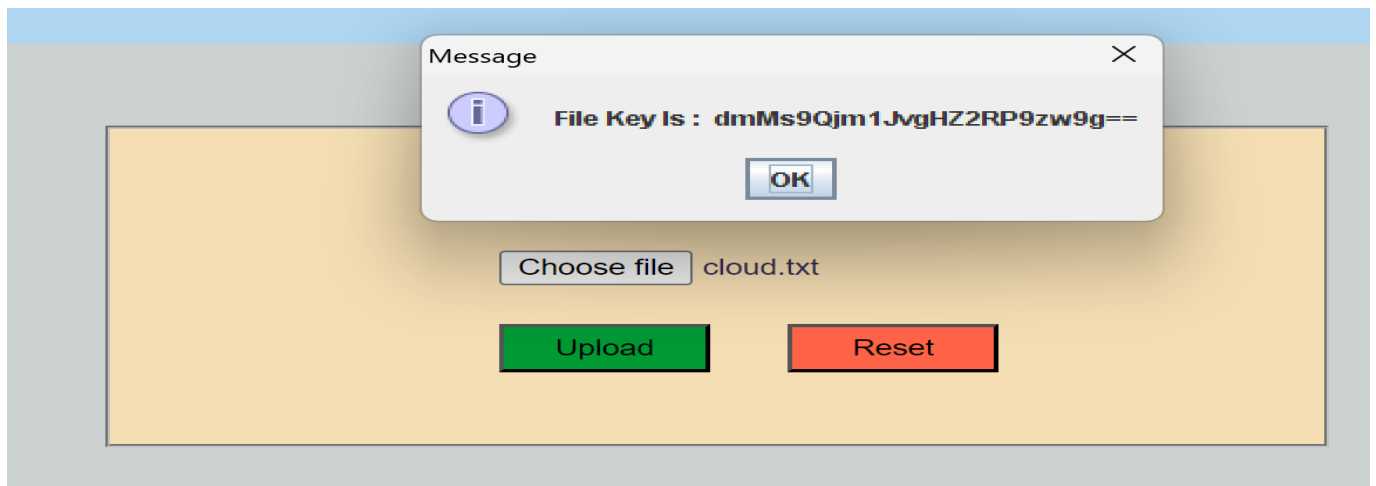


Figure 2: CHOOSING FILE

Data File Name	Date & Time	View
got.txt	2014/Oct/10 13:52:45	View
readme.txt	2014/Nov/06 11:08:26	View
readme.txt	2014/Nov/06 13:23:47	View
	2024/Feb/23 12:37:37	View
catxcxzfghjhgfxcvb.txt	2024/Feb/23 12:37:37	View
catxcxzfghjhgfxcvb.txt	2024/Feb/23 12:37:37	View
PDS MODEL PAPER.docx	2024/Feb/23 12:37:37	View
PDS MODEL PAPER.docx	2024/Feb/23 12:37:37	View
tcs.docx	2024/Feb/23 12:37:37	View
cloud.txt	2024/Feb/23 16:30:10	View

FIGURE 3: DATA STORAGE

4.3.2 Findings:

The "findings" typically refer to the insights or discoveries gained from the implementation process and any associated research or analysis. In the context of implementing group data sharing in cloud computing with Identity-Based Encryption (IBE), the findings may include:

Effectiveness of IBE: Evaluation of the effectiveness of Identity-Based Encryption (IBE) in securely encrypting and decrypting data for group data sharing in the cloud. This includes assessing the strength of the encryption algorithms used and their suitability for protecting sensitive data.

User Experience: Analysis of user experience with the implemented system, including ease of use, navigation, and satisfaction with the user interface. Findings may highlight areas for improvement to enhance user experience and adoption.

Security Assessment: Assessment of the security measures implemented in the system, including access control mechanisms, encryption practices, and compliance with security standards and regulations. Findings may identify vulnerabilities or areas for strengthening security measures.

Scalability and Performance: Evaluation of the system's scalability and performance under various loads and conditions. Findings may include insights into system responsiveness, throughput, and resource utilization, as well as recommendations for optimizing performance.

Compliance and Legal Considerations: Assessment of the system's compliance with relevant regulations, industry standards, and organizational policies related to data protection and privacy. Findings may identify areas of non-compliance and recommend remediation measures.

Collaboration and Productivity: Analysis of the impact of the implemented system on collaboration and productivity within user groups. Findings may include improvements in communication, workflow efficiency, and collaboration effectiveness.

Cost-Effectiveness: Evaluation of the cost-effectiveness of the implemented system, including the total cost of ownership, return on investment, and cost savings realized through improved efficiency and security.

User Feedback and Adoption: Analysis of user feedback and adoption rates to assess user satisfaction, acceptance, and usage patterns. Findings may highlight user preferences, concerns, and areas for further training or support.

Lessons Learned: Identification of lessons learned during the implementation process, including challenges encountered, successful strategies, and areas for improvement in future implementations.

CHAPTER 5 CONCLUSION

The first accountable and revocable large universe multi-authority attribute-based encryption scheme with outsourcing decryption based on prime order bilinear groups. An audit mechanism is given to judge if the suspicious key was leaked by a malicious user or by authorities and to determine the identity of the leaker. The malicious user who divulges key can be punished by user-attribute revocation. The revocation mechanism is resistant to collusion attacks undertaken by revoked users and non-revoked users. Meanwhile, it satisfies the requirements of forward and backward security. The proposed scheme is static security in the random oracle model. To save resources, the outsourced decryption module is optional for users with restricted resources. According to the results of the performance analysis, it is suited for large-scale cross-domain cooperation in the dynamic cloud-aided IoT. However, the author considers improving the scheme for security without the random oracle model and more efficiency in future work.

SCOPE OF FUTURE ENHANCEMENT

The system can be made more flexible and scalable using these recommendations. Please note that the system implemented here is just a prototype of idea presented via this project.

The proposed scheme is static security in the random oracle model. To save resources, the outsourced decryption module is optional for users with restricted resources. According to the results of the performance analysis, it is suited for large-scale cross-domain cooperation in the dynamic cloud-aided IoT. However, the author considers improving the scheme for security without the random oracle model and more efficiency in future work.

GITHUB LINK

<https://github.com/Mukesh-developer83/Accountable-privacy-preserving-with-attribute-based-encryption>

VIDEO LINK

[https://drive.google.com/file/d/16KwM70GJYWa2m6ZRmscbKHpN59LJVaN2/view?usp=drive link](https://drive.google.com/file/d/16KwM70GJYWa2m6ZRmscbKHpN59LJVaN2/view?usp=drive_link)

REFERENCES

1. N. Chen, J. Li, Y. Zhang, and Y. Guo, “Efficient CP-ABE scheme with shared decryption in cloud storage,” *IEEE Trans. Comput.*, early access, Dec. 14, 2022
2. . Li, Q. Huang, X. Chen, S. S. M. Chow, D. S. Wong, and D. Xie, “Multiauthority ciphertext-policy attribute-based encryption with accountability,” in *Proc. 6th ACM Symp. Inf., Comput. Commun. Secur. (ASIACCS)*, 2021, pp. 386–390
3. Z. Liu and D. S. Wong, “Traceable CP-ABE on prime order groups: Fully secure and fully collusion-resistant blackbox traceable,” in *Proc. Int. Conf. Inf. Commun. Secur. Cham, Switzerland: Springer*, 2019
4. J. Ning, Z. Cao, X. Dong, J. Gong, and J. Chen, “Traceable CP-ABE with short ciphertexts: How to catch people selling decryption devices on eBay efficiently,” in *Proc. Eur. Symp. Res. Comput. Secur. Cham, Switzerland: Springer*, 2019
5. J. Li, Y. Zhang, J. Ning, X. Huang, G. S. Poh, and D. Wang, “Attribute based encryption with privacy protection and accountability for CloudIoT,” *IEEE Trans. Cloud Comput.*, early access, Feb. 19, 2020.