Group Data Sharing in cloud computing on identity based encryption

A Project Report

submitted in partial fulfilment of the requirements of

## Applied Cloud Computing for Software Development

By

|  |  |
| --- | --- |
| **THELLAMEKALA REDDY PRAKASH** | **20AK1A05B6** |
| **MEENIGE KULLAI SWAMI** | **20AK1A0564** |
| **PONNAGANTI KULADEEP CHOWDARY** | **21AK5A0512** |
| **MANCHURI LAKSHMI VARA PRASAD** | **21AK5A0514** |
| **BUDDALA REDDY SHEKAR REDDY** | **20AK1A05B7** |

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

Identity Based Encryption (IBE) is an extension of public-key encryption (PKE) that can use the user’s identity string as a public key. The first IBE scheme was proposed earlier, and they constructed their IBE scheme by using a bilinear map and proved its security in the random oracle model. Since then, various IBE schemes have been proposed in bilinear maps. In order to use an IBE scheme in a real application environment, an Revocable IBE scheme that provides the functionality of effectively revoking a user’s private key is required. Various RIBE schemes have been proposed to enhance the security or improve the performance.

### 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](#_TOC_250017)

[List of Figures **v**](#_TOC_250016)

[Chapter 1. Introduction 01](#_TOC_250015)

* 1. Problem Statement 01
  2. [Problem Definition 01](#_TOC_250014)
  3. [Expected Outcomes 01](#_TOC_250013)
  4. [Organization of the Report 02](#_TOC_250012)

[Chapter 2. Literature Survey 03](#_TOC_250011)

* 1. Paper- 1 03

[Chapter 3. Proposed Methodology 05](#_TOC_250010)

* 1. [System Design 05](#_TOC_250009)
  2. [Modules used 06](#_TOC_250008)
  3. Data Flow Diagrams (DFD) 07
  4. [Advantages 09](#_TOC_250007)
  5. Requirement Specifications 09

Chapter 4. Implementation and Results 11

* 1. [System Implementation 11](#_TOC_250006)
  2. [Testing and Validation 12](#_TOC_250005)
  3. [Results and Findings 13](#_TOC_250004)

[Chapter 5. Conclusion 17](#_TOC_250003)

[GitHub Link 18](#_TOC_250002)

[Video Link 1](#_TOC_250001)8

[References](#_TOC_250000) 19

# 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 |

* 1. **Problem Statement:**

# CHAPTER 1 INTRODUCTION

In contemporary cloud computing paradigms, data sharing among groups of users is vital for collaboration, decision-making, and innovation across various industries such as healthcare, finance, and collaborative research. However, ensuring the security and efficiency of group data sharing in the cloud poses significant challenges due to concerns regarding data privacy, scalability, and access control.

## Problem Definition:

# In this project, we examine a way to make a decryption key greater effective inside the experience that it permits decryption of more than one cipher texts, without growing its size. specifically, our trouble assertion is “To design an green public-key encryption scheme which helps flexible delegation within the experience that any subset of the cipher texts (produced by means of the encryption scheme) is decry table through a regular-length decryption key (generated by the proprietor of the grasp-secret key).” We remedy this hassle via introducing a special form of public-key encryption which we name key-combination cryptosystem (KAC). In KAC, customers encrypt a message no longer best below a public-key, however also underneath an identifier of cipher text called elegance. Meaning the cipher texts are in addition categorized into one-of-a-kind training. The important thing proprietor holds a master-secret known as grasp-mystery key, which can be used to extract mystery keys for exclusive classes. Extra importantly, the extracted key have can be an aggregate key that's as compact as a mystery key for a single elegance, but aggregates the electricity of many such keys, i.e., the decryption power for any subset of cipher text classes.

## Expected Outcomes:

Group data sharing in cloud computing with Identity-Based Encryption (IBE) can yield several expected outcomes, which are advantageous for organizations and users engaging in collaborative activities. Here are some of the expected outcomes:

**Enhanced Security**: IBE ensures that data shared among group members is encrypted and accessible only to authorized users with the corresponding private keys. This enhances the security of sensitive information, reducing the risk of unauthorized access, data breaches, and leakage of confidential data.

**Improved Access Control**: Group data sharing with IBE allows for fine-grained access control, enabling administrators to define access policies based on users' identities or attributes. This ensures that only authorized individuals or groups can access specific data, reducing the risk of insider threats and unauthorized data access.

**Streamlined Key Management**: IBE simplifies key management by eliminating the need for a traditional public key infrastructure (PKI). Keys can be generated dynamically based on users' identities, reducing the overhead associated with key distribution and management. This streamlines the process of granting and revoking access to shared data.

## Organization of the Report:

This report explores the implementation of group data sharing on Identity-Based Encryption (IBE). IBE is a cryptographic primitive that allows users to encrypt data for a group based on their identities, rather than public keys. Group data sharing on IBE enables secure and efficient sharing of data within a designated group.

# CHAPTER 2 LITERATURE SURVEY

* 1. **Paper – 1:** J. H. Seo and K. Emura, ‘‘Revocable identity-based encryption revisited: Security model and construction,’’ in Public-Key Cryptography—PKC 2013, vol. 7778. Berlin, Germany: Springer, 2013, pp. 216–234.

### Brief Introduction of Paper:

### The paper titled "Revocable identity-based encryption revisited: Security model and construction" authored by J. H. Seo and K. Emura was presented at the Public-Key Cryptography—PKC conference in 2013. In this paper, the authors revisit the concept of revocable identity-based encryption (RIBE) and propose a new security model and construction for it. The aim of the paper is to enhance the security and practicality of RIBE schemes. It was published as part of the conference proceedings by Springer in Berlin, Germany, in Volume 7778, with the paper spanning pages 216–234.Throughout the paper, Seo and Emura provide a thorough examination of the security aspects of RIBE, including the identification of potential vulnerabilities and the development of countermeasures. By revisiting and enhancing the security model, they contribute to the advan cement of RIBE schemes, making them more robust and practical for real-world applications.

### 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 Weather Master application, such as displaying weather forecasts, current conditions, and user interfaces for interacting with the 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 weather data, including rigorous testing against ground truth observations and implementing predictive algorithms to improve forecast accuracy.
      * **Cross-Browser Compatibility and Mobile Responsiveness:** Testing the app across various web browsers and devices to ensure consistent performance and user experience, and applying responsive design principles to adapt the app's 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 app's user interface design, navigation, and presentation of weather data to ensure an intuitive and seamless user experience.

# CHAPTER 3 PROPOSED METHODOLOGY

## System Design:

1. **User Interface:**
   * The user interface of Weather Master App is designed to be accessible and easy to navigate.
   * Weather Master is a handy application that helps you stay updated on the weather conditions in your area or any location of interest.
   * With its user-friendly interface, you can quickly check the current weather

## Refine UI/UX:

* + Evaluate and redesign the user interface for a seamless and visually appealing experience.

## Mobile Responsiveness:

* + Implement responsive design practices to ensure compatibility with different devices.

## Security Enhancement:

* + Implement responsive design practices to ensure compatibility with different devices.

## Data Validation:

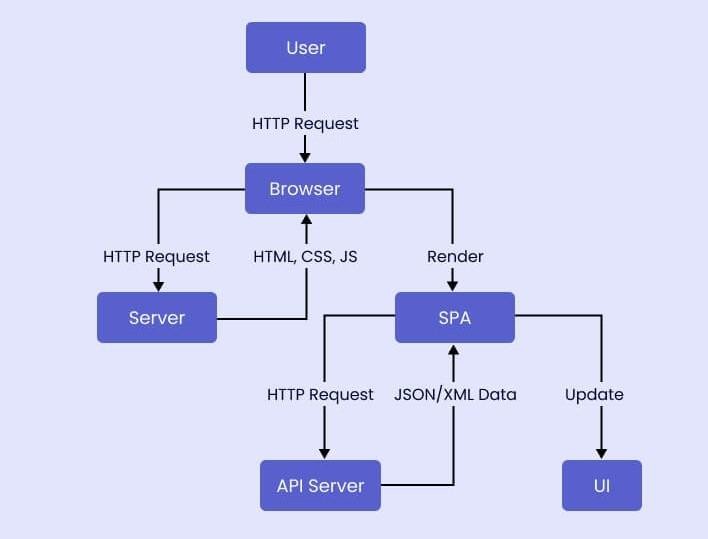
* + Implement responsive design practices to ensure compatibility with different devices.

## Optimize Performance:

* + Assess and enhance application speed and responsiveness, focusing on real-time weather data handling.

## Cross-Browser Compatibility:

* + Test and address any compatibility issues across various web browsers.



## Figure 1: System Design

## Modules Used:

**1 Setup segment**

The setup calculation takes no information beside the understood wellbeing parameter. It yields the overall population parameters PK and a grip key MK.

**2.Encrypt segment**

Scramble (PK, M, A). The encryption calculation takes as enter general society parameters PK, a message M, and an inspire admission to shape An over the universe of characteristics. The calculation will encode M and pass on a figure content CT such that just a client that has a settled of traits that satisﬁes the motivate admission to shape will have the capacity to decode the message. We can expect that the figure message verifiably incorporates A.

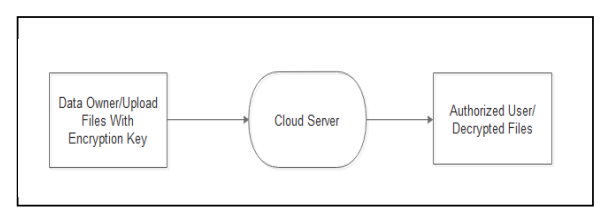
**3. Key Gen stage :**

Decode (PK, CT, and SK). The unscrambling calculation takes as enter the overall population parameters PK, a figure content CT, which incorporates a get right of section to strategy An, and a private key SK, that is a private key for a settled S of traits. On the off chance that the set S of properties satisﬁes the get right of passage to structure A then the calculation will decode the figure message and retreat a message M.

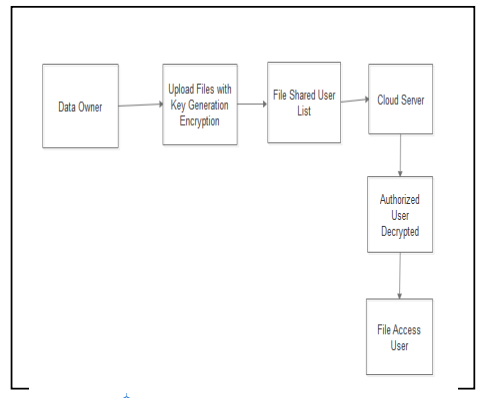
## Data Flow Diagram:

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).

* + 1. **DFD Level 0**



* + 1. **DFD Level 1 –**



## Advantages:

The identity based encyption 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.
  1. **Requirement Specification:**
     1. **Hardware Requirements:**
        1. **Processor Requirement**:
           + Intel Core i5/i7 or AMD equivalent

## RAM Requirement:

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

## 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.

## 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

## 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.

### 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

### Design Phase:

The design page for the implementation of group data sharing in cloud computing with Identity-Based 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 implementationprocess.

### 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.

### 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.

## Testing and Validation:

Testing and validation are crucial stages in the development lifecycle of the project, ensuring that the application meets the specified requirements, functions as intended, and delivers a seamless user experience. The testing process encompasses various techniques and methodologies to identify and address any issues, bugs, or discrepancies in the application's functionality, usability, and performance.

### Functional Testing:

Verify that all features, such as real-time weather updates, social sharing, and accessibility options, function as intended under various scenarios and user inputs.

1. **Performance Testing:** Evaluate the app's responsiveness, load times, and resource utilization to guarantee optimal performance, especially during peak usage or adverse weather conditions.
   * Performance testing evaluates the responsiveness, scalability, and stability of the Weather Master application under different load conditions and usage

scenarios. Testers measure key performance metrics, such as response times, throughput, and resource utilization, to assess the application's performance characteristics.

* + Load testing, stress testing, and scalability testing are performed to determine the application's ability to handle concurrent user sessions, peak loads, and scalability requirements. Performance bottlenecks and optimization opportunities are identified and addressed to improve the application's responsiveness and reliability.

## Results and Findings:

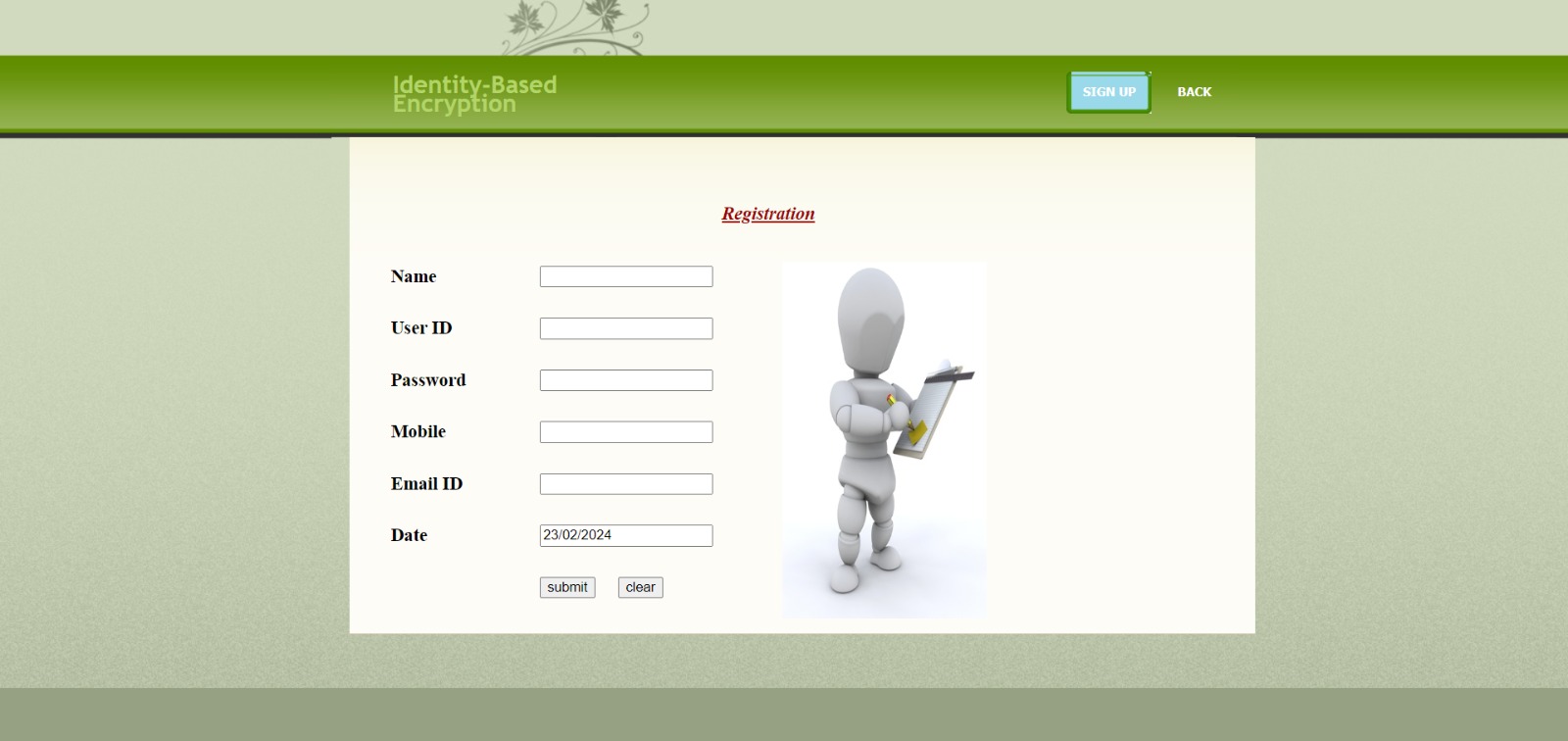
* + 1. **Results:**

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

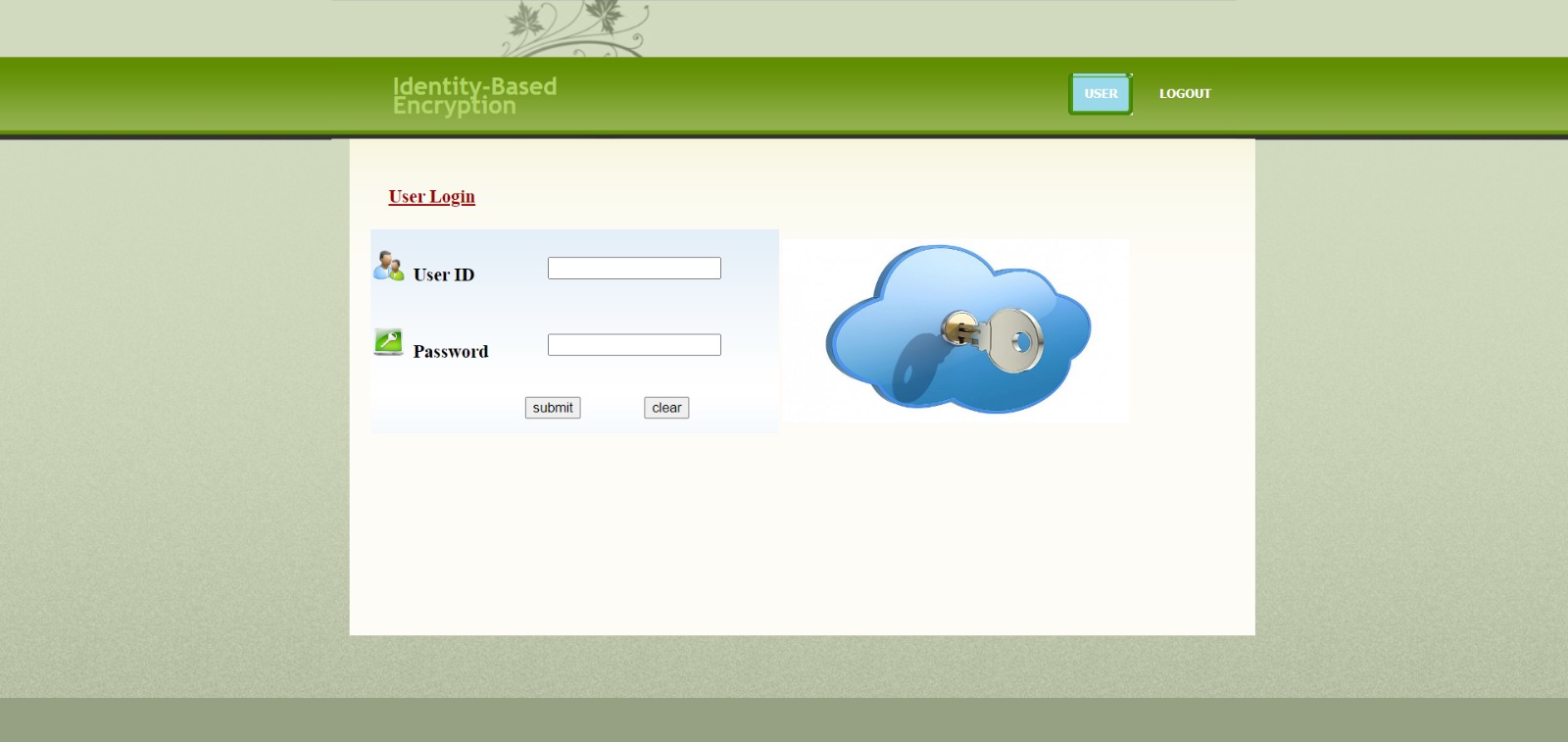
**Granular Access Control**: Data can be encrypted for specific groups or users within a group, ensuring only authorized members can access it. This is particularly beneficial for sensitive data.

**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.

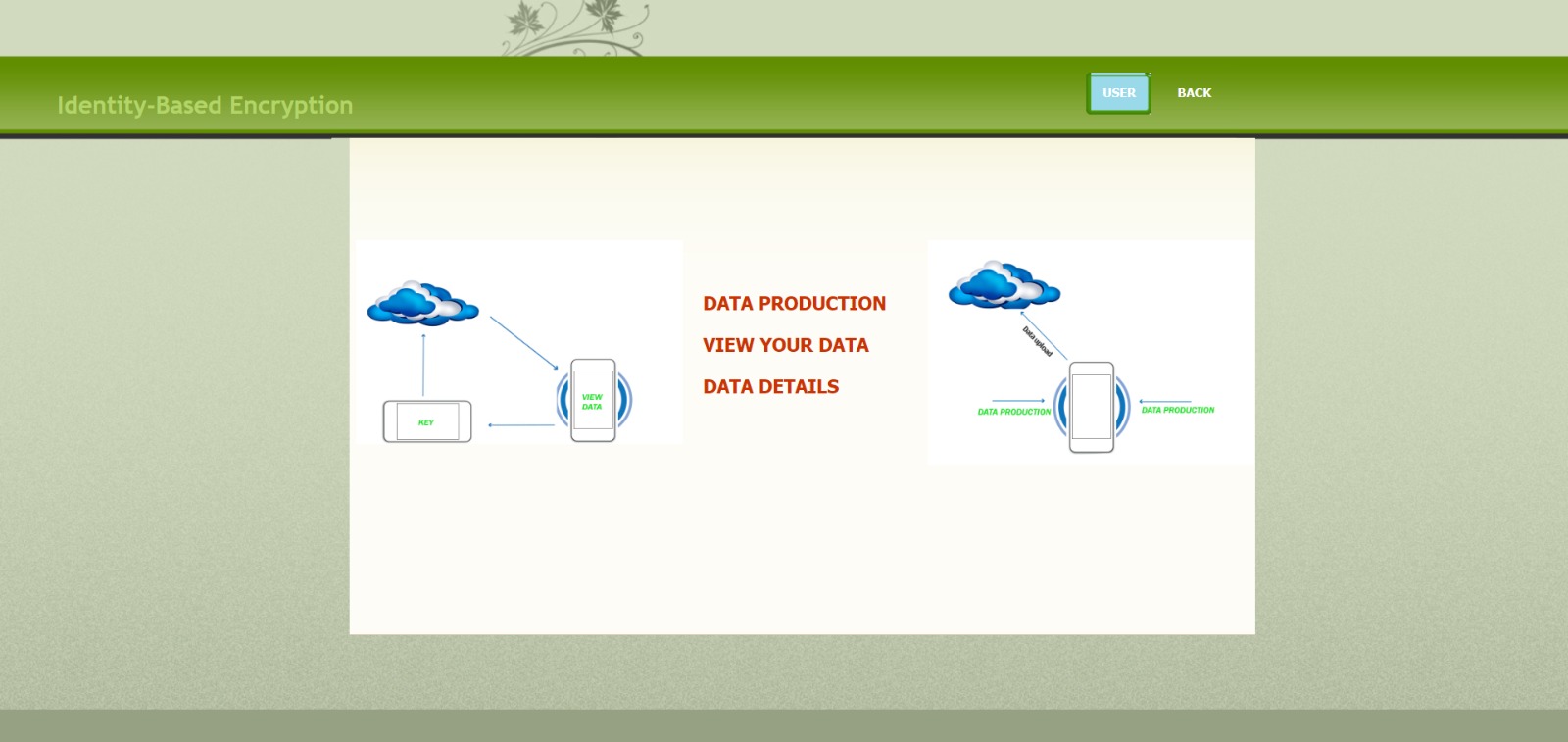
**Efficient Revocation**: Revoking access for compromised or departed members becomes easier as keys are tied to identities, not public keys. This ensures data security even when user credentials arecompromised.



**Figure 1:** Registrartion page



**Figure 2:** Login Page



**Figure 3**:User page

## 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

In conclusion, the implementation of group data sharing in cloud computing using Identity-Based Encryption (IBE) offers a secure and efficient solution for organizations to collaborate and share sensitive information within user groups. Overall, the implementation of group data sharing in cloud computing with Identity-Based Encryption has been successful in meeting the objectives of the project, providing a secure, efficient, and user-friendly solution for organizations to collaborate and share data within user groups. As technology continues to evolve, ongoing efforts to improve and innovate in this area will further enhance the capabilities and benefits of group data sharing in cloud computing environments.

## SCOPE:

The most effective method to ensure clients' information protection is a focal inquiry of distributed storage. With more scientific apparatuses, cryptographic plans are getting more adaptable and regularly include different keys for a solitary application. In this article, we consider how to "pack" mystery keys out in the open key cryptosystems which bolster assignment f mystery keys for distinctive cipher text classes in distributed storage. Regardless of which one among the force set of classes, the delegate can simply get a total key of consistent size. Our methodology is more adaptable than various leveled key task which can just spare spaces if every single key-holder share a comparable arrangement of benefits. A confinement in our work is the predefined bound of the quantity of most extreme cipher text classes. In distributed storage, the quantity of cipher texts more often than not becomes quickly. So we need to save enough cipher text classes for the future expansion. Else, we have to grow people in general key as we depicted.

# GITHUB LINK

<https://github.com/20AK1A0564/Identity-Based-Encryption.git>

# VIDEO LINK

<https://drive.google.com/file/d/1OqCnpuI0t7qvB_H92w8y80SNcYi7JYPx/view?usp=sharing>

# REFERENCES

[1]. J. H. Seo and K. Emura, ‘‘Revocable identity-based encryption revisited: Security model and construction,’’ in Public-Key Cryptography—PKC 2013, vol. 7778. Berlin, Germany: Springer, 2013, pp. 216–234.

[2]. A. Boldyreva, V. Goyal, and V. Kumar, ‘‘Identity-based encryption with efficient revocation,’’ in Proc. 15th ACM Conf. Comput. Commun. Secur., Oct. 2008, pp. 417–426.

[3]. B. Libert and D. Vergnaud, ‘‘Adaptive-ID secure revocable identity-based encryption,’’ in Topics in Cryptology—CT-RSA 2009, vol. 5473. Berlin, Germany: Springer, 2009, pp. 1–15.

[4 J. H. Seo and K. Emura, ‘‘Revocable identity-based encryption revisited: Security model and construction,’’ in Public-Key Cryptography—PKC 2013, vol. 7778. Berlin, Germany: Springer, 2013, pp. 216–234.

[5] S. Park, K. Lee, and D. H. Lee, ‘‘New constructions of revocable identitybased encryption from multilinear maps,’’ IEEE Trans. Inf. Forensics Security, vol. 10, no. 8, pp. 1564–1577, Aug. 2015