A Unified Hierarchical Key Assignment Scheme for Enhanced Scalability and Efficiency

[1]Dr. R. HAMSAVENI, [2]Chavvakula Suresh, [3]Pegada Venkata Sai Teja, [4]Chandu bala venkata Dilli, [5]k.hari manikanta

[1]*.HOD & Professor/MCA, Sri Venkateswara College of Engineering and Technology (Autonomous) Chittoor, Andhra Pradesh-517217

[2,3,4] MCA Students, Sri Venkateswara College of Engineering and Technology (Autonomous) Chittoor, Andhra Pradesh-517217

Abstract*— This study presents a hierarchical key assignment scheme (HKAS) built on the closest vector problem in an inner product space (CVP-IPS). The proposed scheme delivers a scalable, flexible, cost-effective, and high-performance solution. Key features include a CVP-IPS-based construction, the use of two public keys, a unique basis set assigned to each class, a direct access mechanism for enhanced user convenience, and a thorough mathematical and algorithmic framework detailing all processes. Unlike traditional top-down approaches, this scheme avoids hierarchical dependencies, ensuring uniform basis set lengths and consistent key derivation costs across all classes. This design significantly reduces the overhead typically incurred by higher classes in conventional structures. With its ability to support both vertical and horizontal scalability through the use of access graphs, the scheme is proven to achieve strong key indistinguishability security (S-KI-security). This research marks a substantial advancement in HKAS systems, offering improved efficiency, robust security, and practical benefits for diverse applications.

1. INTRODUCTION

A Unified Hierarchical Key Assignment Scheme is designed to enhance the scalability and efficiency of secure access control in large-scale systems. Traditional key management approaches often struggle with increasing computational and storage of overhead as the number of users and access levels grows. This scheme introduces a structured, hierarchical approach where cryptographic keys are assigned in a way that optimizes both security and resource utilization. By leveraging a unified framework, it ensures that users at different levels of the hierarchy can efficiently derive the necessary keys without

2. RELATED WORK

Title: "A Hierarchical Key Assignment Scheme: A Unified Approach for Scalability and Efficiency

Author: Ibrahim Celikbilek, Baris Celiktas, and Enver Ozdem

Publication : IEEE

Description:
is study introduces a hierarchical key assignment scheme (HKAS) based on the closest vector problem in an inner product space (CVP-IPS). The proposed scheme aims to enhance scalability and efficiency in secure access control systems by leveraging mathematical structures to optimize key distribution and managemen.

Title: "Efficient and Scalable Hierarchical Key Assignment Schemeand data sets,"

Author: M.-L. Zhang

Publication : IEEE

Description:
This paper proposes an efficient and scalable hierarchical key assignment scheme that operates without the need for tamper-resistant devices. The scheme allows users to select their own passwords as secret keys, with the trusted authority generating corresponding masks for subordinates and publishing them on an authenticated public board. This approach facilitates secure key derivation and management in hierarchical structures.

Title: Efficient Provably-Secure Hierarchical Key Assignment Schemes

Author: A. Habib, J. Ashraf

Publication : IEEE

Description:
He authors design and analyze hierarchical key assignment schemes that are both provably secure and efficient. They focus on key indistinguishability, ensuring that adversaries cannot derive unauthorized keys. The proposed constructions support dynamic updates to the hierarchy with localized changes to public information, eliminating the need for redistributing private information.

Title: A Novel Hierarchical Key Assignment Scheme for Data Access Control in the Internet of Things

Author: D. Fryer, I. Str¨umke,

Publication: IEEE

Description:
This paper presents a hierarchical key assignment scheme based on multilinear maps to address multigroup access control in IoT data sharing. The scheme aims to provide a flexible and secure method for managing data access across multiple groups within IoT environments, enhancing both scalability and efficiency.

Title: A Hierarchical Key Assignment Scheme: A Unified Approach for Scalability and Efficiency,

Author: J. L. Godwin,

Publication: IEEE

Description:
This study introduces a hierarchical key assignment scheme (HKAS) based on the closest vector problem in an inner product space (CVP-IPS). The scheme is designed to enhance scalability and efficiency in secure access control systems by utilizing mathematical structures to optimize key distribution and management.

3. RESEARCH METHODOLOGY

3.1 PROBLEM DEFINITION

The scheme integrates advanced encryption techniques and access control policies to dynamically generate and distribute keys based on predefined authorization levels. This approach significantly improves scalability, as it reduces the number of keys each entity must store, making it ideal for large-scale applications such as cloud computing, IoT networks, and enterprise security frameworks.
To further enhance efficiency, the system optimizes key derivation mechanisms, ensuring minimal computational complexity while maintaining strong security guarantees. Additionally, it incorporates mechanisms for efficient key revocation and updates, preventing unauthorized access when permissions change.

ADVANTAGES OF PROPOSED SYSTEMS

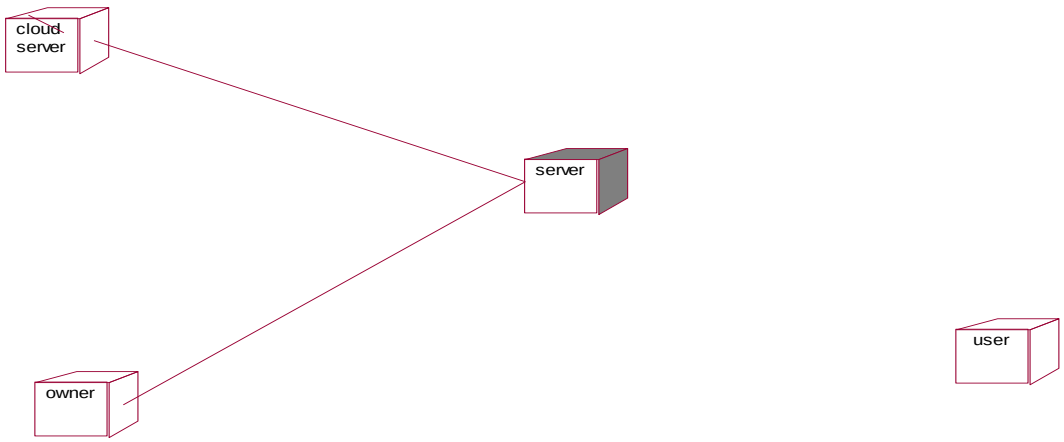
flexible, scalable, and secure key management framework that adapts to dynamic environments, ensuring seamless and efficient access control in large and complex systems.

ALGORITHM

Triple DES Algorithm
In the field of cryptography, Triple DES (3-DES) is a symmetric-key block cypher that encrypts each data block three times using the Data Encryption Standard (DES) encryption algorithm.
After 1990, users of DES started to feel uneasy about the speed of exhaustive key searches against DES. Users did not wish to replace DES, however, because it is very expensive and time-consuming to update widely used encryption algorithms that are built into complex security structures. Instead of fully giving up on the DES, the realistic approach called for changing how it is used. As a result, Triple DES' modified schemes were created (sometimes known as 3DES).
The 3-key Triple DES (3TDES) and the 2-key Triple DES are two different versions of Triple DES (2TDES). Although triple DES systems are visibly slower than single DES, they are noticeably more secure than single DES.

DEPLOYMENT DIAGRAM

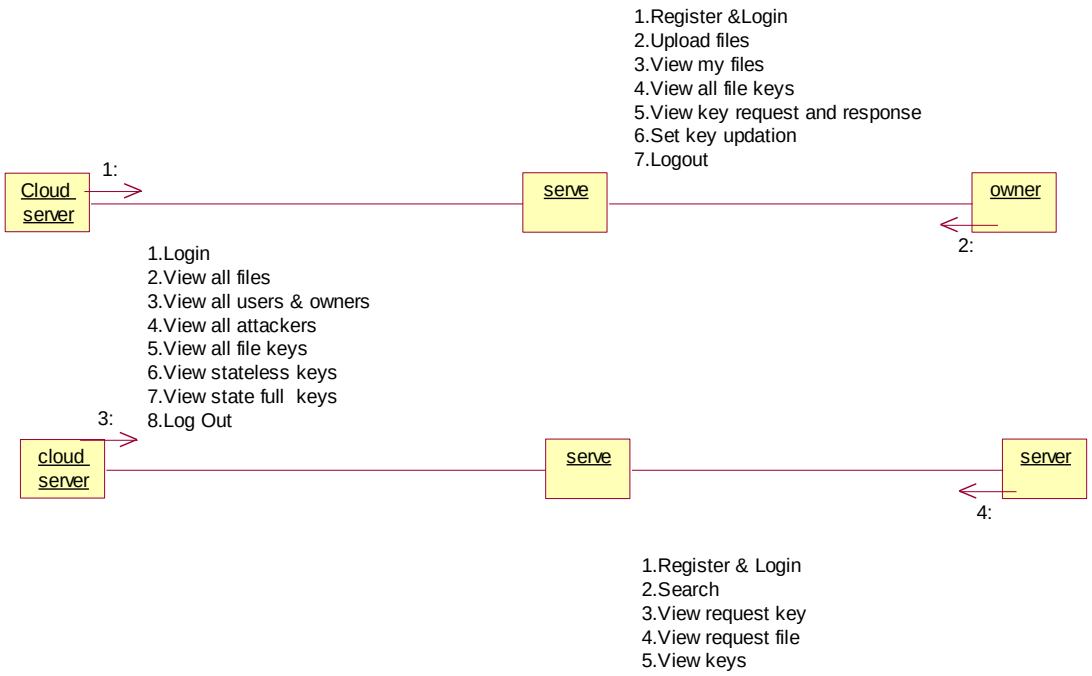
Deployment diagram represents the deployment view of a system .It is related to the Component diagram. Because the components are deployed using the deployment diagrams. A deployment diagram consists of nodes. Nodes are nothing but physical Hardware’s used to deploy the Applications.



Deployment Diagram

COLLABORATION DIAGRAM

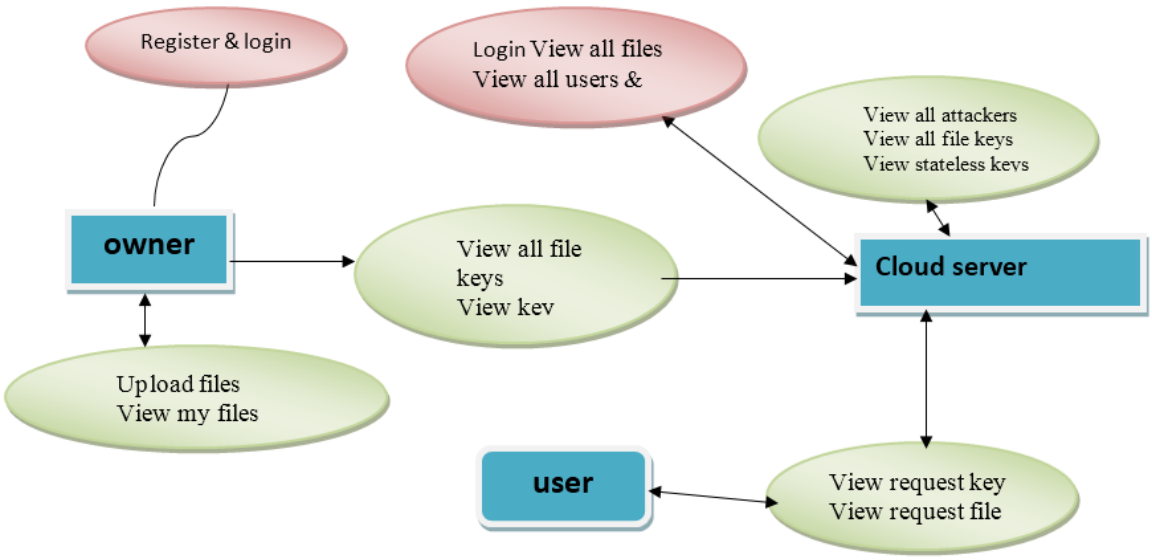
A collaboration diagram, also known as a communication diagram, is an illustration of the relationships and interactions among software objects in the Unified Modeling Language (UML). These diagrams can be used to portray the dynamic behavior of a particular use case and define the role of each object.



Collaboration Diagram

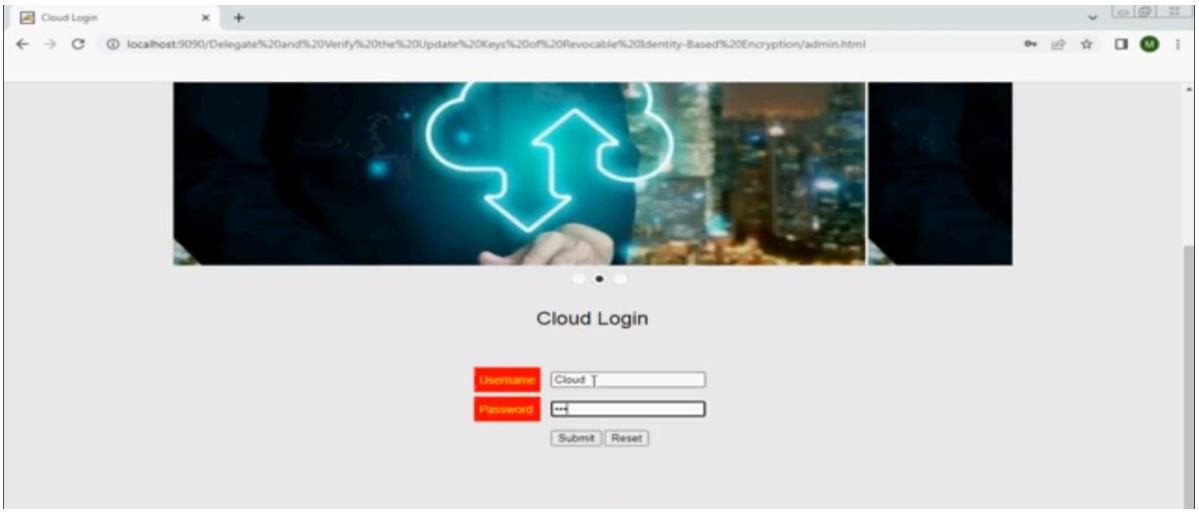
DATA FLOW DIAGRAM (DFD)

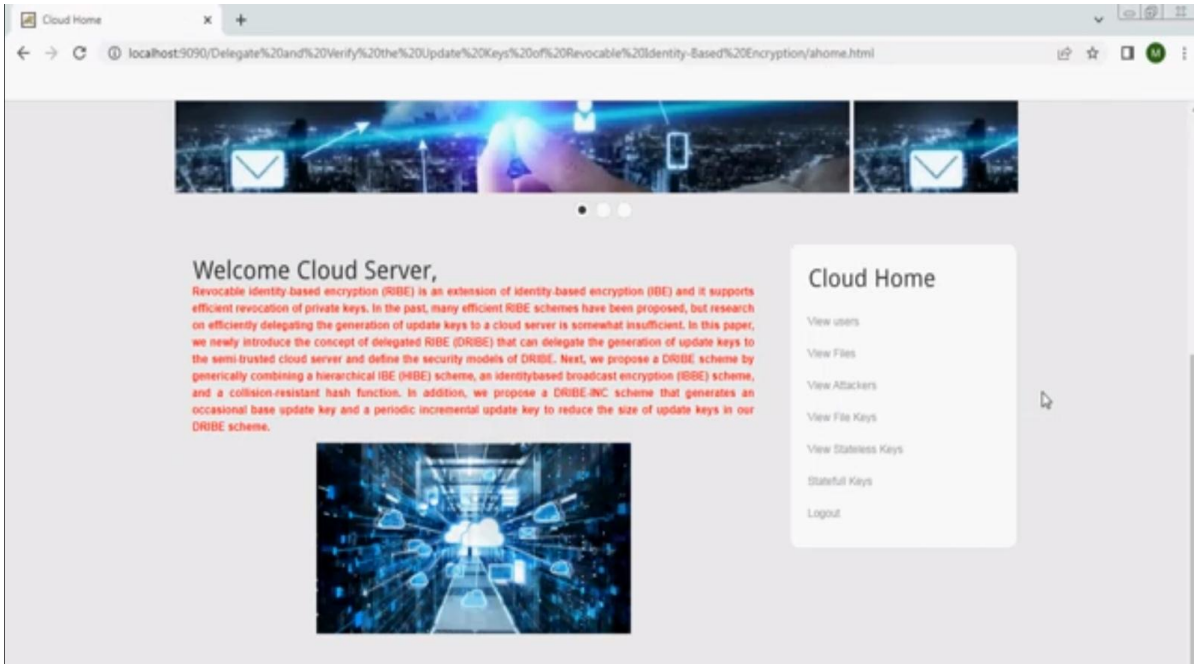
A Data Flow Diagram (DFD) is a traditional way to visualize the information flows within a system. A neat and clear DFD can depict a good amount of the system requirements graphically. It can be manual, automated, or a combination of both. It shows how information enters and leaves the system, what changes the information and where information is stored. The purpose of a DFD is to show the scope and boundaries of a system as a whole. It may be used as a communications tool between a systems analyst and any person who plays a part in the system that acts as the starting point for redesigning a system.

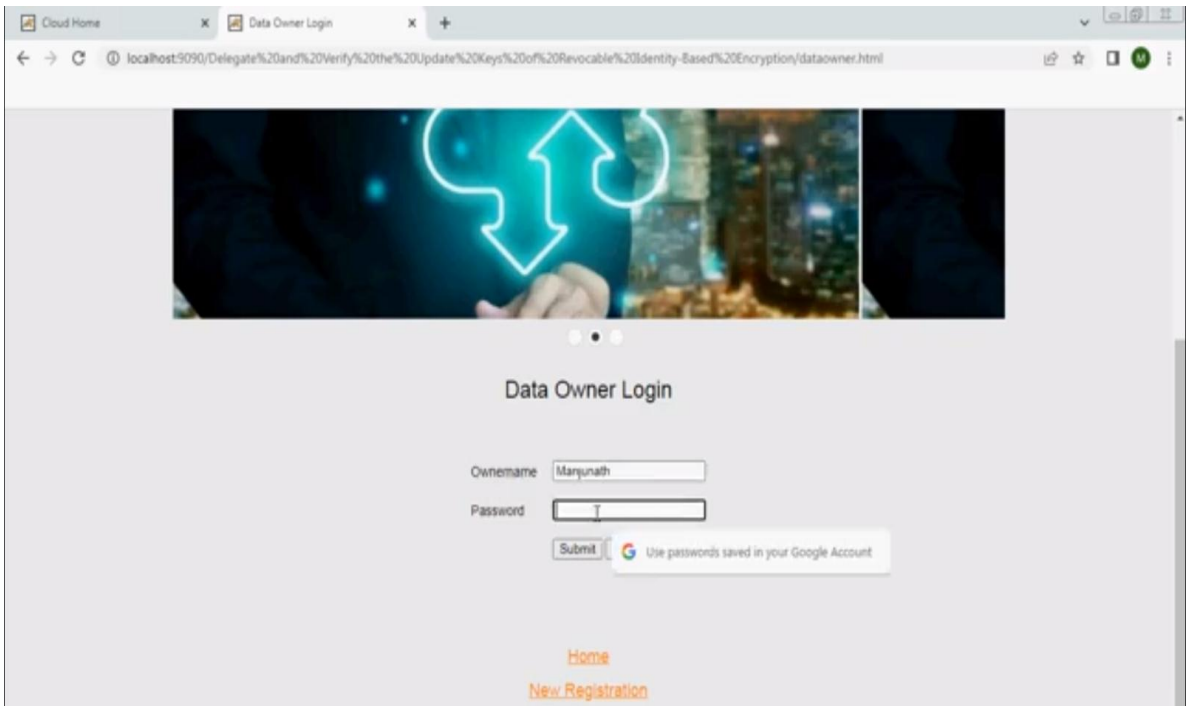


EXPECTED OUTCOMES

The expected outcome for flexible identity-based encryption (IBE) hinging on authorizing and confirming key alterations would involve advancements in cryptographic techniques that provide enhanced security, usability, and flexibility in managing encryption keys based on user identities. Here are potential outcomes By integrating mechanisms for authorizing and confirming key alterations, flexible identity-based encryption can strengthen security against unauthorized access and key tampering. This includes protecting against insider threats, unauthorized key revocation, and unauthorized key updates. Flexible IBE allows for fine-grained access control based on user identities, roles, or attributes. By incorporating authorization mechanisms for key alterations, organizations can exert greater control over who can modify encryption keys, ensuring that only authorized personnel can make changes. Simplifying the process of authorizing and confirming key alterations can enhance the usability of identity-based encryption systems, reducing the burden on administrators and end-users. This includes streamlined workflows for key management, efficient key update procedures, and user-friendly interfaces for managing encryption keys.







REFERENCES

[1] D. Boneh and M. K. Franklin, ‘‘Identity-based encryption from the Weil pairing,’’ in *Advances in Cryptology—CRYPTO 2001*, vol. 2139. Berlin, Germany: Springer, 2001, pp. 213–229.

[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.

[6] K. Lee, D. H. Lee, and J. H. Park, ‘‘Efficient revocable identity-based encryption via subset difference methods,’’ *Des., Codes Cryptogr.*, vol. 85, no. 1, pp. 39–76, Oct. 2017.

[7] Y. Watanabe, K. Emura, and J. H. Seo, ‘‘New revocable IBE in primeorder groups: Adaptively secure, decryption key exposure resistant, and with short public parameters,’’ in *Topics in Cryptology—CT-RSA 2017*, vol. 10159. Berlin, Germany: Springer, 2017, pp. 432–449.

[8] J. H. Seo and K. Emura, ‘‘Efficient delegation of key generation and revocation functionalities in identity-based encryption,’’ in *Topics in Cryptology—CT-RSA 2013*, vol. 7779. Berlin, Germany: Springer, 2013, pp. 343–358.

[9] G. Ryu, K. Lee, S. Park, and D. H. Lee, ‘‘Unbounded hierarchical identity-based encryption with efficient revocation,’’ in *Information Security Applications—WISA 2015*, vol. 9503. Berlin, Germany: Springer, 2015, pp. 122–133.

[10] J. H. Seo and K. Emura, ‘‘Revocable hierarchical identity-based encryption: History-free update, security against insiders, and short ciphertexts,’’ in *Topics in Cryptology—CT-RSA 2015*, vol. 9048. Berlin, Germany: Springer, 2015, pp. 106–123.