**Three-Factor Authentication for Clouds**

## **1V Nitin, 2Yedla Devisri, 3Karthikeya Reddy Kotha, 4Aleti Anvesh, 5S.Yeswanth Kumar Reddy**

1Assistant Professor in the Department of IT MLR Institute of technology,Hyderabad, Telangana, India.

2,3,4.5 UG Scholar in Department of IT MLR Institute of technology,Hyderabad, Telangana, India.

**Abstract -** In the evolving landscape of cloud technology, services efficiently migrate, emphasizing the need for accessible and private services on public networks. This shift highlights three-factor Mutual Authentication and Key Agreement protocols for multi-server setups. However, many existing protocols lack formal security proof, making them vulnerable to attacks and incurring high computational and communication costs. Additionally, a common issue is the absence of a dynamic revocation mechanism in most three-factor MAKA protocols, leading to delayed revocation for malicious users. To address this, we propose a dynamic revocable three-factor MAKA protocol using Schnorr signatures for user management, providing formal security proof within the random oracle. Rigorous security analysis confirms its suitability for diverse multi-server environments, while performance analysis deems it fitting for resource-constrained smart devices. Comprehensive simulation implementation substantiates the proposed protocol's feasibility and efficacy, contributing to enhancing security and efficiency in cloud-based services by addressing critical shortcomings in existing protocols.

**Keywords**: Evolving cloud services,Three-factor authentication,Formal security analysis,Dynamic revocation,Computational Efficiency,Schnorr signatures.

**1. INTRODUCTION**

## **Introduction**

In recent years, the transformative evolution of cloud computing has significantly enhanced service reliability and efficiency, prompting a substantial migration to cloud platforms. This shift, driven by the dual objectives of ensuring convenient service access and fortifying communication privacy on public networks, has brought multi-server architectures, particularly three-factor Mutual Authentication and Key Agreement (MAKA) protocols, into the spotlight. Despite their widespread use, these protocols grapple with critical challenges, lacking formal security proofs and an efficient dynamic revocation mechanism, resulting in delays in access revocation. To address these issues, this paper introduces a groundbreaking solution: a provable dynamic revocable three-factor MAKA protocol. Leveraging Schnorr signatures and providing formal security proof within the random oracle, the protocol showcases adaptability in multi-server environments. Additionally, performance analysis underscores its suitability for resource-constrained smart devices. Subsequent sections comprehensively explore the protocol's design intricacies, security considerations, and performance evaluations, affirming its efficacy in elevating the standards of security and efficiency in cloud-based services.

**Motivation of the Project:**

The project is motivated by the evolving landscape of cloud technology, emphasizing the need for secure and efficient multi-server setups. Existing Three-factor Mutual Authentication and Key Agreement (MAKA) protocols lack formal security proof, making them vulnerable and resource-intensive. The absence of a dynamic revocation mechanism in many protocols delays revocation for malicious users. To address these issues, the project proposes a dynamic revocable three-factor MAKA protocol using Schnorr signatures, providing formal security proof within the random oracle. The motivation is to enhance security and efficiency in cloud-based services by addressing critical shortcomings in existing protocols.

**Problem Statement:**

Due to the limitations of existing Three-factor Mutual Authentication and Key Agreement (MAKA) protocols within the evolving cloud technology landscape. Specifically, these protocols lack formal security proof, rendering them susceptible to vulnerabilities and incurring high computational and communication costs. Additionally, a common issue is the absence of a dynamic revocation mechanism, leading to delayed revocation for malicious users in multi-server setups. The project aims to rectify these shortcomings by proposing a dynamic revocable three-factor MAKA protocol using Schnorr signatures for user management. The overarching problem is to enhance the security and efficiency of cloud-based services by providing a robust protocol that addresses these critical issues.

**2. Literature Survey**

**2.1 Multi-Server Password Authenticated Key Agreement Scheme using smart cards with access control.**

**Chin-Chen Chang (2004)**

As a password-authenticated key agreement scheme utilizing smart cards with access control, this solution addresses the growing trend of remote computer access facilitated by the rapid advancements in science and technology. Consequently, the importance of user authentication and key agreement has escalated significantly. These elements are crucial not only to validate the legitimacy of users but also to ensure the security of subsequent communications. In the online environment, each server typically offers a range of services, some of which may not be accessible to every user. Therefore, effective access management is essential in multi-service settings.

**2.2 An Enhanced and Provably Secure Chaotic Map-Based Authenticated Key Agreement in Multi-Server Architecture**

**Azeem Irshad**

The Multi-Server Authentication (MSA) paradigm, where subscribers access multiple services from various providers after registering with a central authority, introduces a novel approach to simplify user experience. This method requires only one password for all service providers, thereby alleviating the burden of individual registrations on servers. Despite the convenience offered by MSA, several schemes exhibit drawbacks, prompting the need for improvement. Irshad's work specifically addresses these challenges, focusing on enhancing both the security and usability aspects of Multi-Server Authentication within multi-server architectures.Irshad's research emphasizes the incorporation of a Chaotic Map-Based Authenticated Key Agreement to bolster the security of MSA protocols. By leveraging chaotic maps, the proposed approach aims to enhance the cryptographic strength of key agreements, providing a provably secure foundation for multi-server authentication. This work not only contributes to the advancement of MSA protocols but also aims to mitigate existing vulnerabilities and usability concerns in the context of multi-server architectures.

**2.3 Security analysis and improvement of user authentication framework for cloud computing**

**N Chen**

Study critically examines the security challenges inherent in cloud computing, focusing on an existing user authentication framework. Identifying security vulnerabilities, the research introduces an improved user authentication scheme with a primary emphasis on user legitimacy verification for enhanced confidentiality and mutual authentication. The security of this proposed scheme is formally validated using the strand space model theory and authentication test method. Simulations complement these validations by demonstrating the scheme's efficient communication performance, providing a comprehensive evaluation of its real-world applicability. This work stands as a significant contribution to the field, advancing the security aspects of cloud computing through a robust user authentication approach.

**3. OVERVIEW OF THE SYSTEM**

## **Existing System**

In the evolving landscape of cloud computing, services are moving to cloud platforms for enhanced reliability and efficiency. To ensure easy and secure access to these services, especially over public networks, Three-factor Mutual Authentication and Key Agreement (MAKA) protocols for multi-server setups have become crucial. However, the complexity of these setups demands a more dynamic approach. In response, this research introduces a new Three-factor MAKA protocol using Schnorr signatures, offering enhanced security and efficiency. The protocol is designed for multi-server environments and resource-constrained devices, contributing to safer and more efficient cloud-based services.

**3.2 Proposed System**

To enhance the security and efficiency of cloud-based services, this research proposes a dynamic revocable Three-factor Mutual Authentication and Key Agreement (MAKA) protocol. The current reliance on Three-factor MAKA protocols in multi-server setups sets the backdrop for our innovation. Leveraging Schnorr signatures and providing formal security proof in the random oracle model, our protocol addresses security concerns while ensuring efficiency.

The proposed system introduces dynamism and revocability to the authentication process, offering an improved approach for secure communication across multiple servers. This protocol is especially designed to be efficient, making it suitable for resource-constrained devices like smart devices. Comprehensive simulation implementations validate the feasibility of our proposed protocol, showcasing its potential to significantly enhance the security and efficiency of cloud-based services.

**3.3 Proposed System Design**

We propose to decompose the proposed system architecture into five main modules:

1. User Module
2. User Registration
3. Login
4. Cloud Server
5. Admin

***3.3.1 User Module***

The User Module serves as the interface for individuals accessing cloud services. Users can efficiently manage their interactions with the cloud, ensuring seamless navigation and secure operations.

***3.3.2 User Registration***

User Registration provides a streamlined process for onboarding new users onto the cloud platform. This module allows individuals to create accounts securely, offering a foundation for personalized and secure interactions.

***3.3.3 Login***

The Login module facilitates user access to the cloud system. Through secure authentication mechanisms, users can enter the platform, ensuring the confidentiality and integrity of their data during login sessions.

***3.3.4 Cloud Server:***

The Cloud Server module forms the backbone of the system, hosting and managing services. It ensures reliable data storage, processing, and access for users, fostering a robust and scalable infrastructure for cloud-based operations.

***3.3.5 Admin***

The Admin module caters to system administrators, providing tools for overseeing and managing user accounts, security protocols, and overall system performance. Admins can efficiently monitor and control various aspects of the cloud environment to ensure optimal functionality and security.

**4 Architecture**

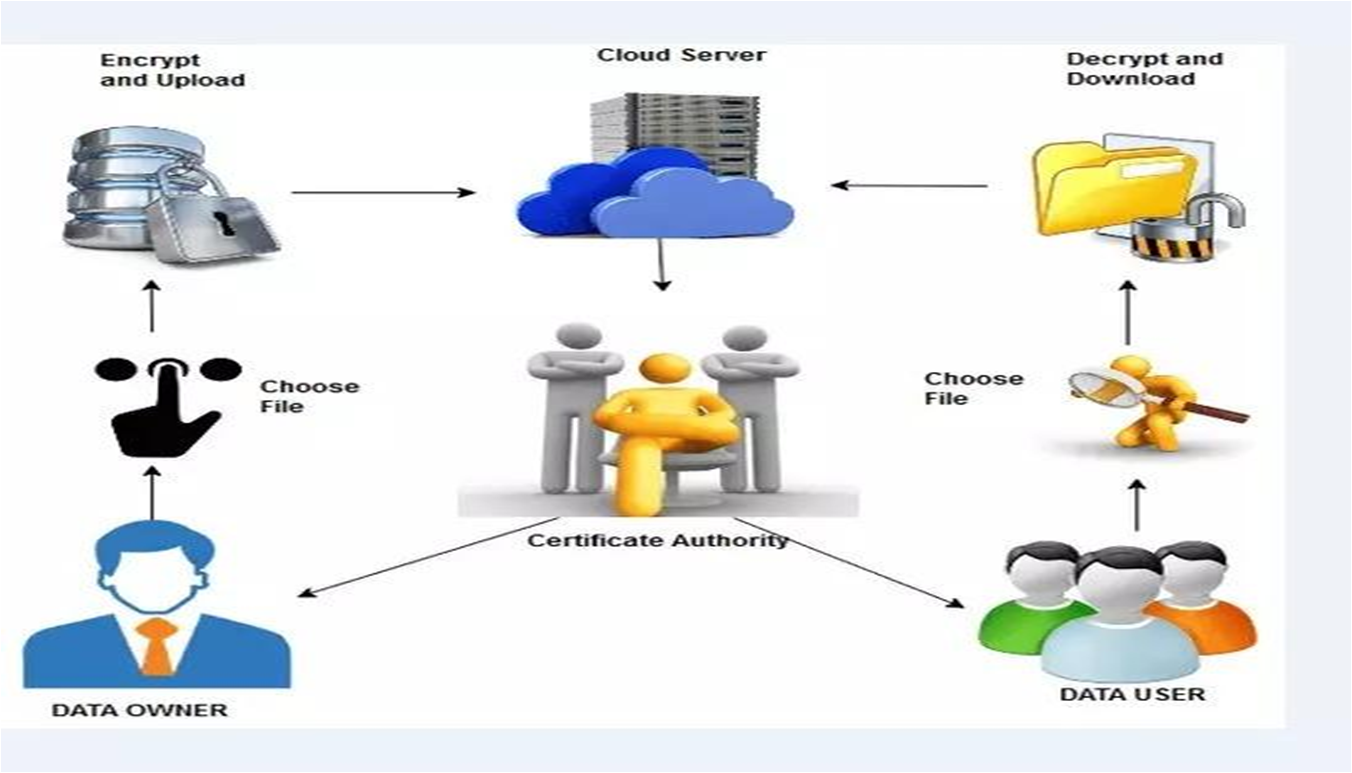
****

Fig 1: System Architecture

**5 RESULTS SCREENSHOTS**

## 