Marathwada Shikshan Prasarak Mandal’s

Deogiri Institute of Engineering and Management Studies,
Aurangabad

Project Report

on

Design Of Secure Authenticated Key Management Protocol For Cloud Computing Environments

Submitted By

Neha Sanjay Kumavat (46001)
Gayatri Ratan Puri (46069)
Mayuri Madhukarrao Kulkarni (46108)

Dr. Babasaheb Ambedkar Technological University
Lonere (M.S.)

Department of Computer Science and Engineering

Deogiri Institute of Engineering and Management Studies,
Aurangabad

(2022- 2023)

Project Report

on

Design of Secure Authenticated Key Management Protocol for Cloud Computing Environments

Submitted By

Neha Sanjay Kumavat (46001)

Gayatri Ratan Puri (46069)

Mayuri Madhukarrao Kulkarni (46108)

In partial fulfillment of

Bachelor of Technology

(Computer Science & Engineering)

Guided By

Dr. Pramod Bhalerao

Department of Computer Science & Engineering

Deogiri Institute of Engineering and Management Studies,

Aurangabad

(2022- 2023)

CERTIFICATE

This is to certify that, the Project entitled “ **Design of Secure Authenticated Key Management Protocol for Cloud Computing Environments** ” submitted by **Neha Sanjay Kumavat (46001), Gayatri Ratan Puri (46069), and Mayuri Madhukarrao Kulkarni (46108)** is a bonafide work completed under my supervision and guidance in partial fulfillment for award of Bachelor of Technology (Computer Science and Engineering) Degree of Dr. Babasaheb Ambedkar Technological University, Lonere.

Place: Aurangabad
Date: 24/12/2022

Dr. Pramod Bhalerao
Guide

Prof. S. B. Kalyankar
Head

Dr. Ulhas D. Shiurkar
Director,
Deogiri Institute of Engineering and Management Studies,
Aurangabad

DECLARATION

This is to certify that, the partial project report entitled , **“Design of Secure Authenticated Key Management Protocol for Cloud Computing Environments”** Submitted by Group Members is a bonafide work completed under my supervision and guidance in partial fulfillment for award of Bachelor degree in Computer Science and Engineering of Deogiri Institute of Engineering and Management Studies, Aurangabad under Dr. Babasaheb Ambedkar Technological University, Lonere.

Place: Aurangabad
Date:

Dr. Pramod Bhalerao
External Examiner Guide

ABSTRACT

With the maturity of cloud computing technology in terms of reliability and efficiency, a large number of services have migrated to the cloud platform. To convenient access to the services and protect the privacy of communication in the public network, three-factor Mutual Authentication and Key Agreement (MAKA) protocols for multi-server architectures gain wide attention. However, most of the existing three-factor MAKA protocols don't provide a formal security proof resulting in various attacks on the related protocols, or they have high computation and communication costs. And most of the three-factor MAKA protocols haven't a dynamic revocation mechanism, which leads to malicious users can not be promptly revoked.

To address these drawbacks, we propose a provable dynamic revocable three-factor MAKA protocol that achieves the user dynamic management using Schnorr signatures and provides a formal security proof in the random oracle. Security analysis shows that our protocol can meet various demands in the multi-server environments. Performance analysis demonstrates that the proposed scheme is well suited for computing resource constrained smart devices. The full version of the simulation implementation proves the feasibility of the protocol.

We propose a provable dynamic revocable three-factor MAKA protocol that achieves the user dynamic management provides a formal security proof in the random oracle. Security analysis shows that our protocol can meet various demands in the multi-server environments. Performance analysis demonstrates that the proposed scheme is well suited for computing resource constrained smart devices.

Contents

List Of Abbreviations

Sr.No	Acronym	Abbreviation
1	SRS	Software Requirement Specification.
2	SQL	Structured Query Language.
3	CSS	Cascading style sheet.
4	HTML	Hypertext Markup Language.
5	MAKA	Mutual Authentication and Key Agreement.
6	XML	Extensible markup language.
7	QR code	Quick Respose code
8	DFD	Data Flow Diagram.
9	RC	Registration Centre
10	OS	Operating System
11	MSA	MultiSserverAauthentication
12	UML	Use Case Diagram
13	SDLC	Software Development Life Cycle

List of Figures

List of Screens

1. INTRODUCTION

1.1 Introduction

In the recent decade, cloud computing technology has been completely commercialised. It can not only improve service efficiency but also reduce costs. More and more companies are putting their services on the cloud platform for development, management and maintenance. This not only reduces the local maintenance burden for these enterprises, but also provides unified security and operation management for all services on the third-party cloud platform, as shown in Fig. 1. Although third-party cloud platforms have more powerful technologies and more standard technical specifications to ensure that the servers run in a relatively secure environment, users and servers communicate in the public network. Therefore, authentication and key agreement are critical for the communication security. The use of mutual authentication and key agreement (MAKA) protocols not only prevent attackers from abusing server resources, but also prevent malicious attackers posing as the server to obtain the user's information. Therefore, the MAKA protocols have been extensively studied since Lamport proposed a password-based authentication protocol.

Cloud computing technology has reached full commercialization in the last decade. Because of this, it's capable of both increasing service efficiency and decreasing expenses. Cloud computing is being embraced by more and more businesses for application creation, administration, and maintenance. There is a significant reduction in the amount of time and resources needed to maintain the third-party cloud platform because of this, as illustrated in Fig.1. No matter how safe a platform's third party cloud services are, users and third-party cloud services interact over a public network, not the platform's private network. So authentication and key agreement are essential to the security of communication. In addition to preventing attackers from misusing server resources, mutual authentication and key agreement (MAKA) protocols also prohibit attackers masquerading as the server in order to acquire the user's information. Since Lamport introduced a password-based authentication mechanism, the MA- KA protocols have been widely explored. A single-server architecture was the focus of the earlier MAKA protocol. As the number of Internet users increases exponentially so has the number of cloud servers providing various services. If you're using a single server, you'll have a hard time remembering different passwords for each one. Many researchers have proposed more flexible MAKA protocols for multi-server settings to enhance user experience. Such protocols may be easily implemented when used in conjunction with the cloud platform's unified management capabilities. Users and cloud servers simply need to register at the registration centre (RC) for mutual authentication and key agreement in the protocols for the multi-server architecture model depicted. There are two types of MAKA protocols used in multi-server environments: identity-only MAKA protocols and identity-password-biometrics MAKA protocols. Identity-password-biometrics MAKA protocols use three factors: identity, password, and biometrics.

Password-based MAKA protocols, such as those in, are vulnerable to a variety of attacks, including the guessing password attack. As computer technology advances, the cost of a password guessing attack on a password-based system decreases. As an alternative, users often use passwords consisting of just letters or digits, and many people simply accept the device's default password when prompted to do so by their smart gadgets. A number of biometrics-based MAKA protocols have been suggested to deal with this issue. The three-factor MAKA protocols for multi server settings are more secure than the two factor protocols because of the uniqueness, availability, and non-transferability of biometrics keys (palm print, iris, finger print, etc.). Adversaries have complete access to wireless networks because of the openness of such systems. To thwart the aforementioned attacks, the MAKA protocols need anonymity and untraceability as well. The three-factor MAKA protocols now in use, however, have the following flaws.

1) Security vulnerabilities: Most of the existing MA- KA protocols based on the three factors haven’t a formal proof, but some informal security analysis. And some protocols embed insecure factors such as key authentication factors easily extracted. We will analyse such weaknesses in the security comparisons and cryptanalysis subsection.

2) Incomplete basic functions: Some important basic functions, such as dynamic user management, authentication phase without RC, are not considered in most MAKA protocols.

3) High cost: Some three-factor MAKA protocols didn’t take full account of their actual application environment, which results these protocols are not suited for the limited resource of the devices. Therefore, it is still a challenge to design an effective three- factor MAKA protocol for achieving secure communication between user and server.

Earlier MAKA protocols are designed for single-server architecture. As Internet users grow exponentially, the number of cloud servers rendering different services has also grown significantly. For the single-server architecture, it is difficult for users to maintain a variety of passwords for each server. To improve user experience, many scholars propose more flexible MAKA protocols for multi-server environments. Combined with the unified management features of the cloud platform, such protocols can be conveniently applied. The protocols for multi-server architectures model as shown in users and cloud servers only need to register in the registration centre (RC) to mutual authentication and key agreement. In the multi-server environments, the MAKA protocols can be further divided into two categories, two-factor MAKA protocols, namely identity, password, and three-factor MAKA protocols, namely identity, password, biometrics.

The works in have shown that the passwordbased MAKA protocols suffer from several attacks such as guessing password attack. The cost of the password guessing attack on password-based protocol becomes lower and lower as the rapid development of computers. On the other hand, users usually use simple letters or numbers as their passwords, and even a large number of users directly use the default password if the smart devices don't require the user to modify the password. In order to solve this problem, several biometrics-based MAKA protocols have been proposed. Due to the uniqueness, availability and non-transferability of biometrics keys (palm print, iris, finger print etc.), the three-factor MAKA protocols for multi-server environments provide more security than the two-factor protocols. In view of the openness of wireless networks, an adversary can intercept, modify, delete and replay any communication messages. Anonymity and untraceability are also indispensable part of the MAKA protocols to resist the above-mentioned attacks.

In Design of secure authenticated key management protocol for cloud computing environment, we propose a provable dynamic revocable user dynamic management provide a formal security in the formal oracle. Security analysis shows that our protocol can meet various demands in the multi-server environments. Performance analysis demonstrates that the proposed scheme is well suited for computing resource constrained smart devices.

1.2 Necessity

Design of secure authentication key is aimed to develop a authentication system for to secure access and upload the file. The scope of the design of secure authentication key is that we are developing this system for the Businessmen’s. and also for collages, Hospitals. Whereever data is generating there our project will helps user to store there data and informations safely. To provide a better way to store the data in a more secure way file uploads represent an easy way for an attacker to inject malicious code into your application.

1.3 Objectives

The objective of this project is to provide secure file upload and access to the design of secure authentication keys. Using encrypted file transfer and secure file transfer protocols safeguards sensitive information and helps avoid data breaches. A secure file transfer service ensures that your files are guarded at rest and in motion and arrive at their destination unscathed.

They enable the sharing of large files, eliminate cloud or network-based threats, and make the user accountable for the file transfer.

Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerised system.

It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow. With the maturity of cloud computing technology in terms of reliability and efficiency, a large number of services have migrated to the cloud platform. To convenient access to the services and protect the privacy of communication in the public network, three-factor Mutual Authentication and Key Agreement (MAKA) protocols for multi-server architectures gain wide attention.

However, most of the existing three-factor MAKA protocols don't provide a formal security proof resulting in various attacks on the related protocols, or they have high computation and communication costs. And most of the three-factor MAKA protocols haven't a dynamic revocation mechanism, which leads to malicious users not be promptly revoked. To address these drawbacks, we propose a provable dynamic revocable three-factor MAKA protocol that achieves the user dynamic management provides a formal security proof in the random oracle. Security analysis shows that our protocol can meet various demands in the multi-server environments. Performance analysis demonstrates that the proposed scheme is well suited for computing resource constrained smart devices. The full version of the simulation implementation proves the feasibility of the protocol.

1.4 methodology

In this project, we propose a dynamic revocable three-factor mutual authentication and key agreement (3DRMAKA) protocol which has more comprehensive functions, reliable security and relatively higher execution efficiency. Our con- tribution can be summarised as follows:

1) We design a three-factor MAKA protocol which implements three-factor security. And we show that the proposed protocol can meet the demands of multi-server architectures such as anonymity, non traceability, resistance password guessing attack and smart card extraction attack, and so on.

2) Our scheme achieves the user's dynamic management. In our protocol, users can be dynamically revoked to promptly prevent attacks from malicious users. Without a dynamic revocation mechanism, RC can't punish malicious users in a timely manner. This may result in such malicious users still active in the network to communicate with other servers.

3) In the random oracle, we provide a formal proof of the proposed protocol based on BDH, CDH and Schnorr signatures. We show that the proposed protocol is mutual authentication secure and authenticated key agreement secure.

4) Our protocol has good execution efficiency. Especially on the client side, the computation cost of our scheme is the lowest in the related existing protocol This shows that our protocol is more suitable for device mobiles with limited computing resources.

1.5 Theme of the Project

Users Registration Phase

In the first module, we develop the Users registration module, where the users who need to access the cloud server need to get registered and then only able to login and access or upload their cloud files. The user registration is done by collecting the details of user name, password and other basic details.

QR Code Generation

Once after the user registration is done, the user will login with the username and password. But even after the username and password is given, the user cannot access the cloud, as the other layer of security should be checked, which is QR Code. In this module, QR code is generated in the backend and stored. Users need to verify the QR Code using QR code extractor to validate the authorised user and then only be able to login or access the cloud. Any user cannot bypass this security feature.

Malicious User Revocation

In this module, we develop the system to identify the malicious user and also provide the option of user revocation. We develop the system with a certain threshold where the user tries to bypass the QR code with wrong QR Code or fake QR code, then the malicious user is identified and blocked by the admin/cloud server. In practice, the importance of an efficient revocation mechanism is self-evident. It has positive meaning both in preventing malicious users and improving the efficiency of cloud servers.

User Apply For Revocation

In the earlier module, during the session, if servers find that a user is visiting illegally, the server reports and it will verify the authenticity. If the situation is true, he/she is immediately blocked. Otherwise, the cloud server will punish the service to a certain degree of downgrade. If this process is done wrong, then the user is able to request, so the user revocation process can also be done in this module. The user sends the revocation request with identity through the secure channel. After receiving the message, the server checks the identity and gives the access with new QR code.

Cloud Server

In this module, we develop the Cloud server module, where we design the system to upload the files in a free cloud server named DriveHQ. Is an entity with powerful computation and storage resources. CS stores a massive amount of encrypted data, and receives the semantic queries to look for the required documents on behalf of the data user. The cloud finds the relevant documents, and sends them back to the data user. The cloud server is an intermediate service provider that performs the retrieval process.

2. LITERATURE SURVEY

Literature survey is the most vital step in the software development process. Before developing the tool, it's necessary to work out the time factor, economy and company strength. Once this stuff is satisfied, ten next steps are to work out which OS and language used for developing the tool. This literature survey is mainly used for identifying the list of resources to construct this proposed application.

A well-known author Sherali Zeadally, has written a paper on" An Enhanced and Provably Secure Chaotic Map-Based Authenticated Key Agreement in Multi-Server Architecture". In this paper the authors mainly concentrated on the problem of building and establishing a secure cloud server on the top of all public cloud infrastructures. They mainly identified the high level security preference and also about the recent cryptographic primitives. The authors mainly concentrate on the cryptography techniques which were used for providing security for the data encryption and decryption. Here the authors conducted a survey on the cloud and its importance in the public storage area.

A well-known author, Azeem Irshad, has written a paper on "An Enhanced and Provably Secure Chaotic Map-Based Authenticated Key Agreement in Multi-Server Architecture". In this paper the authors mainly concentrated about the In the multi-server authentication (MSA) paradigm, a subscriber might avail multiple services of different service providers, after registering from registration authority. In this approach, the user has to remember only a single password for all service providers, and servers are relieved of individualised registrations. Many MSA-related schemes have been presented so far, however with several drawbacks.

The first survey of detecting site visitors from social media as Zhen-Yu Wu dialect, et. al., presents the survey paper A Reliable Dynamic User-Remote Password Authentication Scheme over Insecure Network Publisher at 2012. Protocols of user authentication square measure are able to ensure the security of information transmission and users' communication over insecure networks. Among varied documented mechanisms run presently, password-based user authentication, owing to its potency, is the most generally used in several areas, like laptop networks, wireless networks, remote login, operation systems, and direction systems. as it is blessed with the property of straightforward and human unforgettable, that causes such associate degree attacks of brute force, for instance, the previous works typically suffer off-line password shot attack. Therefore, associate degree meliorative password-based authentication theme is projected during this paper, achieving to resist off-line password shot attacks, replay attacks, on-line password shot attacks, and ID-theft attacks. In light of security, the projected theme is given sensible utility, even over insecure networks. Xinyi Huang, et. al., presents the survey paper of Robust Multi-Factor Authentication for Fragile Communications in 2014. In large-scale systems, user authentication sometimes needs the assistance from the central authentication server via networks. The authentication service might be down or unavailable to natural disasters or various cyber-attacks on communication channels. This has raised serious considerations in systems which require sturdy authentication in emergency things. The contribution of this paper is twofold. During a slow affiliation scenario, we have a tendency to give a secure generic multi-factor authentication protocol to hurry up the complete authentication method. Compared with another generic protocol within the literature, the new proposal provides an equivalent performance with vital enhancements in computation and communication. Another authentication mechanism, that we have a tendency to name complete authentication, will manifest users once the affiliation to the central server is down. We have a tendency to investigate many problems in complete authentication and show how to add it on multi-factor authentication protocols in an economical and generic way.

The proposed secure authenticated key management protocol for storing the data under data revocation in this proposed thesis we try to design an idea called maka protocol mutual authentication and key agreement under data revocation for constructing a financial support which can be satisfied by all the primitive objectives. Here we try to address some formal definitions to make algorithms and try to concentrate more about its security. We try to discuss more about the implementation of rs-ibe algorithm and its advantages.

The proposed security model is mainly proposed or designed based on the standard model like the decisional ℓ-bilinear diffie-hellman exponent (ℓ-bdhe) supposition. In other words we can say that the proposed scheme can give more security for the encoding and decoding of user authentication. The proposed technique is best in following ways like : this can provide secrecy of data in both forward and backward methods. The primary role of this proposed plan is that all the data will be initially converted in plain text manner before it is stored into the server location. As the data is stored in an encrypted manner for accessing the file, the user needs the access permission from the cloud server. This access permission will try to restrict unauthorised users.

2.1 Password authentication with insecure communication

AUTHORS: L. Lamport

A method of user password authentication is described which is secure even if an intruder can read the system's data, and can tamper with or eavesdrop on the communication between the user and the system. The method assumes a secure one-way encryption function and can be implemented with a microcomputer in the user's terminal.

2.2 A generic framework for three-factor authentication: Preserving security and privacy in distributed systems

AUTHORS: X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R. H. Deng

As part of the security within distributed systems, various services and resources need protection from unauthorised use. Remote authentication is the most commonly used method to determine the identity of a remote client. This paper investigates a systematic approach for authenticating clients by three factors, namely password, smart card, and biometrics. A generic and secure framework is proposed to upgrade two-factor authentication to three-factor authentication. The conversion not only significantly improves the information assurance at low cost but also protects client privacy in distributed systems. In addition, our framework retains several practice-friendly properties of the underlying two-factor authentication, which we believe is of independent interest.

2.3 Robust multi factor authentication for fragile communications

AUTHORS: X. Huang, Y. Xiang, E. Bertino, J. Zhou, and L. Xu,

In large-scale systems, user authentication usually needs the assistance from a remote central authentication server via networks. The authentication service however could be slow or unavailable due to natural disasters or various cyber attacks on communication channels. This has raised serious concerns in systems which need robust authentication in emergency situations. The contribution of this paper is two-fold. In a slow connection situation, we present a secure generic multi-factor authentication protocol to speed up the whole authentication process. Compared with another generic protocol in the literature, the new proposal provides the same function with significant improvements in computation and communication. Another authentication mechanism, which we name stand-alone authentication, can authenticate users when the connection to the central server is down. We investigate several issues in stand-alone authentication and show how to add it on multi-factor authentication protocols in an efficient and generic way.

2.4 Anonymous authentication for wireless body area networks with provable security

AUTHORS: D. He, S. Zeadally, N. Kumar, and J. Lee

Advances in wireless communications, embedded systems, and integrated circuit technologies have enabled the wireless body area network (WBAN) to become a promising networking paradigm. Over the last decade, as an important part of the Internet of Things, we have witnessed WBANs playing an increasing role in modern medical systems because of its capabilities to collect real-time biomedical data through intelligent medical sensors in or around the patients' body and send the collected data to remote medical personnel for clinical diagnostics. WBANs not only bring us conveniences but also bring along the challenge of keeping data's confidentiality and preserving patients' privacy. In the past few years, several anonymous authentication (AA) schemes for WBANs were proposed to enhance security by protecting patients' identities and by encrypting medical data. However, many of these schemes are not secure enough. First, we review the most recent AA scheme for WBANs and point out that it is not secure for medical applications by proposing an impersonation attack. After that, we propose a new AA scheme for WBANs and prove that it is provably secure. Our detailed analysis results demonstrate that our proposed AA scheme not only overcomes the security weaknesses in previous schemes but also has the same computation costs at a client side.

2.5 A remote password authentication scheme for multiserver architecture using neural networks

AUTHORS: L. Li, L. Lin, and M. Hwang

Conventional remote password authentication schemes allow a serviceable server to authenticate the legitimacy of a remote login user. However, these schemes are not used for multiserver architecture environments. We present a remote password authentication scheme for multiserver environments. The password authentication system is a pattern classification system based on an artificial neural network. In this scheme, the users only remember user identity and password numbers to log in to various servers. Users can freely choose their password. Furthermore, the system is not required to maintain a verification table and can withstand the replay attack.

3. SYSTEM DEVELOPMENT

3.1 Requirement Specification

3.1.1 DFD

The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.

The data flow diagram (DFD) is one of the most important modelling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.

DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

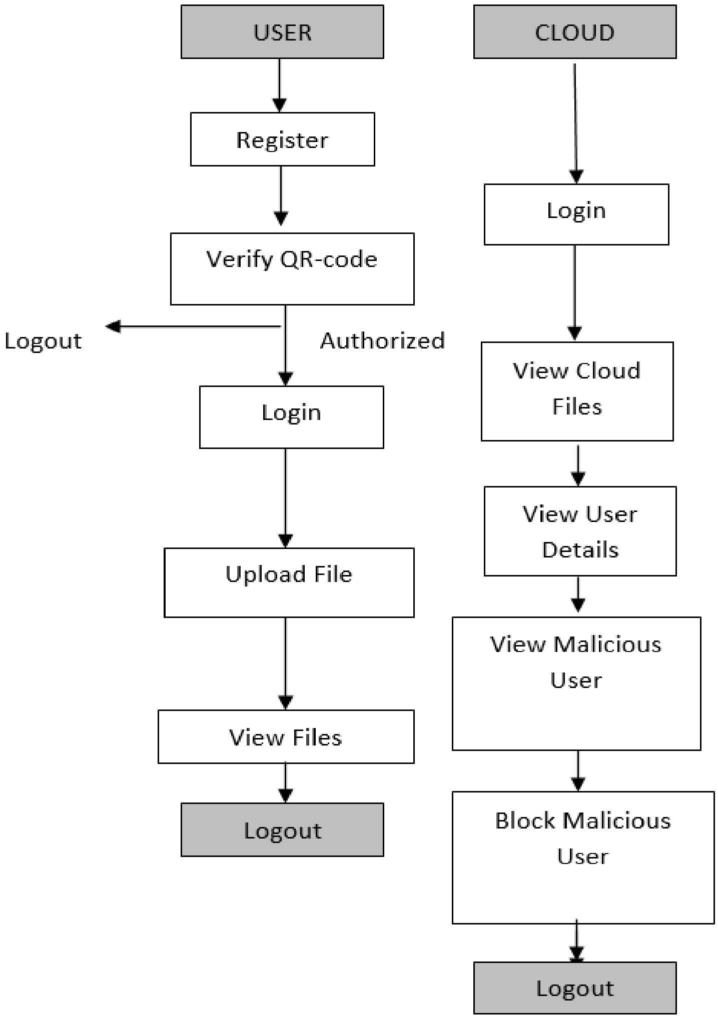

USER
Register
Verify QR-code
Logout
Authorized
Login
Upload File
View Files
Logout
CLOUD
Login
View Cloud Files
View User Details
View Malicious User
Block Malicious User
Logout

Fig 3.1 : DFD

3.1.2 Specification Document/UML Diagrams of all modules

UML stands for Unified Modeling Language. UML is a standardised general-purpose modelling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group.

The goal is for UML to become a common language for creating models of object oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML.

The Unified Modeling Language is a standard language for specifying, Visualization, Constructing and documenting the artefacts of software system, as well as for business modelling and other non-software systems. The UML represents a collection of best engineering practices that have proven successful in the modelling of large and complex systems.

The UML is a very important part of developing objects oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

GOALS:

The Primary goals in the design of the UML are as follows:

1. Provide users a ready-to-use, expressive visual modelling Language so that they can develop and exchange meaningful models.
2. Provide extendibility and specialisation mechanisms to extend the core concepts.
3. Be independent of particular programming languages and development process.
4. Provide a formal basis for understanding the modelling language.
5. Encourage the growth of OO tools market.
6. Support higher level development concepts such as collaborations, frameworks, patterns and components.
7. Integrate best practices.

3.1.3 Use Case Diagram :

A use case diagram in the Unified Modeling Language (UML) is a type of behavioural diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

Use-case diagrams are helpful in the following situations:

- Before starting a project, you can create use-case diagrams to model a business so that all participants in the project share an understanding of the workers, customers, and activities of the business.
- While gathering requirements, you can create use-case diagrams to capture the system requirements and to present to others what the system should do.
- During the analysis and design phases, you can use the use cases and actors from your use-case diagrams to identify the classes that the system requires.
- During the testing phase, you can use use-case diagrams to identify tests for the system.

The following topics describe model elements in use-case diagrams:

- **Use cases**
  A use case describes a function that a system performs to achieve the user's goal. A use case must yield an observable result that is of value to the user of the system.
- **Actors**
  An actor represents a role of a user that interacts with the system that you are modelling. The user can be a human user, an organisation, a machine, or another external system.
- **Subsystems**
  In UML models, subsystems are a type of stereotyped component that represent independent, behavioural units in a system. Subsystems are used in class, component, and use-case diagrams to represent large-scale components in the system that you are modelling.

- **Relationships in use-case diagrams**

  In UML, a relationship is a connection between model elements. A UML relationship is a type of model element that adds semantics to a model by defining the structure and behaviour between the model elements.

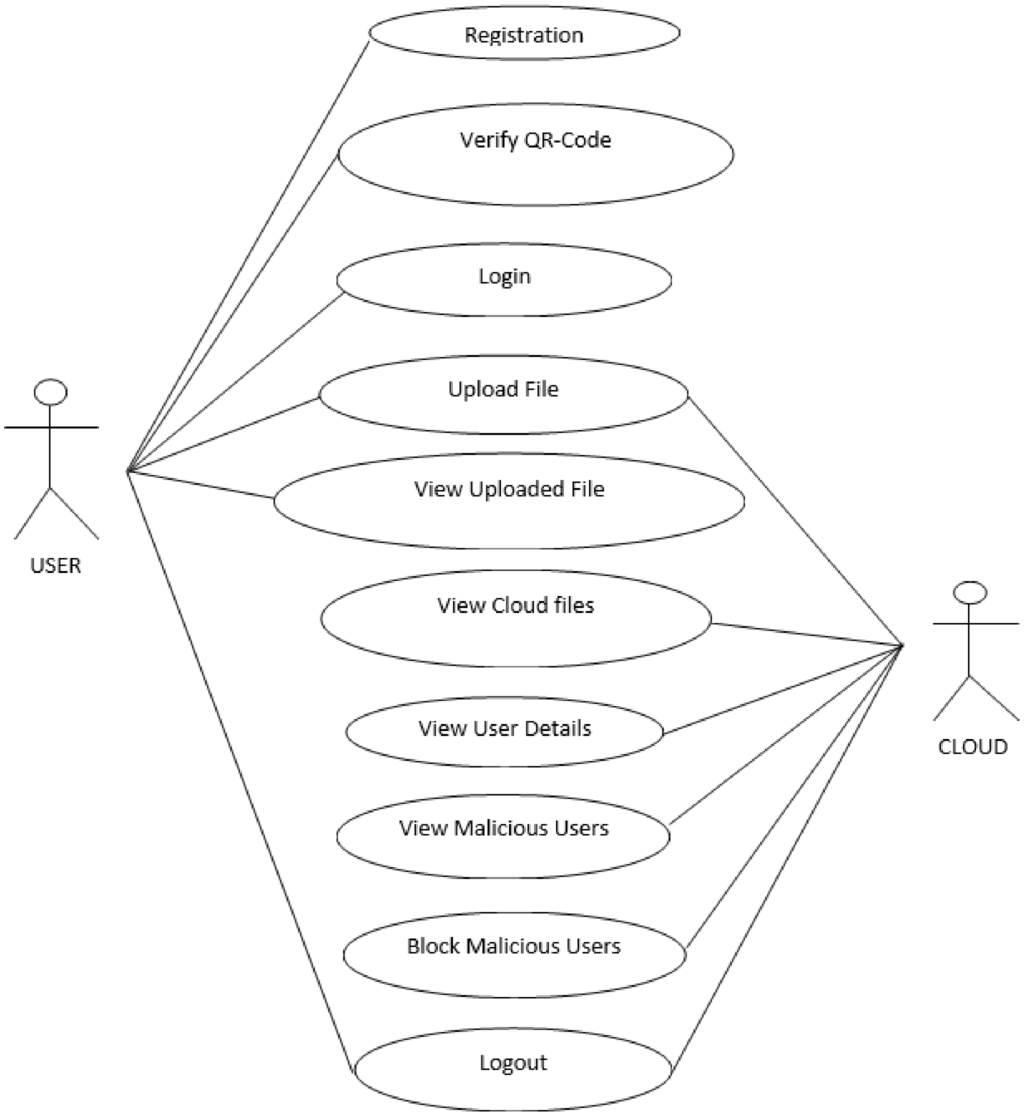


Fig 3.2 : Use Case Diagram.

3.1.4 Class Diagram :

In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information.

Benefits of class diagrams

Class diagrams offer a number of benefits for any organisation. Use UML class diagrams to:

- Illustrate data models for information systems, no matter how simple or complex.
- Better understand the general overview of the schematics of an application.
- Visually express any specific needs of a system and disseminate that information throughout the business.
- Create detailed charts that highlight any specific code needed to be programmed and implemented to the described structure.
- Provide an implementation-independent description of types used in a system that are later passed between its components.

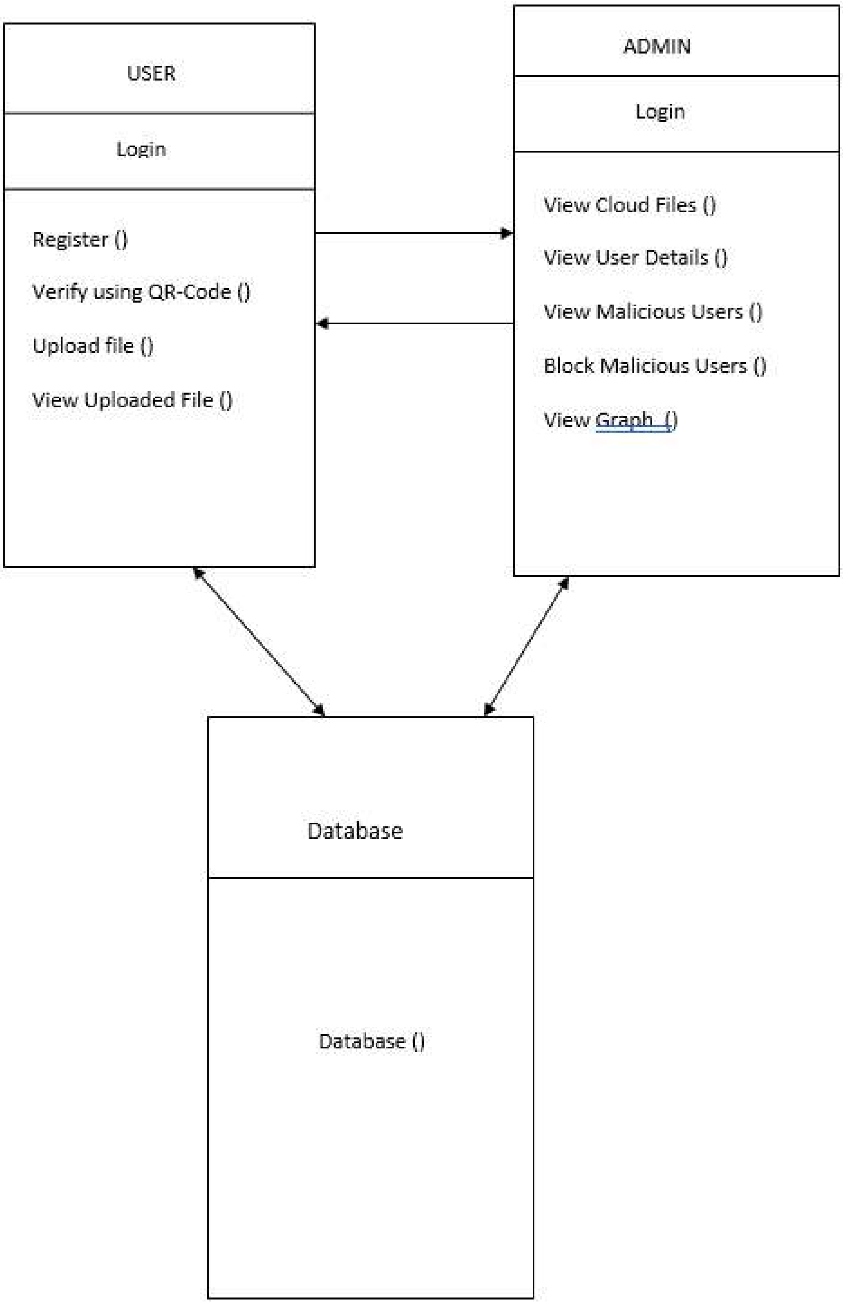


Fig 3.3 : Class Diagram

3.1.5 Sequence Diagram :

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.

Benefits of sequence diagrams

Sequence diagrams can be useful references for businesses and other organisations. Try drawing a sequence diagram to:

- Represent the details of a UML use case.
- Model the logic of a sophisticated procedure, function, or operation.
- See how objects and components interact with each other to complete a process.
- Plan and understand the detailed functionality of an existing or future scenario.

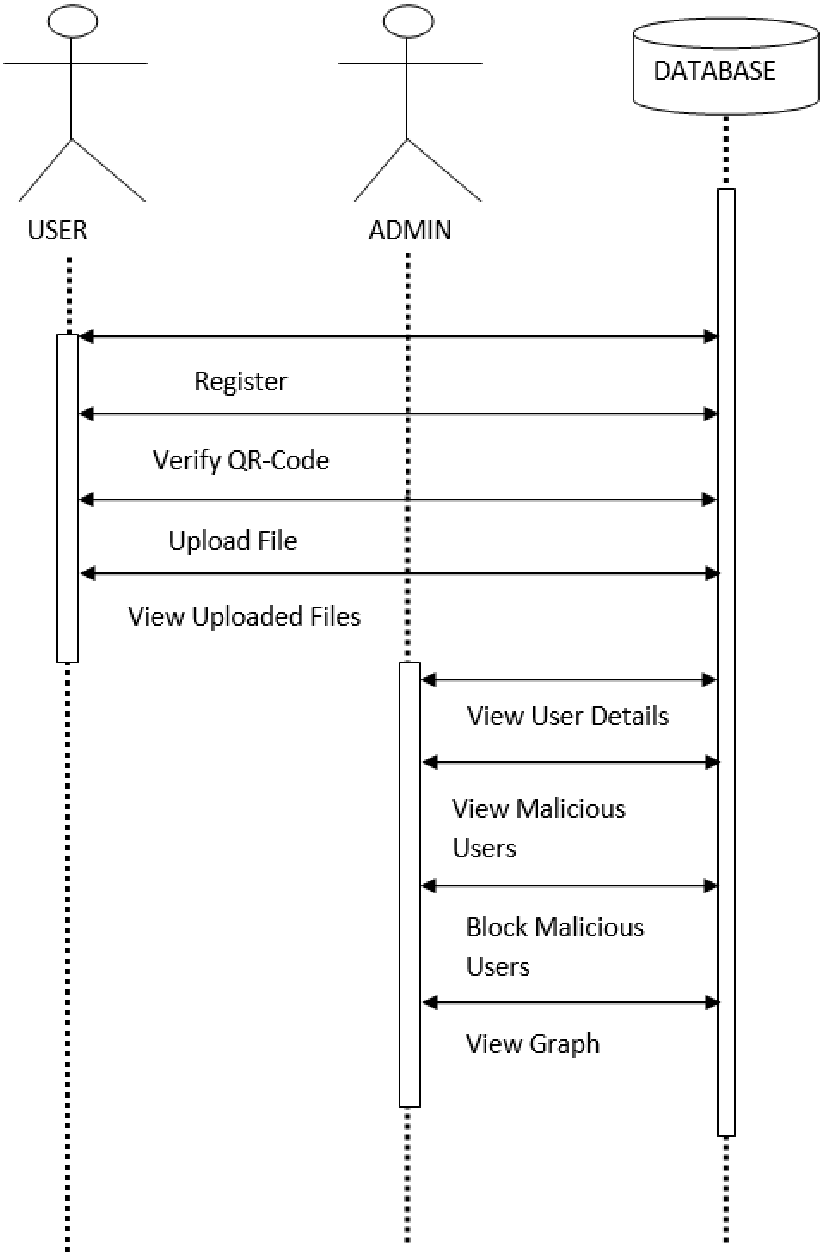
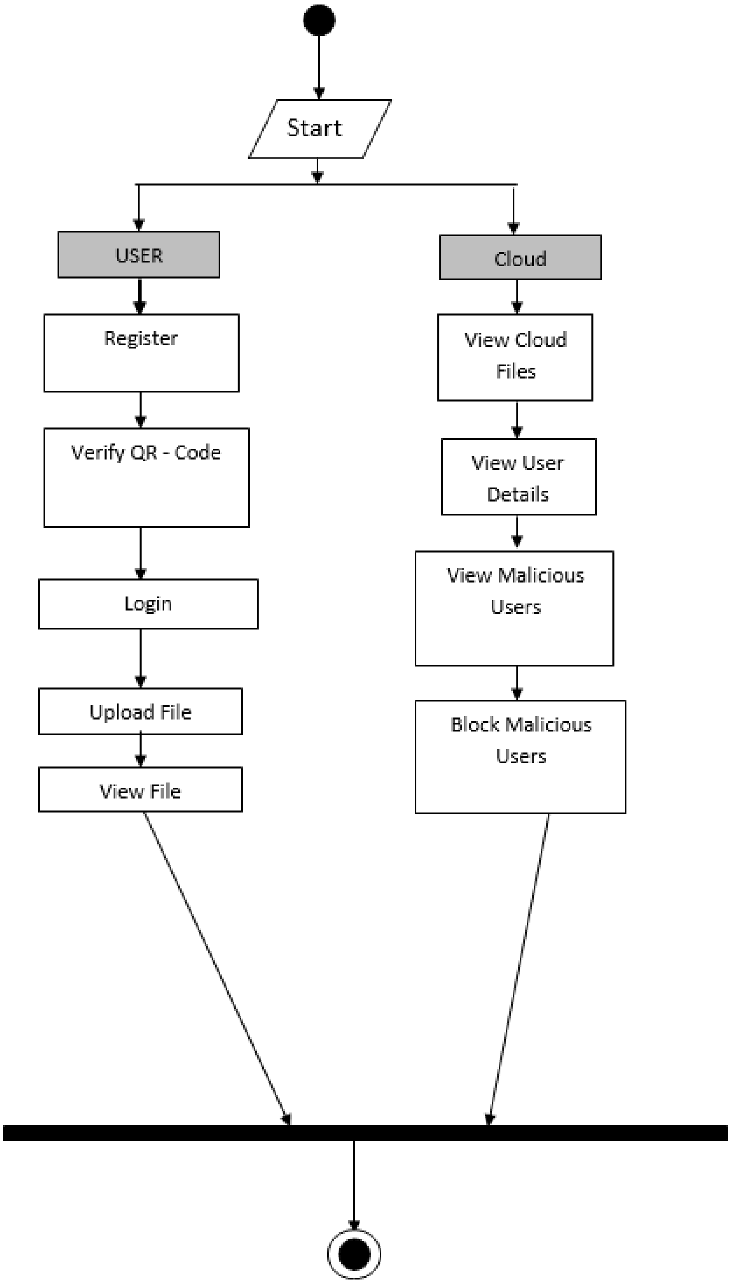


Fig 3.4 : Sequence Diagram

3.1.6 Activity Diagram :

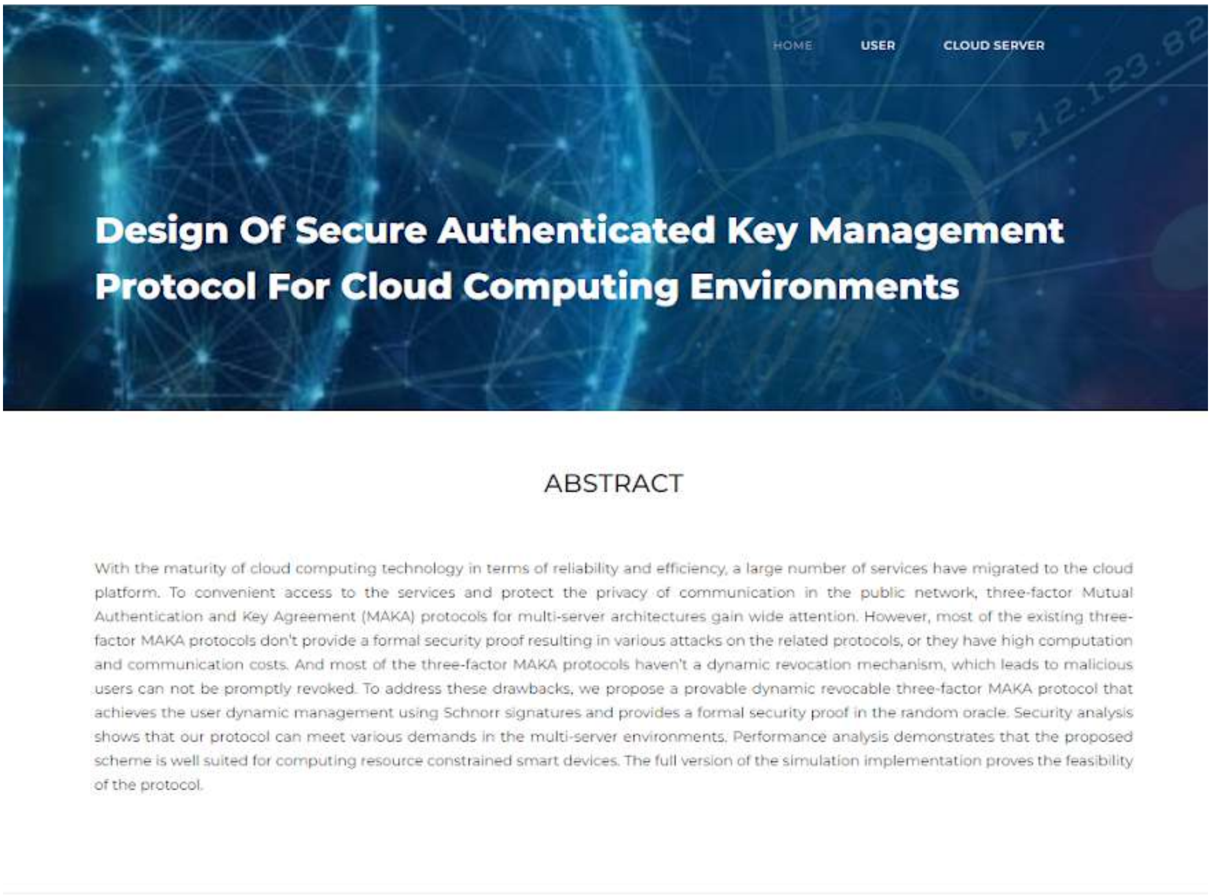
Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.



-

Fig 3.5 : Activity Diagram.

3.2 User Interface Design

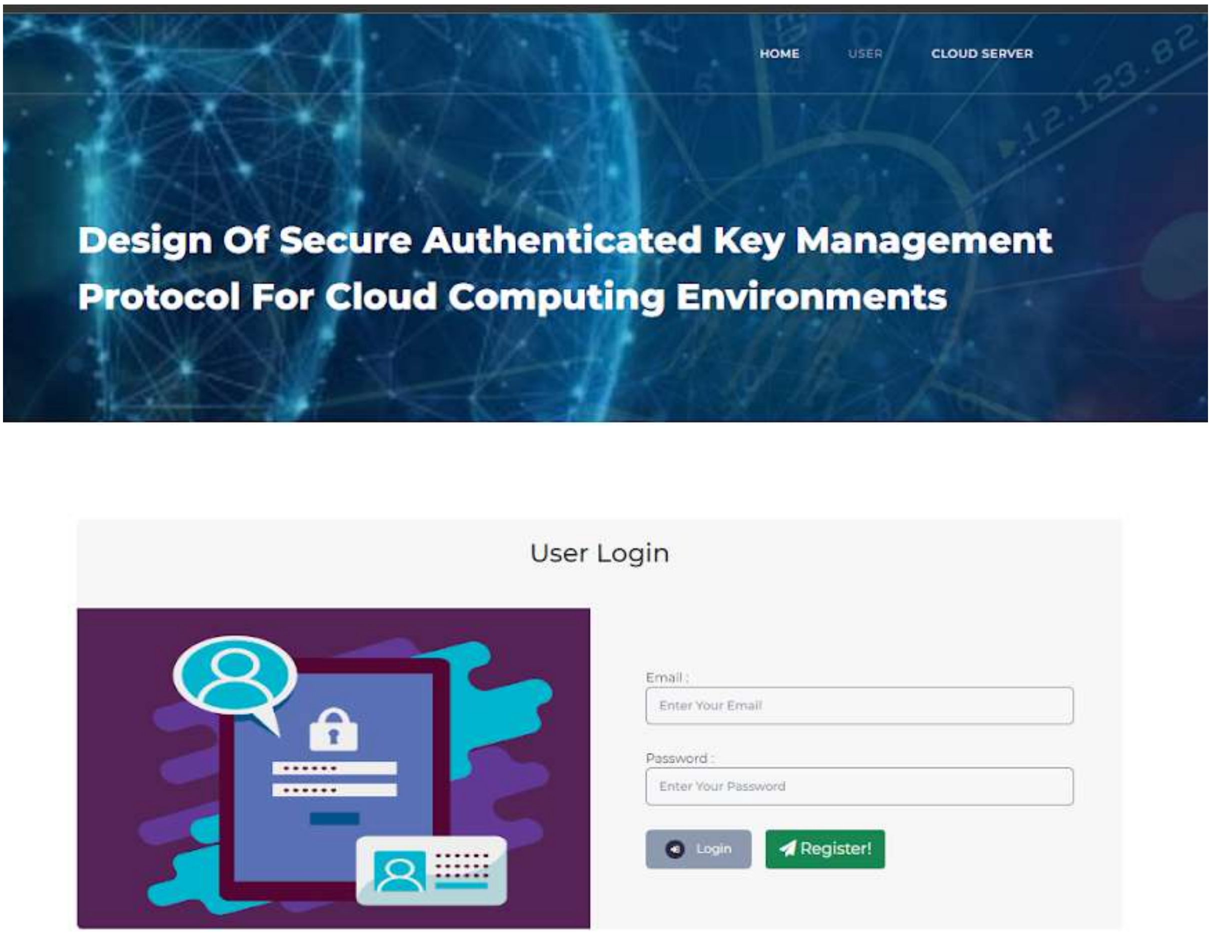


Design Of Secure Authenticated Key Management Protocol For Cloud Computing Environments

ABSTRACT

With the maturity of cloud computing technology in terms of reliability and efficiency, a large number of services have migrated to the cloud platform. To convenient access to the services and protect the privacy of communication in the public network, three-factor Mutual Authentication and Key Agreement (MAKA) protocols for multi-server architectures gain wide attention. However, most of the existing three-factor MAKA protocols don't provide a formal security proof resulting in various attacks on the related protocols, or they have high computation and communication costs. And most of the three-factor MAKA protocols haven't a dynamic revocation mechanism, which leads to malicious users can not be promptly revoked. To address these drawbacks, we propose a provable dynamic revocable three-factor MAKA protocol that achieves the user dynamic management using Schnorr signatures and provides a formal security proof in the random oracle. Security analysis shows that our protocol can meet various demands in the multi-server environments. Performance analysis demonstrates that the proposed scheme is well suited for computing resource constrained smart devices. The full version of the simulation implementation proves the feasibility of the protocol.

Screen 3.1 : Home Page



Design Of Secure Authenticated Key Management Protocol For Cloud Computing Environments

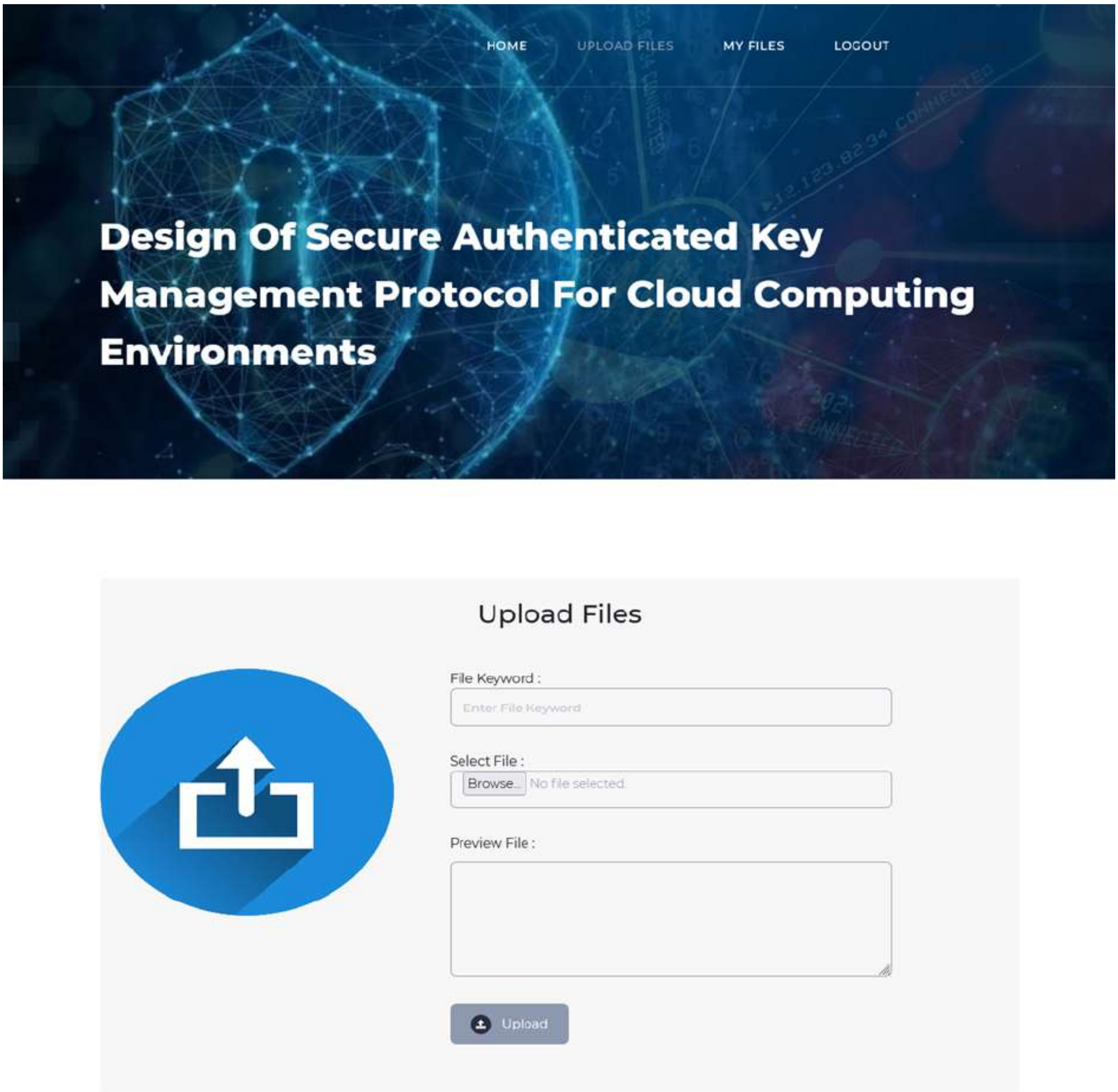
User Login

Email :
Enter Your Email

Password :
Enter Your Password

Screen 3.2 : User Page

,;



Design Of Secure Authenticated Key Management Protocol For Cloud Computing Environments

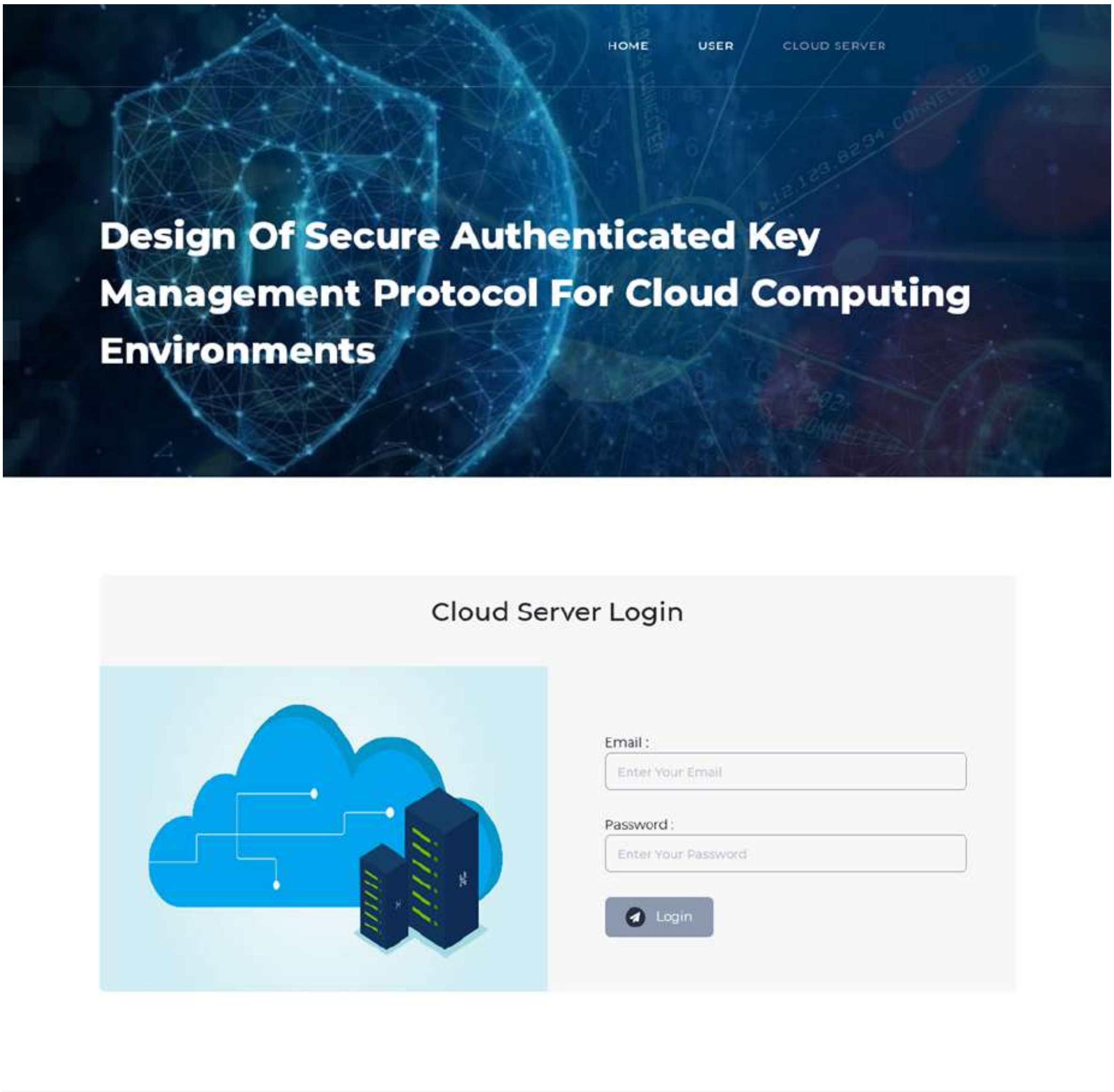
Upload Files

File Keyword : Enter File Keyword

Select File : Browse... No file selected.

Preview File :

Screen 3.3 : Files upload page



Design Of Secure Authenticated Key Management Protocol For Cloud Computing Environments

Cloud Server Login

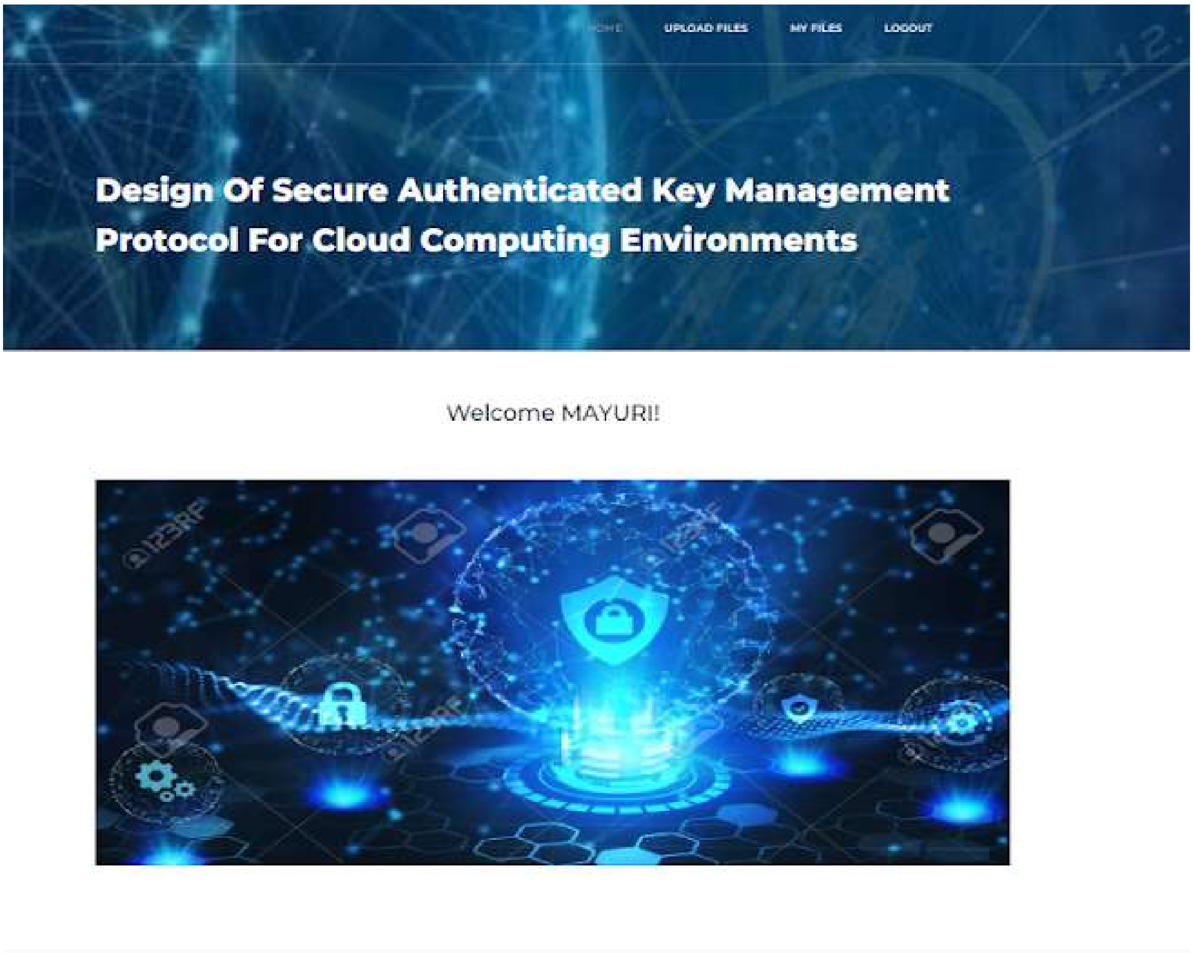
Email :

Enter Your Email

Password :

Enter Your Password

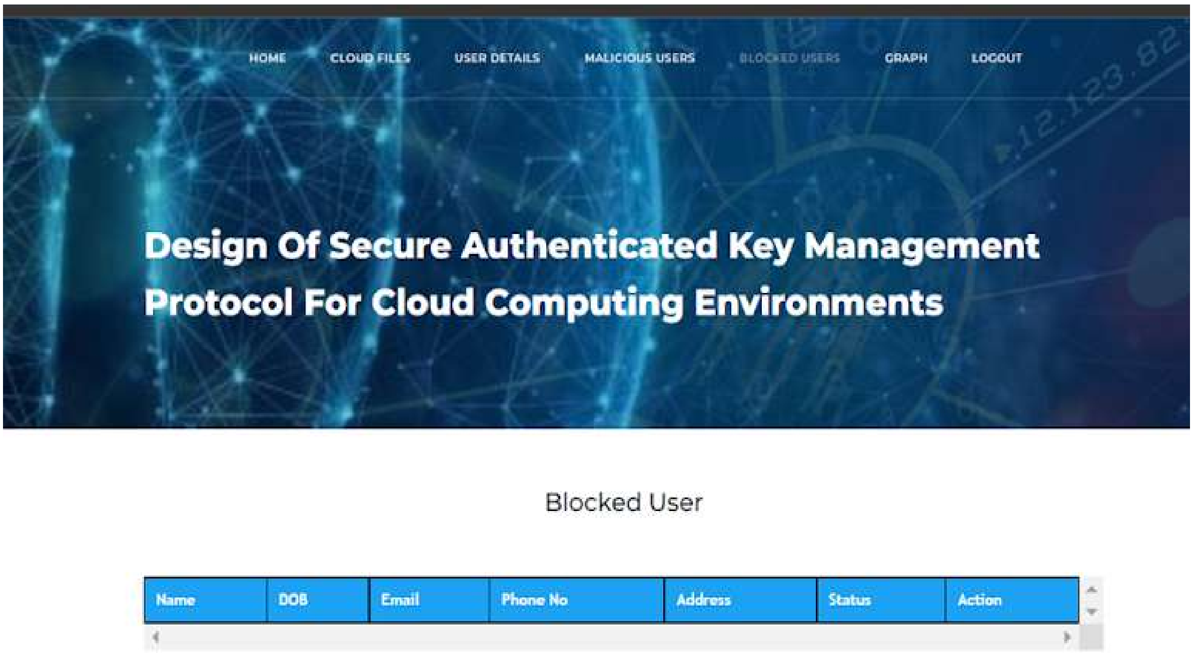
Screen 3.4 : Cloud server page



Design Of Secure Authenticated Key Management Protocol For Cloud Computing Environments

Welcome MAYURI!

Screen 3.5 : Welcome page

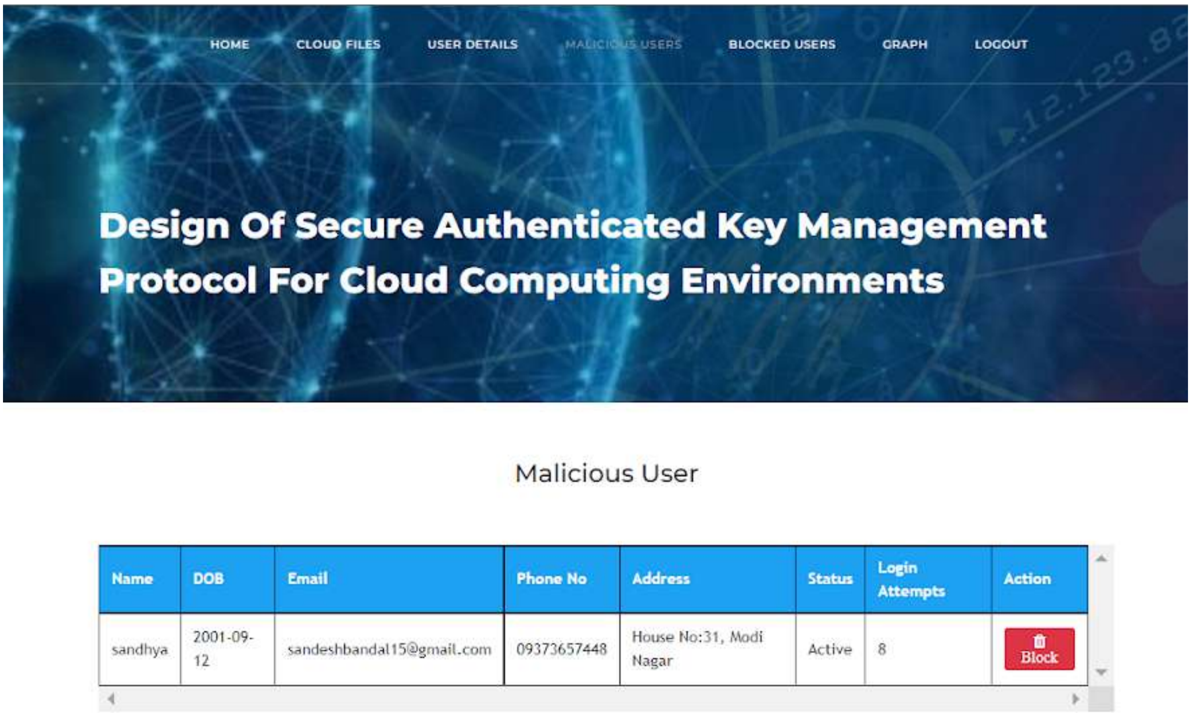


Design Of Secure Authenticated Key Management Protocol For Cloud Computing Environments

Blocked User

Name	DOB	Email	Phone No	Address	Status	Action

Screen 3.6 : Blocked user page

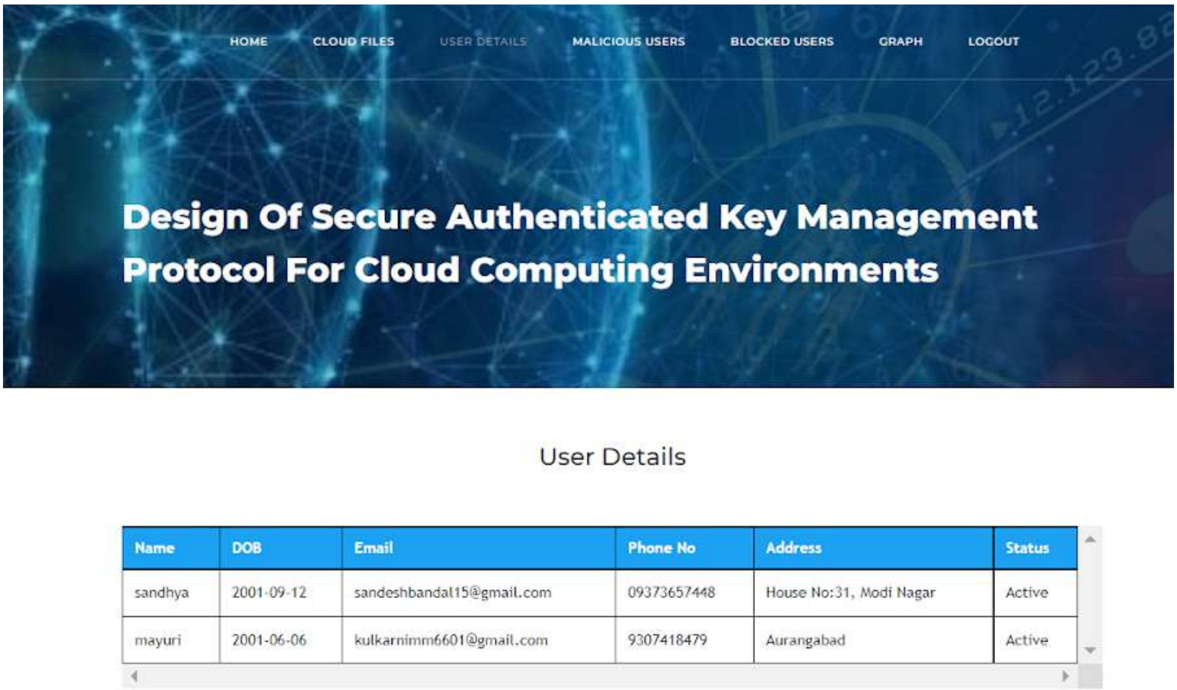


Design Of Secure Authenticated Key Management Protocol For Cloud Computing Environments

Malicious User

Name	DOB	Email	Phone No	Address	Status	Login Attempts	Action
sandhya	2001-09-12	sandeshbandal15@gmail.com	09373657448	House No:31, Modi Nagar	Active	8	Block

Screen 3.7 : Malicious user page

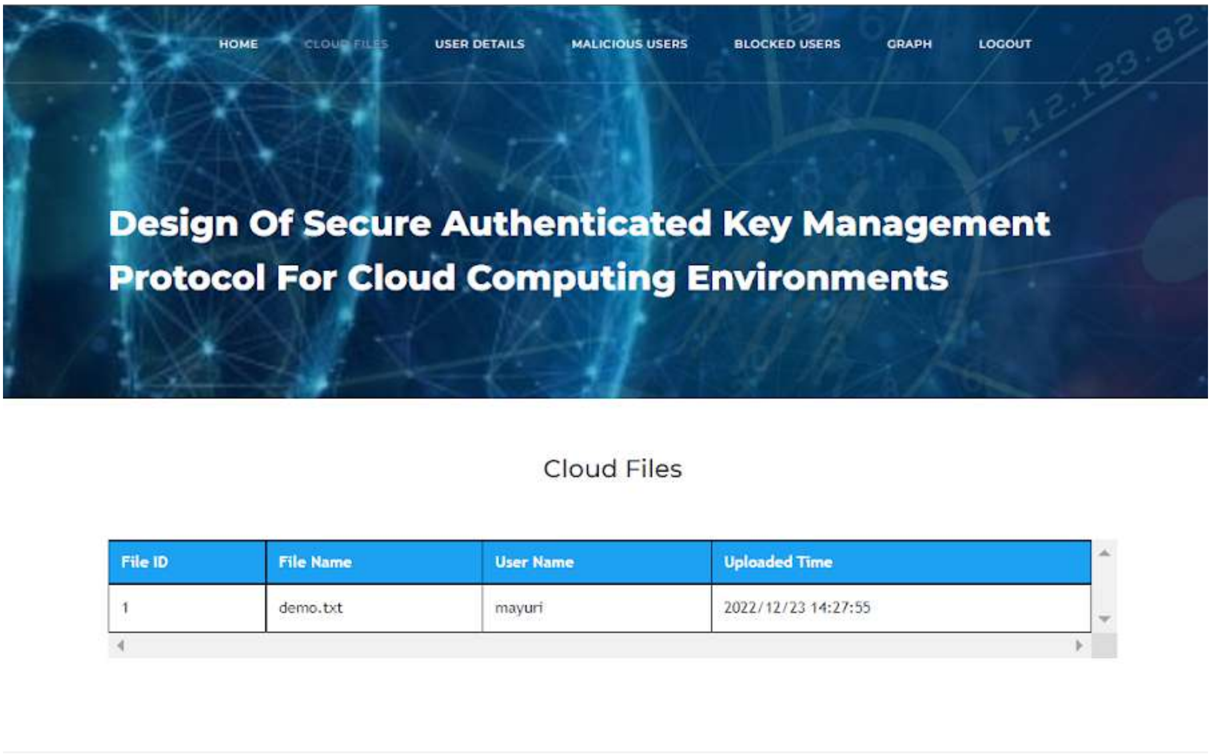


Design Of Secure Authenticated Key Management Protocol For Cloud Computing Environments

User Details

Name	DOB	Email	Phone No	Address	Status
sandhya	2001-09-12	sandeshbandal15@gmail.com	09373657448	House No:31, Modi Nagar	Active
mayuri	2001-06-06	kulkarnimm6601@gmail.com	9307418479	Aurangabad	Active

Screen 3.8 : User details

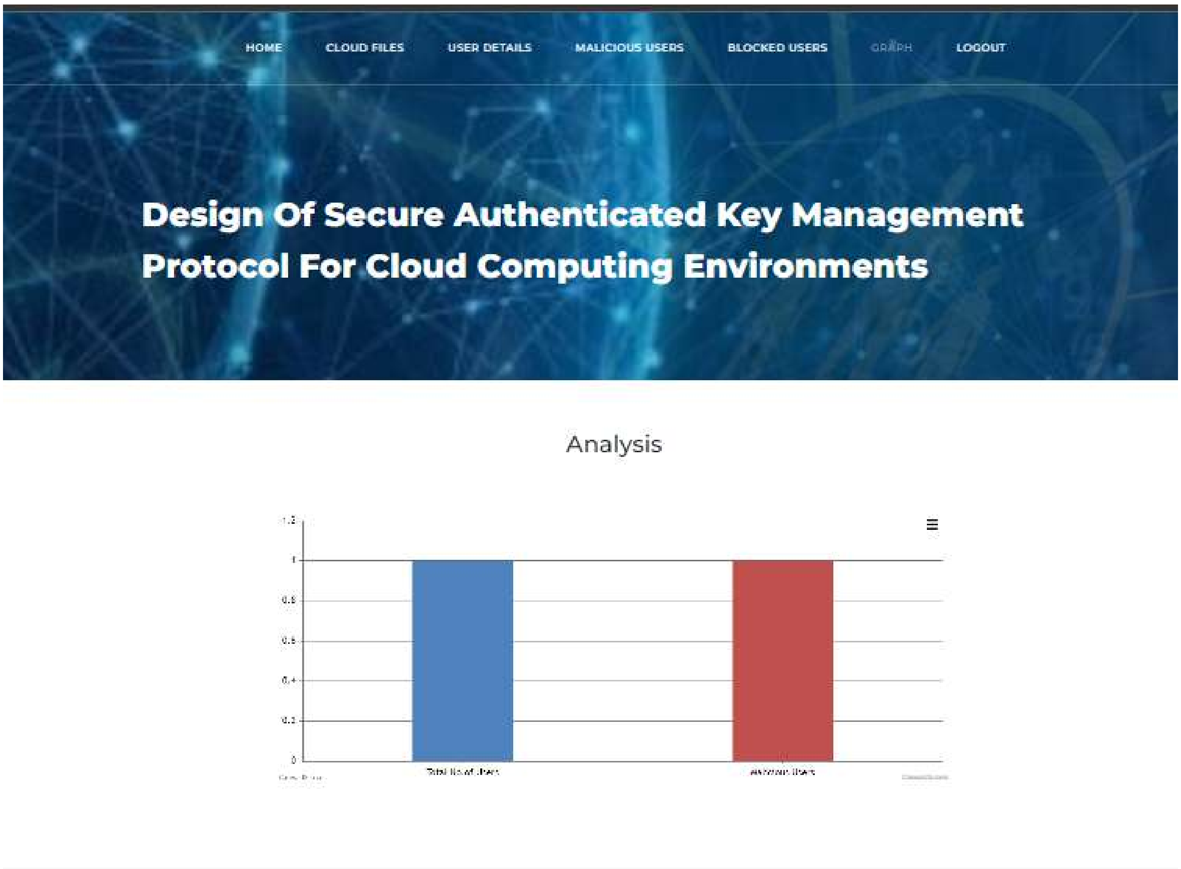


Design Of Secure Authenticated Key Management Protocol For Cloud Computing Environments

Cloud Files

File ID	File Name	User Name	Uploaded Time
1	demo.txt	mayuri	2022/12/23 14:27:55

screen 3.9 : Cloud files



Design Of Secure Authenticated Key Management Protocol For Cloud Computing Environments

Analysis

screen 3.10 : Analysis through graphs

3.3 Database Design

SQL SERVER 2008

A database management, or DBMS, gives the user access to their data and helps them transform the data into information. Such database management systems include dBase, paradox, IMS, SQL Server and SQL Server. These systems allow users to create, update and extract information from their database.

A database is a structured collection of data. Data refers to the characteristics of people, things and events. SQL Server stores each data item in its own fields. In SQL Server, the fields relating to a particular person, thing or event are bundled together to form a single complete unit of data, called a record (it can also be referred to as raw or an occurrence). Each record is made up of a number of fields. No two fields in a record can have the same field name.

During an SQL Server Database design project, the analysis of your business needs identifies all the fields or attributes of interest. If your business needs change over time, you define any additional fields or change the definition of existing fields.

4. PERFORMANCE EVALUATION

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organised, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.

2. Select methods for presenting information.

3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections of the
- Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

Feasibility Study

The feasibility of the project is analysed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

¨ Economical Feasibility
¨ Technical Feasibility
¨ Social Feasibility

Economical Feasibility

This study is carried out to check the economic impact that the system will have on the organisation. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customised products had to be purchased.

Technical Feasibility

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

Social Feasibility

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

Testing

Software testing is the process of evaluating and verifying that a software product or application does what it is supposed to do. The benefits of testing include preventing bugs, reducing development costs and improving performance.

Unit Testing

Unit Testing is a software testing technique by means of which individual units of software i.e. group of computer program modules, usage procedures, and operating procedures are tested to determine whether they are suitable for use or not. It is a testing method using which every independent module is tested to determine if there is an issue by the developer himself. It is correlated with the functional correctness of the independent modules. Unit Testing is defined as a type of software testing where individual components of a software are tested. Unit Testing of the software product is carried out during the development of an application. An individual component may be either an individual function or a procedure. Unit Testing is typically performed by the developer. In SDLC or V Model, Unit testing is the first level of testing done before integration testing. Unit testing is such a type of testing technique that is usually performed by developers. Although due to the reluctance of developers to test, quality assurance engineers also do unit testing.

Objective of Unit Testing:

The objective of Unit Testing is:

- To isolate a section of code.
- To verify the correctness of the code.

- To test every function and procedure.
- To fix bugs early in the development cycle and to save costs.
- To help the developers to understand the code base and enable them to make changes quickly.
- To help with code reuse.

Integration Testing

Integration testing is the process of testing the interface between two software units or modules. It focuses on determining the correctness of the interface. The purpose of integration testing is to expose faults in the interaction between integrated units. Once all the modules have been unit tested, integration testing is performed. Integration testing can be done by picking module by module. This can be done so that there should be proper sequence to be followed. And also if you don’t want to miss out on any integration scenarios then you have to follow the proper sequence. Exposing the defects is the major focus of the integration testing and the time of interaction between the integrated units. Integration test approaches – There are four types of integration testing approaches. Those approaches are the following:

1. Big-Bang Integration Testing – It is the simplest integration testing approach, where all the modules are combined and the functionality is verified after the completion of individual module testing. In simple words, all the modules of the system are simply put together and tested. This approach is practicable only for very small systems. If an error is found during the integration testing, it is very difficult to localize the error as the error may potentially belong to any of the modules being integrated. So, debugging errors reported during big bang integration testing is very expensive to fix.

Advantages:

- It is convenient for small systems.

Disadvantages:

- There will be quite a lot of delay because you would have to wait for all the modules to be integrated.

- High risk critical modules are not isolated and tested on priority since all modules are tested at once.
- Not Good for long Projects.

2. Bottom-Up Integration Testing – In bottom-up testing, each module at lower levels is tested with higher modules until all modules are tested. The primary purpose of this integration testing is that each subsystem tests the interfaces among various modules making up the subsystem. This integration testing uses test drivers to drive and pass appropriate data to the lower level modules.

Advantages:

- In bottom-up testing, no stubs are required.
- A principle advantage of this integration testing is that several disjoint subsystems can be tested simultaneously.
- It is easy to create the test conditions. Best for the applications that uses bottom up design approach.
- It is Easy to observe the test results.

Disadvantages:

- Driver modules must be produced.
- In this testing, the complexity that occurs when the system is made up of a large number of small subsystems.
- As Far modules have been created, there is no working model can be represented.

3. Top-Down Integration Testing – Top-down integration testing technique is used in order to simulate the behaviour of the lower-level modules that are not yet integrated. In this integration testing, testing takes place from top to bottom. First, high-level modules are tested and then low-level modules and finally integrating the low-level modules to a high level to ensure the system is working as intended.

Advantages:

- Separately debugged module.
- Few or no drivers needed.
- It is more stable and accurate at the aggregate level.

- Easier isolation of interface errors.
- In this, design defects can be found in the early stages.

Disadvantages:

- Needs many Stubs.
- Modules at lower level are tested inadequately.
- It is difficult to observe the test output.
- It is difficult to stub design.

4. Mixed Integration Testing – A mixed integration testing is also called sandwiched integration testing. A mixed integration testing follows a combination of top down and bottom-up testing approaches. In top-down approach, testing can start only after the top-level module have been coded and unit tested. In bottom-up approach, testing can start only after the bottom level modules are ready. This sandwich or mixed approach overcomes this shortcoming of the top-down and bottom-up approaches. It is also called the hybrid integration testing. also, stubs and drivers are used in mixed integration testing.

Advantages:

- Mixed approach is useful for very large projects having several sub projects.
- This Sandwich approach overcomes this shortcoming of the top-down and bottom-up approaches.
- Parallel test can be performed in top and bottom layer tests.

Disadvantages:

- For mixed integration testing, it requires very high cost because one part has Top-down approach while another part has bottom-up approach.
- This integration testing cannot be used for smaller systems with huge interdependence between different modules.

5. CONCLUSION

To resist the exhaustion of password attack on the two-factor MAKA protocols, a large number of three-factor MAKA protocols have been proposed. However, almost all three factor MAKA protocols don’t provide formal proofs and dynamic user management mechanism. In order to achieve more flexible user management and higher security, this paper proposes a new three-factor MAKA protocol that supports dynamic revocation and provides formal proof. The security shows that our protocol achieves the security properties of requirements from multi-server environments. On the other hand, through the comprehensive analysis of performance, our protocol doesn’t sacrifice efficiency while improving the function. On the contrary, the proposed protocol has great advantages in terms of the total computation time.

References

- L. Lamport, “Password authentication with insecure communication,” Commun. ACM, vol. 24, no. 11, pp. 770–772, 1981.
- X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R. H. Deng, “A generic framework for three-factor authentication: Preserving security and privacy in distributed systems,” IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 8, pp. 1390–1397, Aug. 2011.
- X. Huang, Y. Xiang, E. Bertino, J. Zhou, and L. Xu, “Robust multi factor authentication for fragile communications,” IEEE Trans. Dependable Secure Comput., vol. 11, no. 6, pp. 568–581, Nov./Dec. 2014.
- D. He, S. Zeadally, N. Kumar, and J. Lee, “Anonymous authentication for wireless body area networks with provable security,” IEEE Syst. J., vol. 22, pp. 1–12, 2016.
- [5] L. Li, L. Lin, and M. Hwang, “A remote password authentication scheme for multi server architecture using neural networks,” IEEE Trans. Neural Netw., vol. 12, no. 6, pp. 1498–1504, Nov. 2001.
- W. Juang, “Efficient multi-server password authenticated key agreement using smart cards,” IEEE Trans. Consumer Electron., vol. 50, no. 1, pp. 251–255, Feb. 2004.
- C. C. Chang and J. S. Lee, “An efficient and secure multi-server password authentication scheme using smart cards,” in Proc. Int. Conf. Cyberworlds, 2004, pp. 417–422.
- J.-L. Tsai, “Efficient multi-server authentication scheme based on one-way hash function without verification table,” Comput. Secur., vol. 27, no. 3C4, pp. 115–121, 2008.
- W. Tsaur, J. Li, and W. Lee, “An efficient and secure multi-server authentication scheme with key agreement,” J. Syst. Softw., vol. 85, no. 4, pp. 876–882, 2012.
- Y. Liao and C. Hsiao, “A novel multi-server remote user authentication scheme using self-certified public keys for mobile clients,” Future Generation Computer. Syst., vol. 29, no. 3, pp. 886–900, 2013.
- T. S. Messerges, E. A. Dabbish, and R. H. Sloan, “Examining smart-card security under the threat of power analysis attacks,” IEEE Trans. Comput., vol. 51, no. 5, pp. 541–552, May 2002.
- D. Wang and P. Wang, Offline Dictionary Attack on Password Authentication Schemes Using Smart Cards. New York, NY, USA: Springer International Publishing, 2015.

ACKNOWLEDGEMENT

We would like to place on record our deep sense of gratitude to Prof. S. B. Kalyankar, HOD-Dept. of Computer Science and Engineering, Deogiri Institute of Engineering and management Studies Aurangabad, for his generous guidance, help and useful suggestions.

We express our sincere gratitude to Dr. Pramod Bhalerao, Dept. of Computer Science and Engineering, Deogiri Institute of Engineering and management Studies Aurangabad, for his stimulating guidance, continuous encouragement and supervision throughout the course of present work.

We are extremely thankful to Dr. Ulhas Shiurkar, Director, Deogiri Institute of Engineering, and management Studies Aurangabad, for providing me infrastructural facilities to work in, without which this work would not have been possible.

Signatures of Students

Neha Sanjay Kumavat
Gayatri Ratan Puri
Mayuri Madhukarrao Kulkarni