INNOVARE JOURNAL OF ENGINEERING & TECHNOLOGY

Vol 6, Issue 1, 2018

ISSN - 2347-1573

Review Article

IMPLEMENTATION OF TWO-FACTOR AUTHENTICATION ACCESS CONTROL IN WEB-BASED SERVICES WITH CLOUD COMPUTING USING C#.NET

GOKILA R, MANIMARAN A

Department of Computer Applications, Karpagam College of Engineering, Coimbatore-32, Tamil Nadu, India.

Email:gokila.r@kce.ac.in

Received: 28 February 2018, Revised and Accepted: 29 March 2018

ABSTRACT

In this project, our propose preventing private information leakage at the phase of access authentication. I introduces two access control mechanism here: (1) user secret key and (2) security device. Our proposed mainly consists of two entities; they are attribute-issuing authority and trustee. Attribute-issuing authority is responsible to generate user secret key for each user. Trustee is responsible for initializing the security device. Secret key cannot use by user in another device. Security device content store inside the security device is not accessible nor modifiable once it is initialize. User can access the system means and both mechanisms are need. Detailed security analysis shows that the proposed two-factor authentication access control system achieves the desired security requirements.

Keywords: Cloud computing, Encryption, Decryption, Networks, Two-factor authentication.

INTRODUCTION

Cloud storage involves storing data on hardware in a remote location, which can be accessed from any device through the internet. Clients send files to a data server maintained by a cloud provider instead of as well as storing it on their own hard drives. Moreover, it is a service where data are remotely maintained, managed, and backed up. The service allows the users to store files in online so that they can access them remotely from any location through the Internet. Moreover, the digital data can also be stored in logical pools and it spans multiple-servers and the environment is fully owned and managed by a hosting company.

CLOUD COMPUTING

Cloud computing is a type of web-based computing paradigm that provides shared computer processing and resources on [1] demand. It enables on demand access to a shared pool of computer resources, networks, servers, storage, and applications. Cloud computing paradigm and storage solutions provide users and organizations with various capabilities to store and process their data in third-party data servers that may be located anywhere in the world.

Cloud environment provides high-capacity networks with minimum cost computers and storage devices. It also supports the implementation of hardware virtualization service-oriented architecture led to a growth in cloud computing [2]. Companies can scale up as computing needs increase and then scales down again as demands decrease. Before 10 years itself, it was reported as cloud computing had become a highly demanded service due to its cost benefits.

MOTIVATION

In an attribute-based access control system, each user has a user secret key issued by the authority. In practice, the user secret key is stored inside the personal computer. Another problem on web- based services is common that computers may be shared by many users, especially in some large enterprises or organizations. User secret keys could be easily stolen or used by an unauthorized party. Even though the computer may be locked by a password, it can still be possibly guessed or stolen by undetected malwares. To find solutions of above problems using two-factor authentication (2FA) method.

EXISTING SYSTEM

As sensitive data may be stored in the cloud for sharing, user authentication has become a critical component for any cloud system. A user is required to login before using the cloud services and using data stored in the cloud. There are two problems for the traditional system. One is that the account/password-based authentication is not privacy preserving. However, it is well acknowledged that privacy is an essential feature that must be considered in cloud computing systems. Another, it is common to share a computer among different people. It may be easy for hackers to install some spyware to learn the login password from the web browser. Second problem is common that computers may be shared by many users, especially in some large organizations.

Demerits

- Poor flexibility for the system.
- Unauthorized user also can access the system and get information from cloud.
- It is common to share a computer among different people. It is easy for hackers to learn login and password from web browser.

PROPOSED SYSTEM

In this project, a fine-grained two-factor access control protocol for web-based cloud computing services can compute some lightweight algorithms and it is tamper resistant. A more secured way is using 2FA. 2FA is very common among web-based services. In addition to a username/password, the user is also required to have a device to display a one-time password. Some systems may require the user to have a mobile phone while the one-time password will be sent to the mobile phone through SMS during the login process. Using 2FA, users will have more confidence to use shared computers. With this device, our protocol provides a 2FA security. First, the user secret key which is usually stored inside the computer is required. In addition, the security device should be also connected to the computer through USB to authenticate the user for accessing the cloud. The user can be granted access only if he has both items. Furthermore, the user cannot use his secret key with another device belonging to others for the access.

Merits

- Greater flexibility for the system to set different access policies according to different scenarios.
- Authorized user only can access the system. Access means with the necessity of both a user secret key and a lightweight security device.
- The user cannot use his secret key with another device.

SOFTWARE DESCRIPTION

Framework is designed to fulfill the following objectives

- To provide a consistent object-oriented programming environment whether object code is stored and executed locally but Internet- distributed,or executed remotely.
- To provide a code-execution environment that minimizes software deployment and versioning conflicts.
- To provide a code-execution environment that guarantees safe execution of code, including code created by an unknown or semi-trusted third party.
- To provide a code-execution environment that eliminates the performance problems of scripted or interpreted environments.
- To make the developer experience consistent across widely varying types of applications, such as Windows-based applications and web-based applications.
- To build all communication on industry standards to ensure that code based on the.NET framework can integrate with any other code.

FEATURES OF C#.NET-FRONT END

C# (pronounced as C-sharp) is a new language for windows applications, intended as an alternative to the main previous languages, C++ and VB. Its purpose is two folds:

It gives access to many of the facilities previously available only in C++, while retaining some of the simplicity to learn of VB. It has been designed specifically with the.NET Framework in mind and hence is very well structured for writing code that will be compiled for the. NET. C# is a simple, modern, object-oriented language which aims to combine the high productivity of VB and raw power of C++. C# is a new programming language developed by Microsoft.

Using C#, we can develop console applications, web applications, and windows applications. In C#, Microsoft has taken care of C++ problems such as memory management and pointers, so forth.

FEATURES OF SQL SERVER BACK END

The OLAP service feature available in SQL server version 7.0 is now called SQL server 2000 analysis services. The term OLAP services have been replaced with the term analysis services. Analysis services also include a new data mining component. The repository component available in SQL server version 7.0 is now called Microsoft SQL Server 2000 metadata services. References to the component now use the term metadata services. The term repository is used only in reference to the repository engine within metadata services

SQL-SERVER database consists of six types of objects.

They are as follows:

- Table.
- Query.
- Form.
- Report.
- Macro.

Table

A database is a collection of data about a specific topic.

Views of table

We can work with a table in two types:

1. Design view.
2. Datasheet view.

Design view

To build or modify the structure of a table, we work in the table design view. We can specify what kind of data will be held.

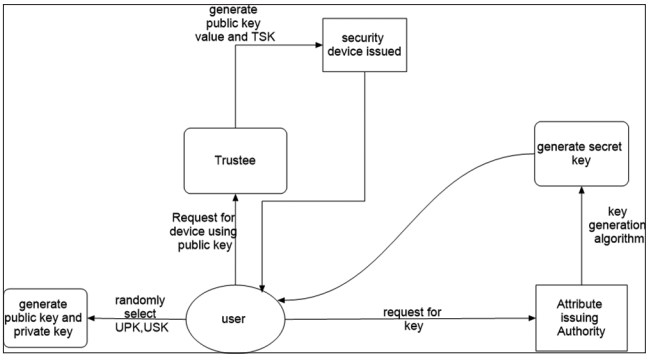
Datasheet view

To add, edit, or analyze the data itself, we work in table datasheet view mode.

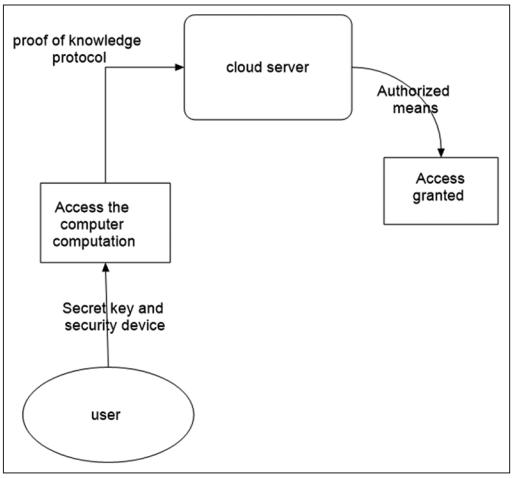
Query

A query is a question that has to be asked the data. Access gathers data that answer the question from one or more table. The data that make up the answer are either Dynaset (if you edit it) or a snapshot (it cannot be edited). Each time, we run query, and we get latest information in the Dynaset. Access either displays the Dynaset or snapshot for us to view or perform an action on it such as deleting or updating.

SYSTEM ARCHITECTURE

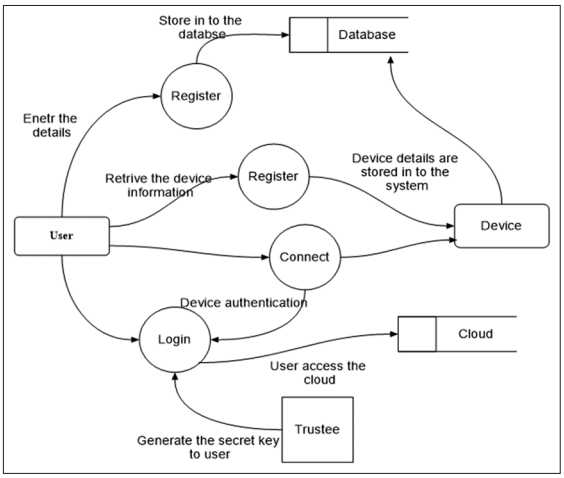


Key generation process



Access authentication process

Data flow diagram



IMPLEMENTATION

Key generation algorithm

Key generation is the process of generating secret keys. A key is used to encrypt and decrypt data being used. Symmetric key uses a single shared key keeping data secret. Public key algorithms use a public key and a private key. The public key is made available to anyone mostly in the form of a digital certificate. A sender encrypts data with the public key, and only the receiver of the private key can decrypt this data. In some cases, keys are randomly generated using a random number generator or pseudorandom number generator. A pseudorandom number generator is a computer algorithm that produces data that appear random under analysis. PNG that uses system entropy to begin data generally produces better results. It makes difficult for an attacker to guess.

Algorithm for proof of knowledge

An integer n=pq, where p and q are primes and x Î QR (n).
Protocol: Repeat lg n times the following steps:
Step 1: Peggy chooses a random v Î Z n* and sends to Vic
Step 2: y = v 2 mod n.
Step 3: Vic sends to Peggy a random i Î {0,1}.
Step 4: Peggy computes a square root u of x and sends to Vic
Step 5: z = u iv mod n.
Step 6: Vic checks whether
Step 7: z 2 ş x i y mod n.

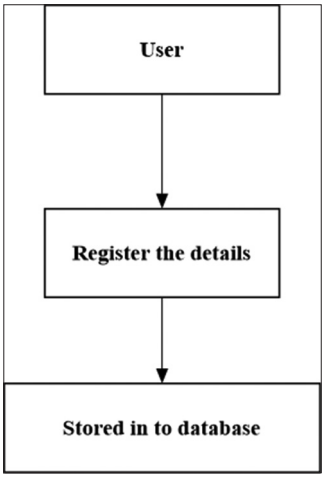
Algorithm key generation

Step 1. Generates 32 pseudo-random bytes with the seed key generator adding the user-supplied seed, U, if any.
Step 2. Set the 192-bit Triple UPK key, K, as the first 24 bytes generated in step 1, and set the seed, S, as the last 8 bytes.
Step 3. Set D as a 64-bit representation of the current date and time.
Step 4. Generates the 64-bit block X0 = G(S, K, D) where G is the X9.
Step 5. Set up to carry out continuous random number generator tests:
Step 6. For R = N, until R is equal to zero, do:
Step 7. Generates a final block Xf = G(S, K, D) and set P = Xf.
Step 8. Zero K, S, D, X, and any other internal buffers used. Retains L and P for subsequent use.

MODULES

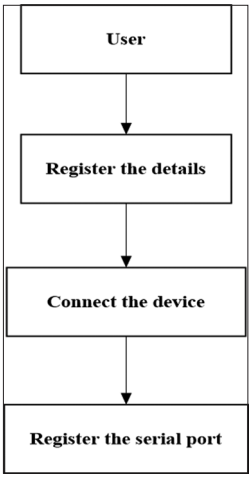
User registration and login

The data user creates their own login credential when they want entering in cloud. User enters the username, password, E-mail, mobile number, device letter, and serial port. These details are stored in database. User enters the username and password and then selects the login option. Authorized user only accesses for the cloud.



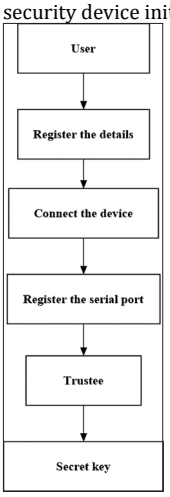
Device registration

User connects the device in system and registers the device details. User enters the serial port for device. Every time, login to the cloud user connects the device. This device used to provide a security for cloud user. The content stored inside the security device is not accessible nor modifiable once it is initialized. In addition, it will always follow the algorithm specification.



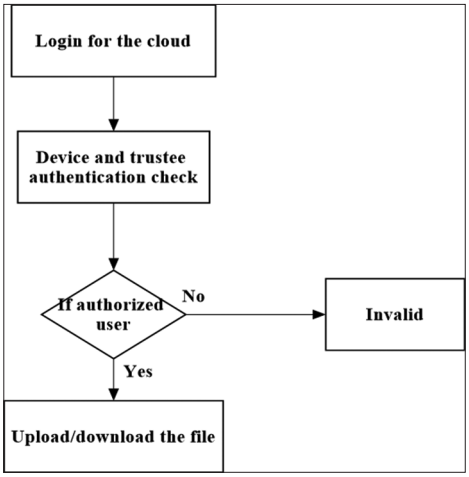
Trustee authentication

This module is responsible for generating all system parameters, initializes the security device, and also assumes that trustee generates the security parameters according to the algorithm prescribed. Other potential attacks such as IP hijacking, distributed denial-of-service attack, and man-in-the-middle attack are out of the scope of this project. It is the player that makes authentication with the cloud server. Each user has a secret key issued by the attribute-issuing authority and a security device initialized by the trustee.



Upload and download the file

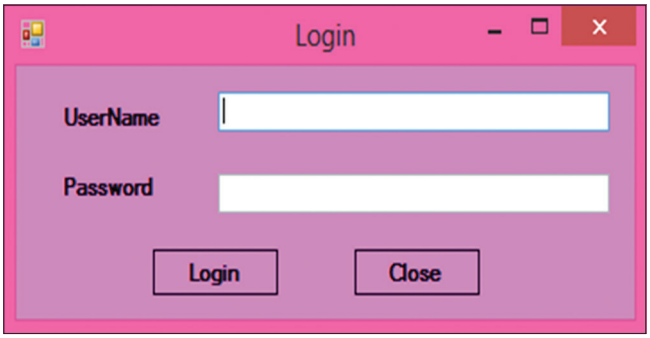
All the dynamic data operations are done in this module. Here, I implements a protocol for this, i.e. the protocol for provable update. All the block level operations such as modification, insertion, updating, and deletions are done in this module. The encrypted file is downloaded from the server to the user to access the file. The files are downloaded in the decrypted format. The user can able to download the data. The data which were encrypted from the cloud were encrypted by the server. The client can able to download the file from the server. Now, the file which was downloaded by the client is in encrypted format. The data which were in the encrypted format are now decrypted automatically by the client.

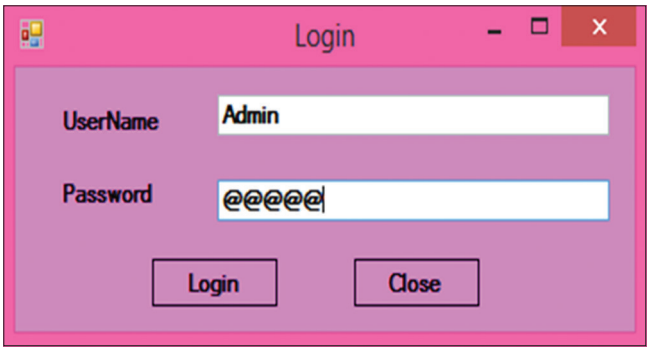


SAMPLE SCREENSHOTS

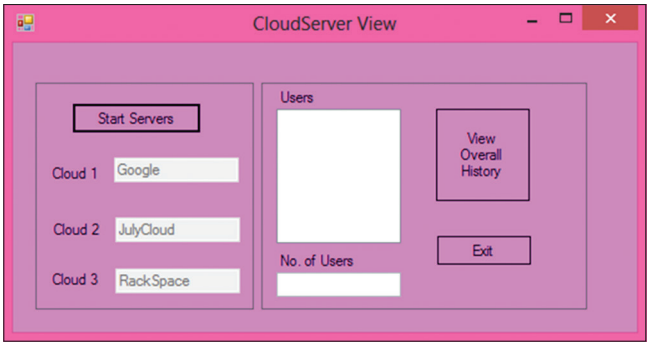
Login form

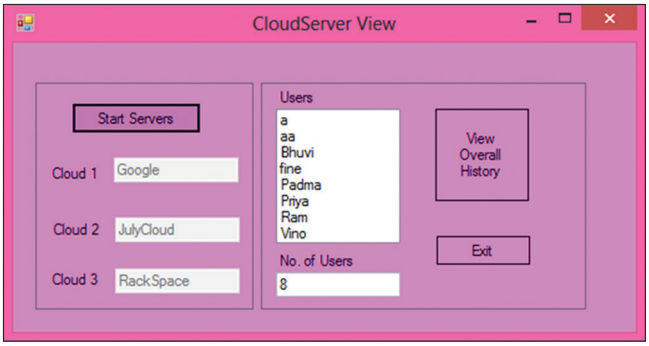
User enters the username and password and then clicks the login option.





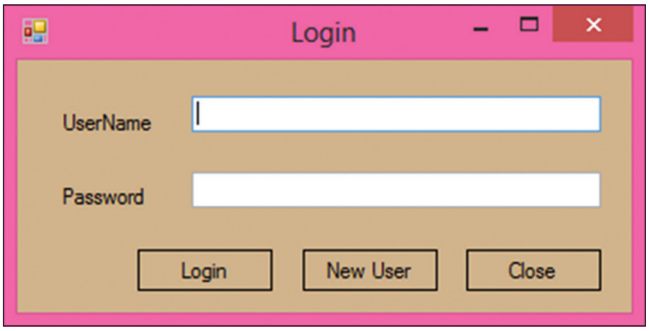
Cloud server selection

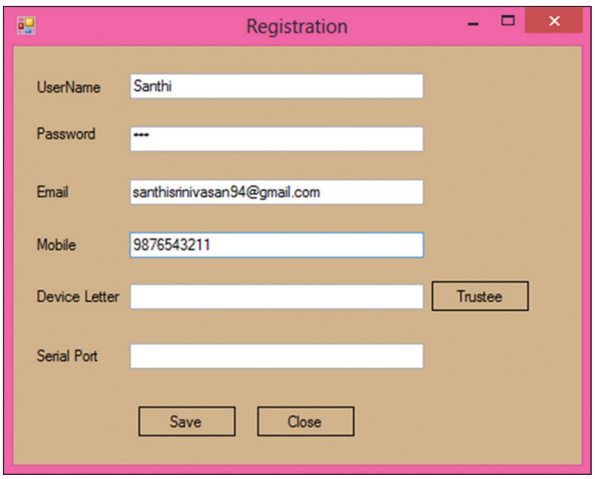


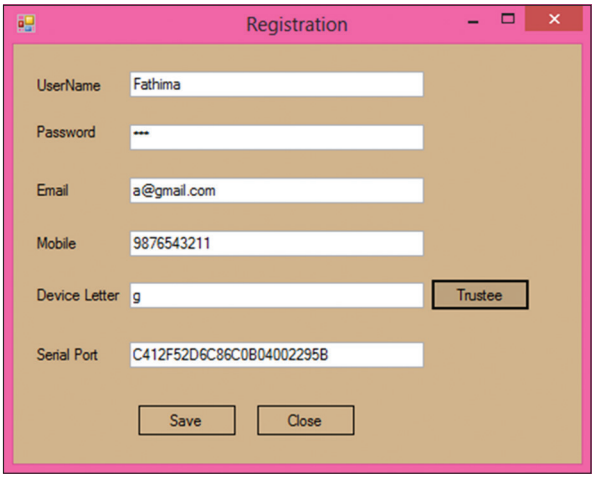


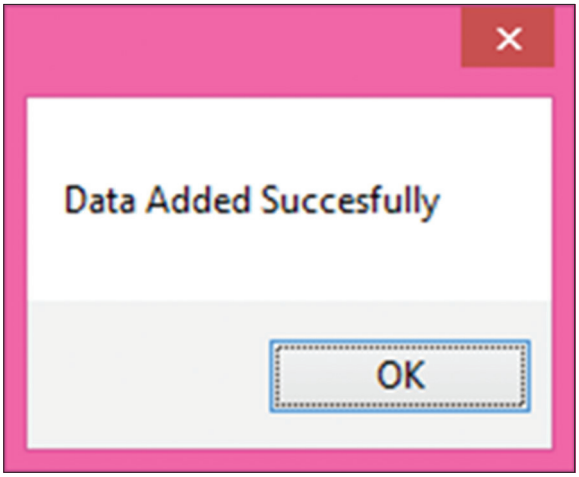
User registration form

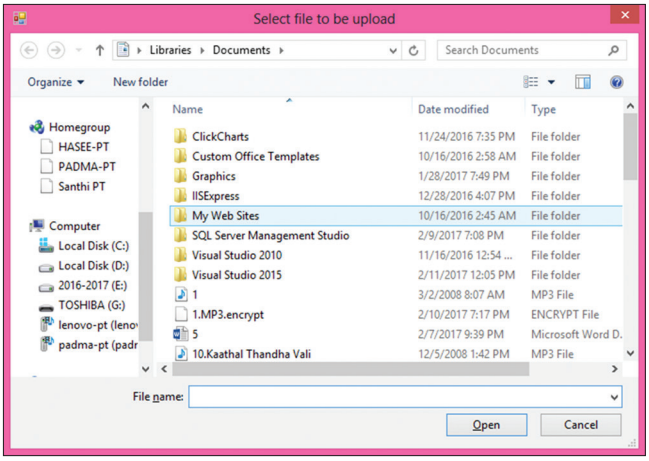
User registers the username, password, E-mail, mobile, device registration, and serial port. These details are stored in database.

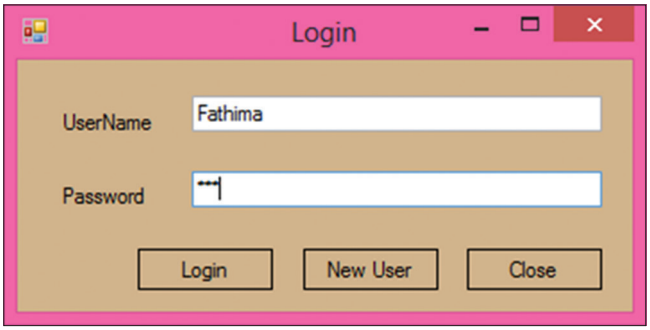




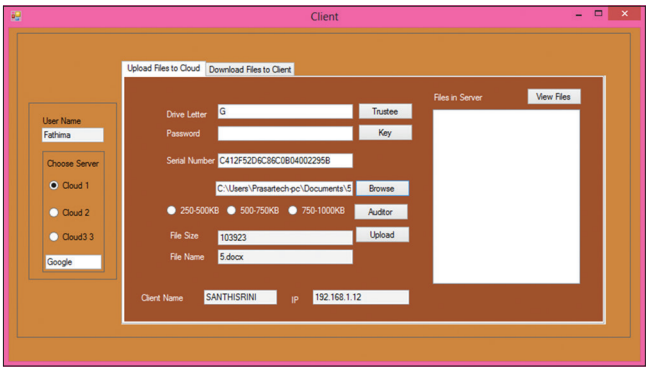






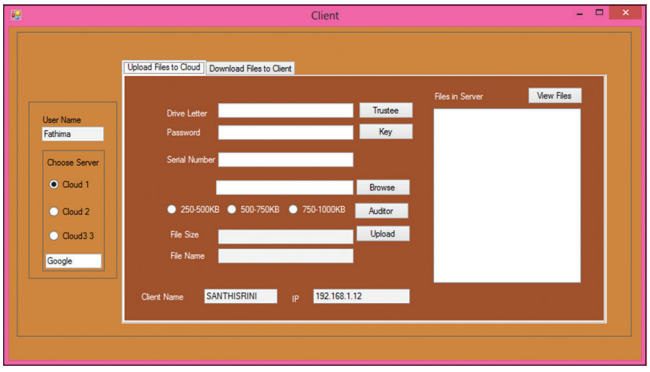


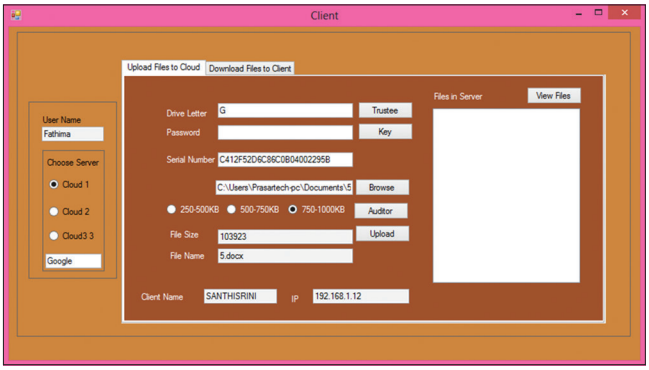
Login form

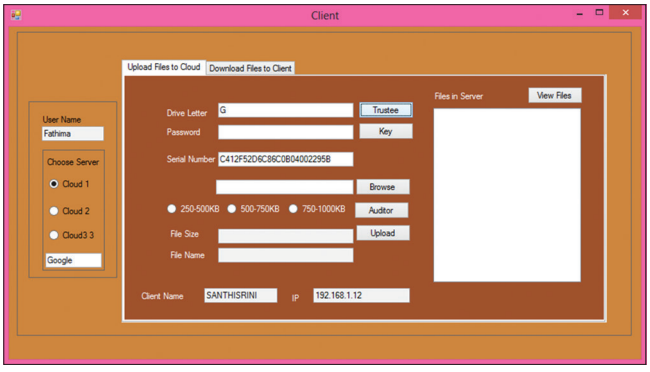


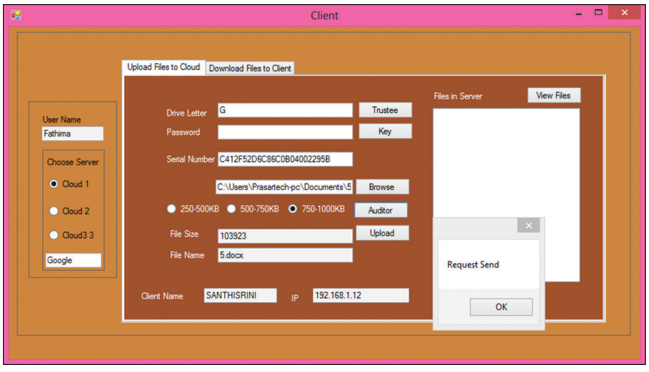
Upload and download form

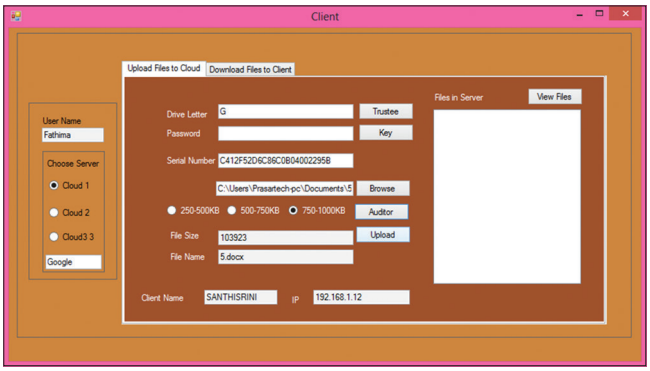
User clicks the trustee option and connects the device and then browses the file in the system, enters the serial port number, and clicks the upload option.

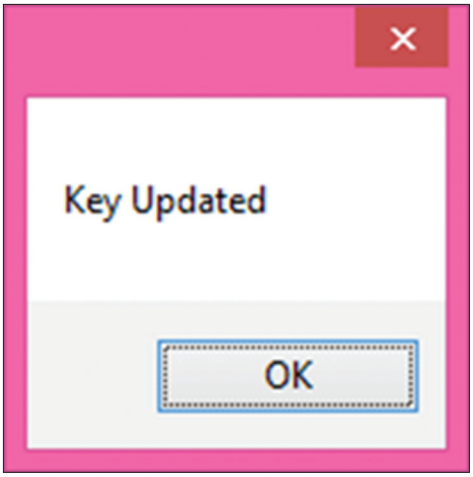




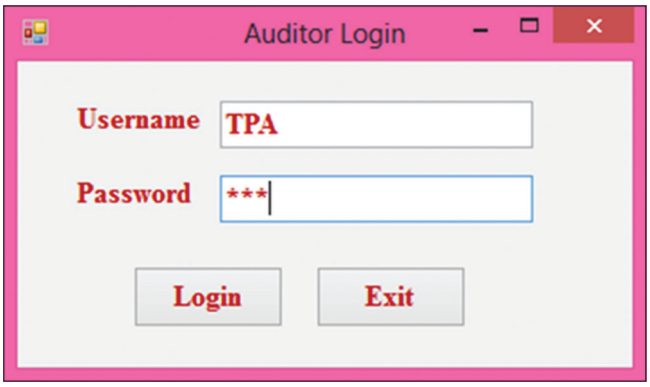


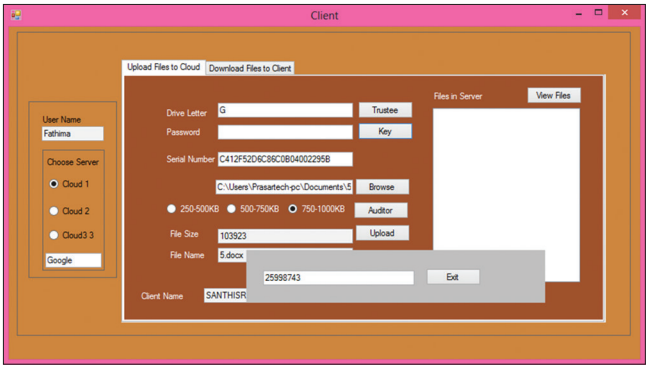


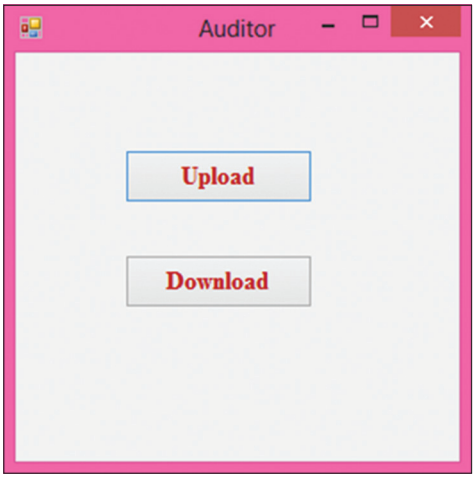


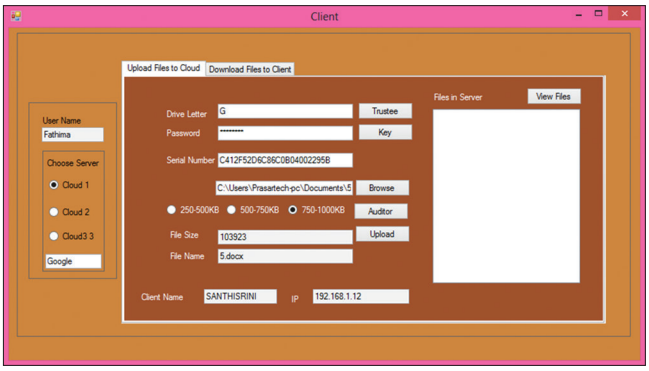


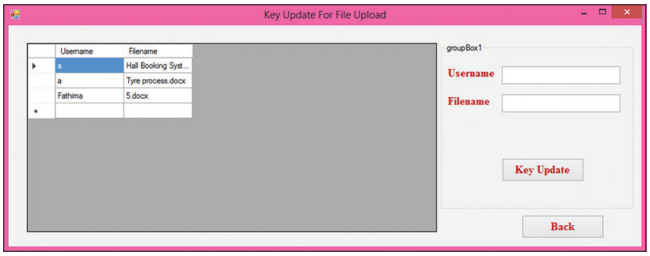
Key generation form

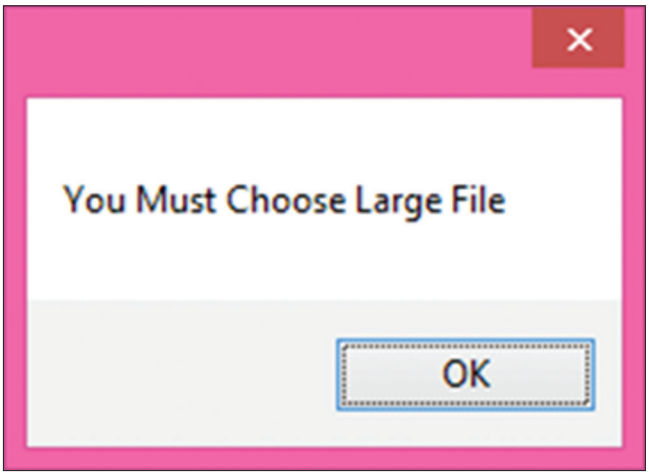


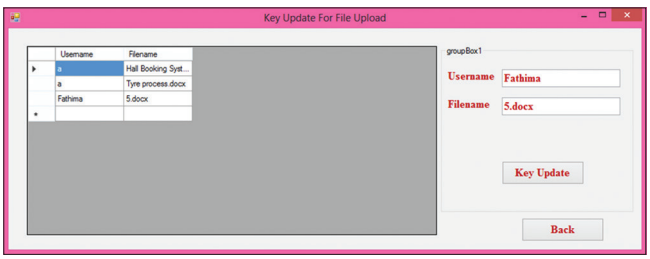


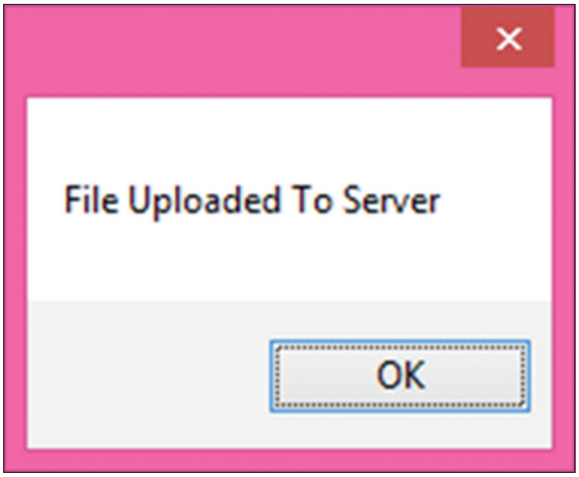






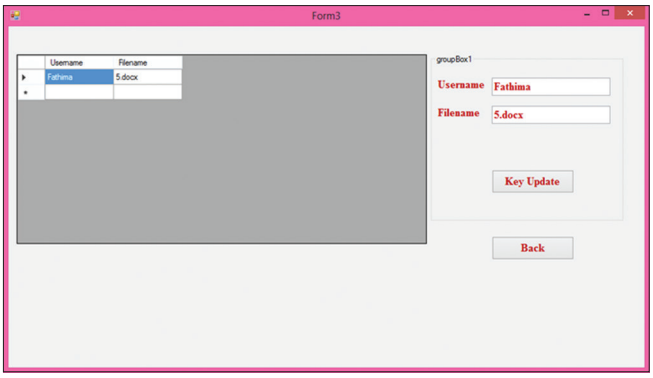




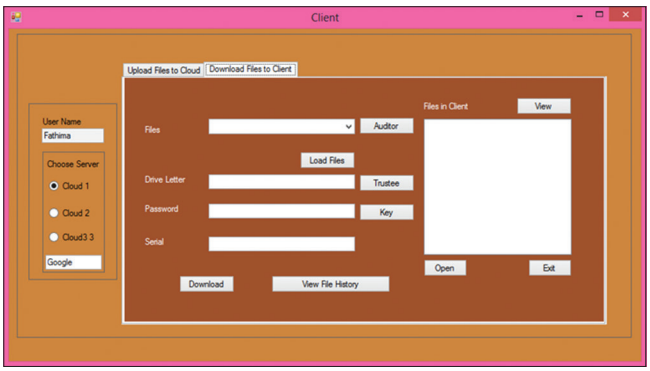


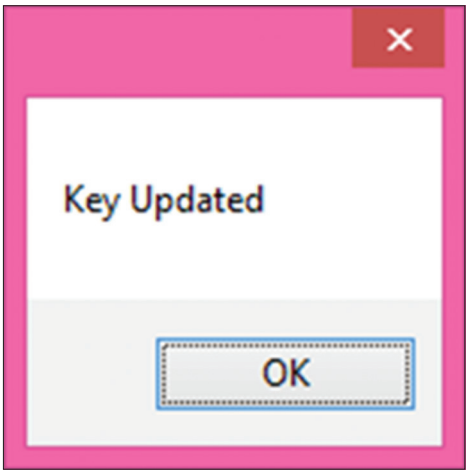
Key generation

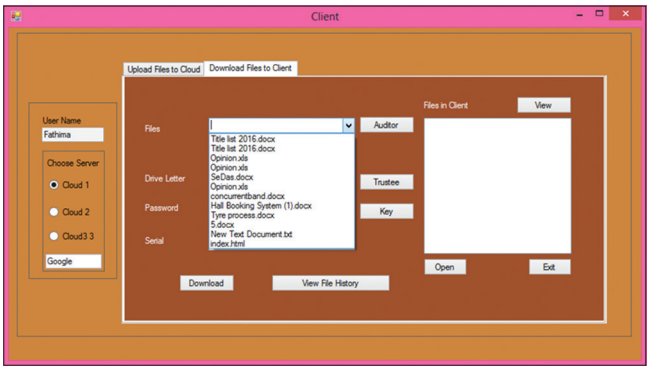
Enter the username and select the file option. Then click the key update option and secret key send to the user.

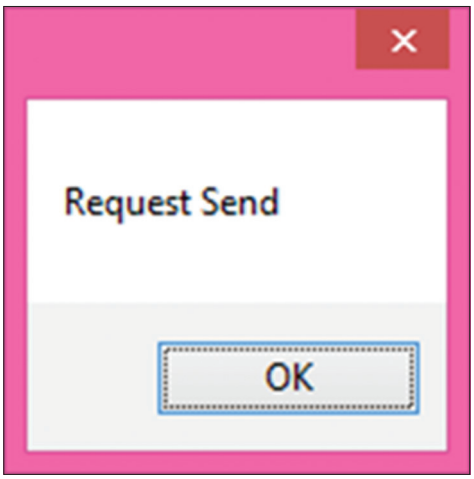


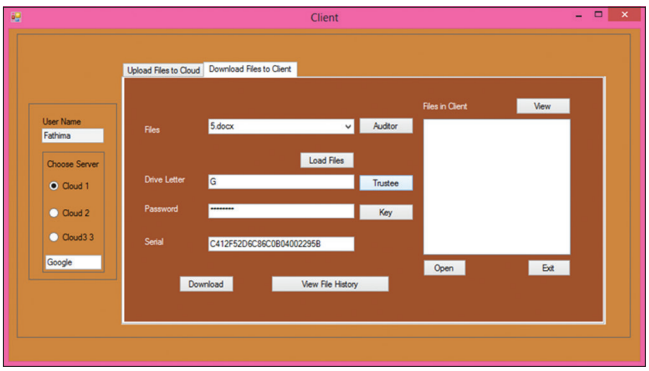
Download form

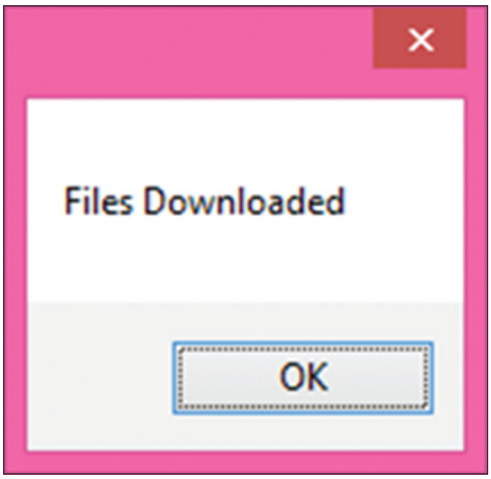












CONCLUSION

In this project, we achieved security and privacy for web-based cloud services. I have presented in this project a new 2FA including both user secret key and a lightweight security device access control system for web-based cloud computing services. 2FA access control system has been identified to enable the cloud server as well as to restrict the access to those users with the same set of attributes and also preserve user's privacy. Security analysis showed that the implemented system achieves the desired security measures.

FUTURE WORK

In future, our proposed method improved efficiency up to 100%, then reduced costs of the system security device, and then increased operational efficiencies, scalability, and flexibility.

REFERENCES

1. Geetha D, Gokila R, Manoharan R. review of security services in cloud computing and management. Asian J Res Soc Sci Hum 2014;4:189-98.
2. Mary AL, Gokila R, Maheswari KU. Integration of cloud computing with internet of things with security. Int J Pure Appl Math 2018;18:313-7.
3. Au MH, Kapadia A. PERM: Practical reputation-based blacklisting without TTPS. In: Raleigh, NC, USA: Proc. ACM Conf. Comput. Commun. Secur. (CCS); 2012. p. 929-40.
4. Au MH, Kapadia A, Susilo W. BLACR: TTP-Free Black Listable Anonymous Credentials with Reputation. In Proc. 19th NDSS; 2012. p. 1-17.
5. Au MH, Susilo W, Mu Y. Constant-Size Dynamic k-TAA. In Proc. 5th Int. Conf. SCN; 2006. p. 111-25.
6. Baek J, Vu QH, Liu JK, Huang X, Xiang Y. A secure cloud computing based framework for big data information management of smart grid. IEEE Trans Cloud Comput 2015;3:233-44.
7. Bellare M, Goldreich O. On Defining Proofs of Knowledge. In Proc. 12th Annu Int CRYPTO; 1992. p. 390-420.
8. Bethencourt J, Sahai A, Waters B. Ciphertext-Policy Attribute- Based Encryption. In: Proc. IEEE Symp. Secur. Privacy; 2007. p. 321-34.
9. Boneh D, Boyen X, Shacham H. Short Group Signatures. In Advances in Cryptology. Berlin, Germany: Springer-Verlag; 2004. p. 41-55.
10. Boneh D, Ding X, Tsudik G. Fine-grained control of security capabilities. ACM Trans Internet Technol 2004;4:60-82.