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

Mrs.R.GOKILA¹ MCA., M.Phil., ISTE., IACSIT., ICST
Assistant Professor
Department of Computer Applications
Karpagam College of Engineering
Coimbatore-32

Manimaran.A, Vijaya Kumar.K
Student-MCA
Department of Computer Applications
Karpagam College of Engineering
Coimbatore-32

ABSTRACT

In this project, our propose preventing private information leakage at the phase of access authentication. We introduce 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 initialize 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 both mechanism are need. Detailed security analysis shows that the proposed 2FA access control system achieves the desired security requirements.

KEY WORDS

Cloud Computing, encryption, decryption, networks, 2FA.

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. And it is a service
where data is 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. And the digital data can also be stored in logical pools and it span 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 demand. It enables on demand access to a shared pool of computer resources, networks, servers, storage, 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 implementation of hardware virtualization service-oriented architecture led to a growth in cloud computing. Companies can scale up as computing needs increase and then scale 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, it 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, 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 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 two-factor authentication (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. By 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 in order 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, 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.

FEARTURES 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++, 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, pointers, so forth.

**FEATURES OF SQL SERVER – BACK END**

The OLAP Services feature available in SQL Server version 7.0 is now called SQL Server 2000 Analysis Services. The term OLAP Services has been replaced with the term Analysis Services. Analysis Services also includes a new data mining component. The Repository component available in SQL Server version 7.0 is now called Microsoft SQL Server 2000 Meta Data Services. References to the component now use the term Meta Data Services. The term repository is used only in reference to the repository engine within Meta Data Services.

SQL-SERVER database consist of six type of objects,

They are,

- 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 hold.
Datasheet View:

To add, edit or analyses the data itself we work in tables datasheet view mode.

Query:

A query is a question that has to be asked the data. Access gathers data that answers the question from one or more table. The data that make up the answer is either dynaset (if you edit it) or a snapshot (it cannot be edited). Each time we run query, 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 use 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 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 appears random under analysis. PNG that use system entropy to begin data generally produce better results. It makes difficult for an attacker to guess.

Algorithm for proof of knowledge

An integer \( n = pq \), where \( p, q \) are primes and \( x \in \mathbb{QR}(n) \).

Protocol: Repeat \( \log n \) times the following steps:

Step 1: Peggy chooses a random \( v \in \mathbb{Z}^* \) and sends to Vic

Step 2: \( y = v^2 \mod n \).

Step 3: Vic sends to Peggy a random \( i \in \{0,1\} \).

Step 4: Peggy computes a square root \( u \) of \( x \) and sends to Vic

Step 5: \( z = u^i \mod n \).

Step 6: Vic checks whether

Step 7: \( z^2 \equiv x^i y \mod n \).

Algorithm key generation:

Step 1. Generate 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. Generate the 64-bit block $X_0 = G(S, K, D)$ 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. Generate a final block $X_f = G(S, K, D)$ and set $P = X_f$.


**MODULES**

**User registration and login:**

The data user create their own login credential when they want entering in cloud. User enter the user name, pass word, E-mail, mobile no, device letter, serial port. These details are stored in database. User enter the user name and password then select the login option. Authorized user only access for the cloud.

![User registration diagram]

**Device registration:**

User connect the device in system and register the device details. User enter the serial port for device. Every time login to the cloud user connect 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:

In this module responsible for generating all system parameters and initialize the security device. Also assume that trustee generates the security parameters according to the algorithm prescribed. Other potential attacks, such as IP hijacking, distributed denial-of-service attack, man-in-the-middle attack, etc., 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 implement a protocol for this i.e. the protocol for provable update. All the block level operation such as modification, insertion, updating, 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 was encrypted from the cloud was encrypted by the server. The client can able to download the file from the server.
server. Now the file which was downloaded by the client is in encrypted format. The data which was in the encrypted format is now decrypted automatically by the client.

SAMPLE SCREENSHOTS

Login form:

User enters the user name and password. Then click the login option.
Cloud server selection:
User Registration Form:
User registers the user name, password, E-mail, mobile, device registration and serial port. These details are stored in database.
Upload and download form:
User click the trustee option and connect the device. Then browse the file in the system. Enter the serial port number and click the upload option.
Key generation form:
Download Form:
Key Generation:
Enter the user name and select the file option. Then click the key update option and secret key send to the user.
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% and then reduced costs of the system security device then increased operational efficiencies, scalability, and flexibility.

REFERENCES
