ISSN : 2321-9602

Indo-American Journal of Agricultural and Veterinary Sciences




editor@iajavs.com
iajavs.editor@gmail.com

Indo-Am. J. Agric. & Vet. Sci., 2021 *ISSN 2321–9602 www.iajavs.com*

Indo-American Journal of Agricultural and Veterinary Sciences

Vol. 9, Issue 1, Jan 2021

FINE-GRAINED TWO-FACTOR ACCESS CONTROL FOR WEB-BASED CLOUD COMPUTING SERVICES

V.LAVANYA1, G.LAKSHMIKANTH2

1M.Tech, Dept of CSE, Sree Rama Engineering College, Tirupati, AP, India.
2Associate Professor & HOD, Dept of CSE, Sree Rama Engineering College, Tirupati, AP, India.

Abstract – For web-based cloud computing services, we provide a novel, finely grained approach of two-factor authentication (2FA). Specifically, in our proposed 2FA access control system, a user secret key and a lightweight security device are required to create an attribute-based access control mechanism. It is possible that the technique, which prevents users from accessing the system unless they have both, might increase the system's security, particularly when several users share a computer for web-based cloud services. It is also possible to limit access to just those users who share a set of qualities, while ensuring user privacy, since the cloud server only knows that the user meets the requisite predicate, but it does not know their actual identity. Finally, we run a simulation to show that our suggested 2FA system is feasible.

I. INTRODUCTION

Computer hardware and software are provided as a service over a network in "the cloud" (the term used to describe the concept) (typically the Internet). As a system diagram symbol, a cloud-shaped cloud is often used as an abstraction for the complicated infrastructure it represents. A user's data, software, and processing are transferred to a third-party service through cloud computing. The term "cloud computing" refers to the use of computer resources that may be accessed through the Internet and controlled by a third party. A wide range of high-end server computer networks and high-end software programmes may be accessed using these services.

It is possible to distribute data processing tasks among a large number of low-cost consumer PCs connected through specialised networks in the cloud. All of the computers in the shared IT infrastructure are connected to one another. In order to get the most out of cloud computing, virtualization is often used.

In accordance with NIST's criteria, the following are some of the most significant features of cloud computing:

II. It is possible for a customer to supply computer capabilities, such as server time and network storage, on demand without needing human intervention from each service's supplier.

III. Capabilities are made accessible across the network and accessed via standard protocols that encourage their usage by diverse thin or thick client systems (e.g., mobile phones, laptops, and PDAs).

IV. Providers use a multi-tenant approach in which distinct physical and virtual resources are constantly allocated and reassigned based on client demand for computing resources. It's possible to declare a place at a higher level of abstraction while still maintaining a feeling of location independence since the customer

typically has no control or knowledge of the specific location of the delivered resources (e.g., country, state, or data center). Virtual machines, storage, computation, and network bandwidth are all examples of resources. Capabilities may be supplied fast and elastically, sometimes automatically, to enable rapid scaling out and expansion. Consumers generally believe that provisioning capabilities are boundless and may be acquired at any moment, in any number.

VVI. Using a metering capability relevant to the kind of service, cloud systems may automatically regulate and optimise resource utilisation (e.g., storage, processing, bandwidth, and active user accounts). The use of resources may be monitored, regulated, and reported, allowing both the supplier and the user of the service to be transparent. Errors are discovered during testing. Work products must be thoroughly tested before they can be released to the general public. You may use it to verify the performance of components, sub-component, assembly, and/or a final product's functionality In order to ensure that the Software system satisfies its requirements and user expectations and doesn't fail in an undesirable way, it is put through its paces by doing software exercises. There are a variety of tests available. Each test type is designed to meet a certain need.

VII. SYSTEM ANALYSIS

A. EXISTING SYSTEM

Concerns around security and privacy for web-based cloud services have emerged as a result of the cloud computing paradigm shift. User authentication has become an essential part of any cloud system because sensitive data may be kept in the cloud for sharing purposes or quick access; and qualified users may also use the cloud system for different apps and services. Before utilising cloud services or gaining access to sensitive data stored in the cloud, users must first check in. The typical account/password-based approach has two flaws.

There are certain issues with the current system:

1) First and foremost, the old method of account/password authentication does not protect users' personal information. Cloud computing solutions must, however, take privacy into account as a critical aspect.

In addition to this, it is normal for many individuals to use the same computer at once. Installing spyware to steal a user's login password from their web browser may be a simple task for hackers.

3) Even if a password is used to secure the computer, malware that has not been identified may still guess the password and take control of the machine.

B. THE SYSTEM I'M TALKING ABOUT

A lightweight security device is used in this research to propose a fine-grained two-factor access control mechanism for web-based cloud computing services. The following characteristics describe the gadget: A tamper-resistant design means that no one can break into it to acquire the secret information held inside, and it can perform certain lightweight algorithms, such as hashing and exponentiation.

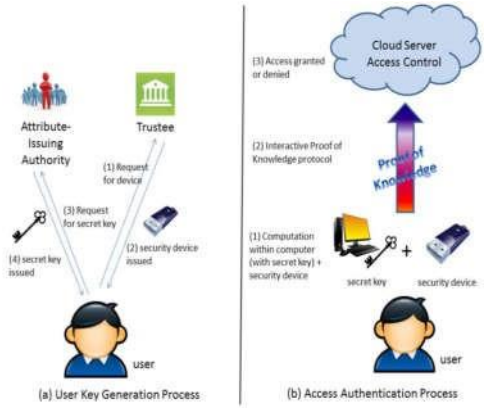
The Proposed System's Benefits:

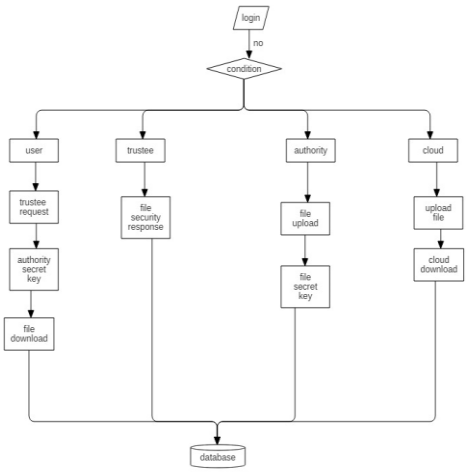
Our system has a two-factor authentication (2FA) feature.

A key feature of our protocol is the ability to create multiple access permissions depending on different conditions and offer the system with significant flexibility. In the meanwhile, the user's privacy is protected.

THE ARCHITECTURE OF THE SYSTEM

It is the interface between the user and the information system. There are a variety of ways to enter data into a computer, including reading it from a written or printed document or having humans input it directly into the system. This includes defining specifications and processes for data preparation. The goal of input design is to maintain the process as easy as possible while also reducing the quantity of input necessary, reducing mistakes, and preventing delays. The input is set up in such a manner that it offers convenience and security while also





DATA FLOW DIAGRAM:

DFD is another name for the bubble chart. For example, it is possible to express a system in terms of input data, processing of this data, and output of this data created by this system in a simple graphical formalism.

2) One of the most essential modelling tools is the data flow diagram (DFD). Models the system's components. External entities that interact with and utilise system data as well as internal information flow are all included in this list.

3) DFD illustrates the information flow and changes that occur when data passes through the system. It's a visual representation of how data goes from input to output and the modifications that take place along the way.

4) DFD is sometimes referred to as a "bubble chart." A DFD may be used at any level of abstraction to depict a system. DFD may be broken down into a series of levels that indicate increasing degrees of information flow and operational depth.

UML DIAGRAMS

The acronym UML refers to a standard modelling language. UML is an object-oriented software engineering modelling language that is widely used. The Object Management Group is in charge of overseeing and developing the standard.

It is hoped that the use of UML would lead to the widespread adoption of object-oriented computer software models. There are two main parts to UML right now: a Meta-model and a notation. A method or process may also be added to or related with UML in the future.

There is a common language for describing, visualising, building and documenting software system artefacts and other non-software system models called the Unified Modeling Language (UML).

Modeling huge and complicated systems has been made easier with the use of the Unified Modeling Language (UML).

An essential aspect of object-oriented software development is the use of the UML. A large portion of the UML's notation is based on graphical representations of software designs.

GOALS:

The following are the primary aims of the UML design:

An expressive visual modelling language should be available for users to create and trade meaningful models.

Give the key principles the flexibility and specialisation they need.

3) Be able to work with a variety of programming languages and frameworks.

Formalize the modelling language and make it easier for students to grasp its idioms

Make it easier for people to get into the OO tools market.

6) Allow for higher-level notions like collaborations, frameworks, patterns, and components to be implemented in your application.

Integrate the best practises.

CASE DIAGRAM:

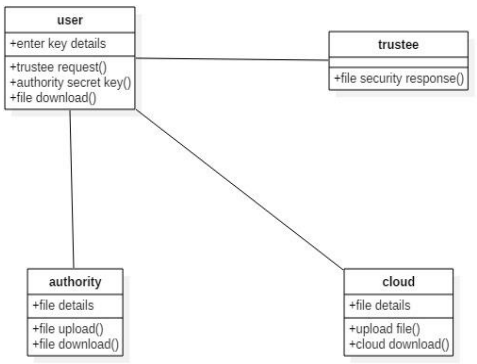
Diagrams in the Unified Modeling Language (UML) based on use cases are known as use cases in the UML. Use cases, actors, and any relationships between them are all depicted graphically to provide a clear picture of the system's capabilities. A use case diagram's primary goal is to explain how the system performs for each actor. System actors may be portrayed by their responsibilities in the system.

USE CASE DIAGRAM:

Diagrams in the Unified Modeling Language (UML) based on use cases are known as use cases in the UML. Use cases, actors, and any relationships between them are all depicted graphically to provide a clear picture of the system's capabilities. A use case diagram's primary goal is to explain how the system performs for each actor. System actors may be portrayed by their responsibilities in the system.

CLASS DIAGRAM:

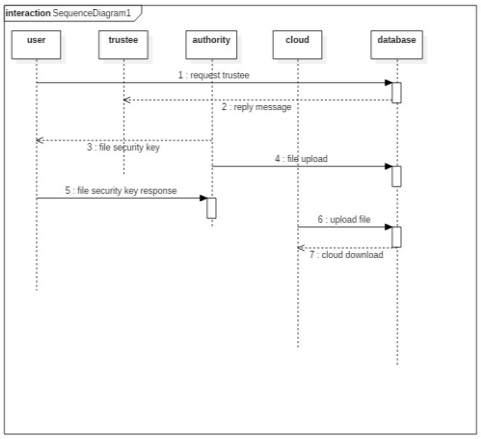
In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains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



SEQUENCE DIAGRAM:

In the Unified Modeling Language (UML), a sequence diagram depicts the order in which processes interact with one another. A Message Sequence Chart is the basis for this diagram. Some people call sequence diagrams event diagrams, events scenarios, or timing diagrams, depending on the context.

It provides services to anonymous authorized users. It interacts with the user during the authentication process.



ACTIVITY DIAGRAM:
Activity diagrams are visual representations of processes that include choice, iteration, and concurrency as well as sequential tasks and actions. For example, activity diagrams may be used to depict the step-by-step operational processes of system components in the Unified Modeling Language (UML). The complete control flow may be seen using an activity diagram.
MODULES
We have four modules in this implementation:
Attribute Authorization Module (AAM)

3) The User Module.

4) Provider Module for Cloud Services

The following is a summary of the content in this module:

Trustee:

System settings are generated and the security device is initialised.

The source of the attribution:

For each user, it generates a unique user secret key based on their qualities.

User:

The player is in charge of establishing an encrypted connection to the cloud server. All users have access to a secret key granted by the attribute-issuing authority, and a security device that has been initialised by the trustee.

Provider of Cloud Computing:

CONCLUSION

In this research, we provide a novel 2FA (two-factor authentication) access control solution for web-based cloud computing services that includes both a user secret key and a lightweight security device. By using a two-factor authentication (2FA) access control system, the cloud server may limit access to just those users who have the same set of qualities, while simultaneously safeguarding the privacy of those users' personal information. The suggested 2FA access control system has been thoroughly analysed in terms of security and is found to meet the necessary levels of security. We were able to establish that the construction is "viable" through performance assessment. We leave it up to the future to increase the system's efficiency while retaining all of its pleasant features.

REFERENCES

[1] In the first place, there's A. Kapadia and M. H Au. No need for TTPS with PERM's reputation-based blacklisting. The ACM Conference on Computer and Communications Security (CCS'12), held in Raleigh, NC, USA from October 16-18, 2012, was edited by T. Yu, G. Danezis and V. D. Gligor. ACM, the year in question is 2012.
[2] In addition to Au, Kapadia and W. Susilo [2, 3], Ttp-free, anonymous, blacklistable credentials with reputation are known as Blacr.

The Internet Society, 2012, in NDSS (National Digital Standards Society).
[3] The Constant-Size Dynamic k-TAA. M. H. Au, W Susilo, and Y. In Lecture Notes in Computer Science, Volume 4116, Pages 111–125. New York City, 2006.
[4] This study was conducted by four researchers: Baek, Vu, Liu, and Xiang in collaboration with Baek, Baek, and Xiang. A smart grid data management architecture based on secure cloud computing. Computing in the Cloud, 3(2):233–244, IEEE Transactions on.
[5] M. Bellare and O. Goldreich, respectively. Knowledge proofs are defined. Lecture Notes in Computer Science 740: CRYPTO, pages 390–391
[6] Springer, 1992, p. 420; reprint.
[7] Sixth Generation: J. Bethencourt, A. Sahai, & B. Waters Encryption based on ciphertext policy attributes. Presented at the IEEE Symposium on Security and Privacy, 321–333. Computer Society of the IEEE, 2007.
[8] D. Boneh, X. Boyen, and H. Shacham are three of the authors. The signatures of a small group. Referenced in Franklin [19], particularly pages 41–55.
[9] Boneh, Boneh, and Tsudik. The ability to fine-tune security measures. (2004) 4(1):60–82 of the ACM Transactions on Internet Technology
[10] According to [9] J. Camenisch, Discrete Logarithm Problem-Based Group Signature Schemes for Payment Systems. thesis completed in 1998 at the Swiss Federal Institute of Technology (ETH). Reprint as ETH Series in Information Security and Cryptography, vol. 2, Hartung-Gorre Verlag, Konstanz, ISBN 3-89649-286-1, 1998.
[11]
J. Camenisch, M. Dubovitskaya, and G. Neven are the authors. Transfer with access control that is blind. This paper was published in the Proceedings of the 2009 ACM Conference on Computer and Communications Security (CCS 2009), which was held in Chicago from November 9–13, 2009. It was co-authored by S. Jha and A. D. Keromytis. In 2009, the ACM.