IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 9, September 2021

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 9, September 2021 ||

| DOI:10.15680/IJIRSET.2021.1009048 |

Attribute based 2Factor Authentication for Cloud Computing

Ganavi J[1], Amith S Bharadwaj[2]

Software Engineer, Altiostar, Bengaluru, India[1]

Software Engineer, Sakha Global, Bengaluru, India[2]

ABSTRACT:In this paper, we introduce a new two-factor authentication (2FA) access control system for web-based cloud computing services. Specifically, in our proposed 2FA access control system, an attribute-based access control mechanism is implemented with the necessity of both a user secret key and a lightweight security device. As a user cannot access the system if they do not hold both, the mechanism can enhance the security of the system, especially in those scenarios where many users share the same computer for web-based cloud services. In addition, attribute-based control in the system also enables the cloud server to restrict the access to those users with the same set of attributes while preserving user privacy, i.e., the cloud server only knows that the user fulfils the required predicate, but has no idea on the exact identity of the user. Finally, we also carry out a simulation to demonstrate the practicability of our proposed 2FA system.

KEYWORDS:Cloud Storage, Encryption, Data Blocker, Cryptography, Two Factor Authentication.

I. INTRODUCTION

Cloud computing is a virtual host computer system that enables enterprises to buy, lease, sell, or distribute software and other digital resources over the internet as an on-demand service. It no longer depends on a server or a number of machines that physically exist, as it is a virtual system. There are many applications of cloud computing, such as data sharing, data storage, big data management, medical information system etc. End users access cloud-based applications through a web browser, thin client or mobile app while the business software and user's data are stored on servers at a remote location. The benefits of web-based cloud computing services are huge, which include the ease of accessibility, reduced costs and capital expenditures, increased operational efficiencies, scalability, flexibility and immediate time to market.Attributes of cloud computing typically include scalability, elasticity, multi-tenancy, payment models that are linked to usage, resources delivered from virtualized environments and the provision of all support and management tasks by a cloud services provider." The concept of a "Private Cloud" can have all of the same properties defined by Andy. In larger enterprises, there is an Internal IT Infrastructure "service provider".

II. SYSTEM DESIGN

Admin

Admin is a super user who creates the Data Trustee user and maintains the cloud servers' configurations. He has the writes to Add, Edit or Delete any number of Broker.

Once the admin logged in he has following functions.

- Cloud Storage(Update)
- Recharge
- Data Broker (Add, Edit, Delete)
- Key Generation (View, Update)
- Department (View Only)
- Designation(View Only)
- Change Password

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 9, September 2021 ||

| DOI:10.15680/IJIRSET.2021.1009048 |

Multi Cloud

In Space and service prediction Application we are providing the four cloud storage sever for storing data from all the available clouds storage which meet the performance requirement, that is, they can offer acceptable throughput and latency when they are not in outage. The storage mode transition does not impact the performance of the service. Since it is not a latency-sensitive process, we can decrease the priority of transition operations, and implement the transition in batch when the proxy has low workload.

Data Hosting

Data Hosting stores data using replication or erasure coding, according to the size and access frequency of the data. Storage Mode Switching (SMS) will decide the replication process for storing the client datas. The implementation of changing storage mode runs in the background, in order not to impact Client Application. Data Hosting and SMS are two important modules in Space and service prediction. Data Hosting decides storage mode and the clouds that the data should be stored in. This is a complex integer programming problem demonstrated in the following subsections.

Storage Mode Switching

In Storage mode Switching proxy, it will get the Cloud Storage Server credential from the DB like Size of the file in KB, Cost for the Uploading File. Availability Cloud Storage based on this credential it will get the Cloud Storage server Details .Then Using FTP Protocol it will connect to cloud to store the user data.

Cost Process

To Show the Multi-Cost Data Hosting, we have to collect the Cloud Storage Server Details like Cost, availability, Price etc., The Cost Details will be calculating by in KB.

Broker

Broker is a person who will store the files in cloud which in turn accessed by the authorized Data user. Trustees are likeLiberian who will upload all the files in the system. Whenever the file is uploaded it will be encrypted by the system using Broker Encryption Key. Broker has to specify the Hierarchical Access Policy for each and every file. Access policies are set using Department Attribute and Designation Attribute.Broker can able to create the Data user and he has to send them Attribute based Decryption Key. Attribute based Decryption Key means it contains the Trustee Decryption Key and Data user Attribution Set (Department, Designation).

Data User

Data user are the data access users, suppose Broker is a college Liberian then data User are like students, lectures and admin staff in a college.Data user will receive their access key (Attributed based Decryption Key) from respective broker through email and lightweight security device.With the help of the access key they can able to download the files for which they have access, remember access control is set by data owner.Suppose the data user wants to download any file, first he has to select the file from the list and the system ask for the access key, After system getting the access key it will separate the Attribute Set from the key and check for the access rights, if the user has the access he can download the encrypted file which in turn decrypted using the decryption key and download to the data consumer local system.

III. IMPLEMENTATION

Encryption of Secret Data

In this, the admin assigns a unique DNA sequence and a unique key to every user which is later used to create the DNA reference sequence for the user using rand() function and hash set constructs.

There is an original data M which the client decides to upload via a network to cloud computing environments. So, there are three sub-phases to provide the final form of M which is M´´´ and upload it to cloud. The data M is read as integer and converted to binary form.

In order to convert binary data into amino acids as a DNA sequence, the base pairing rules must be used. Synthesizing nucleotides in real environment (biology) is done in constant rules.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 9, September 2021 ||

| DOI:10.15680/IJIRSET.2021.1009048 |

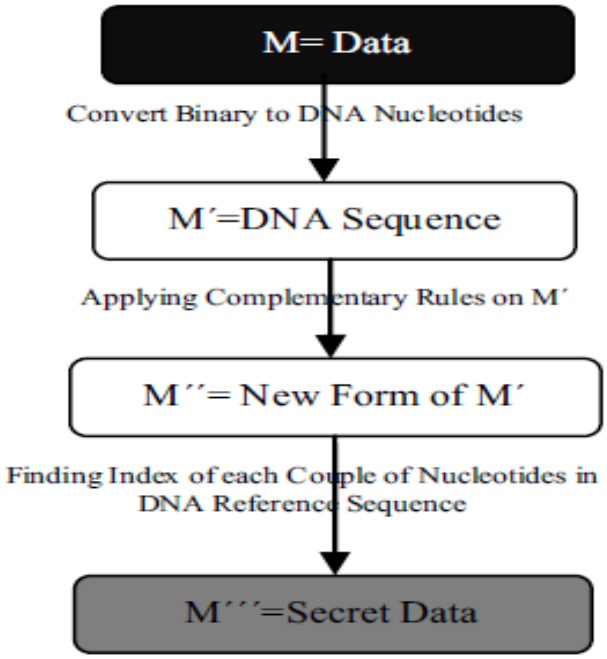

Figure 3.1 Encryption Process

Extracting Original Data

Client2 takes the secret data in form of some numbers. For the purpose of extracting the original data from DNA reference sequence, phase two with its sub phases will extract the original data, correctly depicted in figure 3.2.

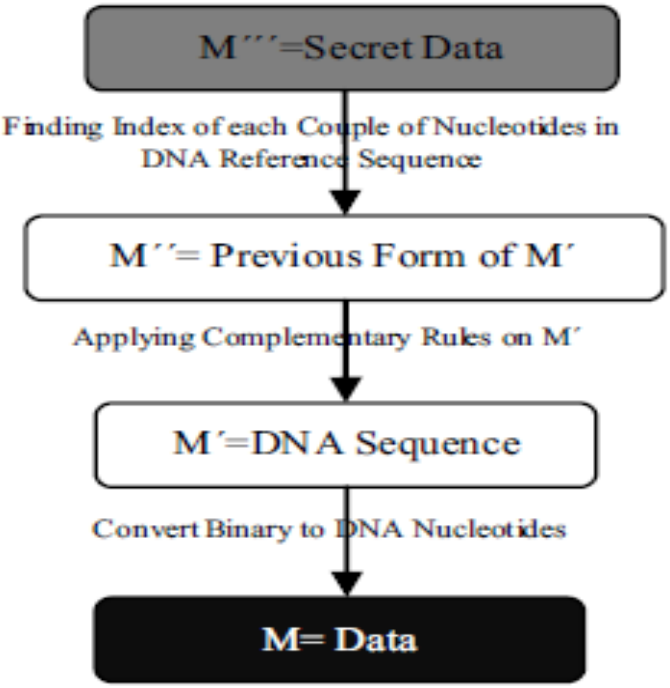

Figure 3.2 Decryption Process

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 9, September 2021 ||

| DOI:10.15680/IJIRSET.2021.1009048 |

When the user is uploading a file from his local machine to web server, it has to be redirected to DNA Encryption Service which is running in cloud server 1 and Cloud server 1 will encrypt the file and the encrypted file has to send to cloud server 2 using web service concept which will store in cloud server 2.

Sequence Diagram

Sequence diagram is the kind of UML diagram, the interaction between the users it show how processes operate with one another and in what order. The messages are constructed in the form of sequence chart. In sequence diagram objects and classes are involved, and messages are exchanged between the object in the sequence form. Another name of the sequence diagram is event diagram, timing diagram.

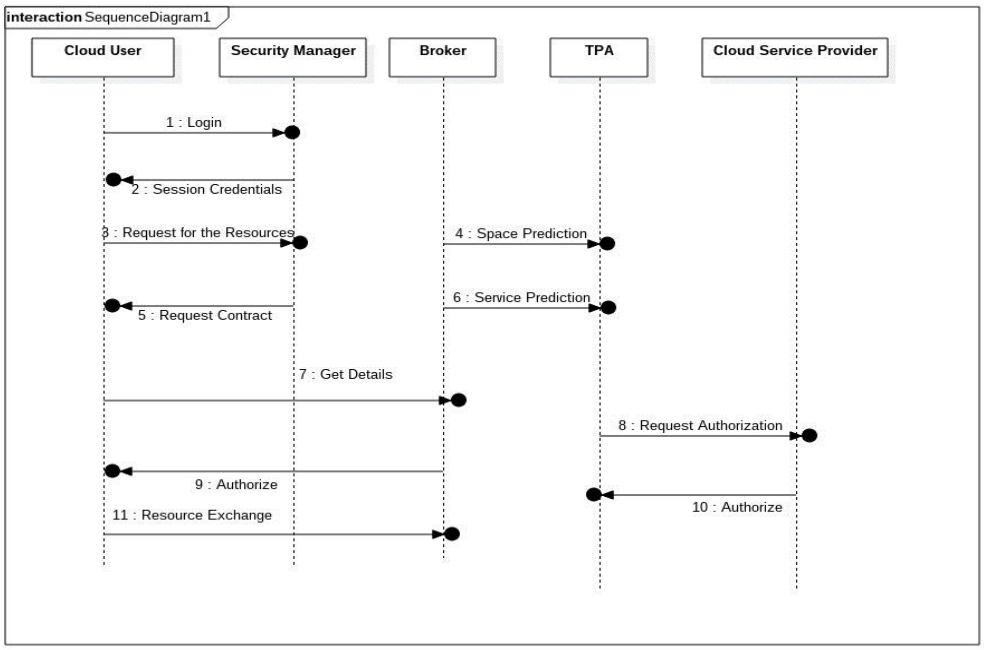

Figure 3.3 Sequence diagram of overall flow

- First step is to cloud user send the request to the broker with necessary user id and password.
- Cloud user request for the resources to the security manager, with user status.
- The security manager sends the request to the cloud user for the contract.
- The cloud users get the details and request service offering supported operations.
- The broker sends request to the TPA where space and service prediction is done and then the cloud service provider for the request authorization.
- The cloud service provider authorizes the requested by the cloud user.
- Cloud user can exchange resource between cloud user and broker.

IV. TESTING ANALYSIS

Validation Testing

Validation testing is a concern which overlaps with integration testing. Ensuring that the application fulfils its specification is a major criterion for the construction of an integration test. Validation testing also overlaps to a large extent with System Testing, where the application is tested with respect to its typical working environment. Consequently for many processes no clear division between validation and system testing can be made.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 9, September 2021 ||

| DOI:10.15680/IJIRSET.2021.1009048 |

Table 1. Test Case

Test ID	Test Cases	Expected Output	Actual Output	Status
1	All set of fields in the login form are to be filled by the admin and should click on submit button	A new form will be displayed.	A page is displayed.	pass
2	wrong admin name or password is entered	Error message is popped to re type the user name and password correctly.	Alert message is shown displaying the user to re enter valid user name and password.	Pass
3.	View transactions	A new form will be displayed with transactions.	A page will be displayed with all users file uploaded transactions.	pass
4.	All set if fields in the login form are to be filled by the user and should click on submit button	A new form will be displayed.	A page is displayed.	pass
5.	wrong user name or password is entered	Error message is popped to re type the user name and password correctly.	Alert message is shown displaying the user to re enter valid user name and password.	Pass
6.	Connect, update	linked and updated	linked and updated	Pass
7.	Uploading file	message is popped to with statues.	Alert message will be displayed with success status	Pass
8.	Checking files	Deduplication process .	It will check for the deduplication based	Pass

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 9, September 2021 ||

| DOI:10.15680/IJIRSET.2021.1009048 |

			on this process hash code will generated.	
9.	Hash code generate	A 32character hash code will be generated in the cloud.	Based on file content a hash code will be generated.	Pass
10.	Manage users and profiles	Different operations	Results as according to mode	Pass
11.	Logout	All options verified	Results as accordingly made	Pass

V. CONCLUSION

In this paper, we have presented a new 2FA (including both user secret key and a lightweight security device) access control system for web-based cloud computing services. Based on the attribute-based access control mechanism, the proposed 2FA access control system has been identified to not only enable the cloud server to restrict the access to those users with the same set of attributes but also preserve user privacy. Detailed security analysis shows that the proposed 2FA access control system achieves the desired security requirements. Through performance evaluation, we demonstrated that the construction is "feasible". We leave as future work to further improve the efficiency while keeping all nice features of the system.

REFERENCES

[1] Balachandra Reddy Kandukuri, RamkrishnaPaturi V, DR. AtanuRakshit, "Recent Developments in Cloud Based Systems", 2009 IEEE International Conference on Services Computing.

[2] Neha Ramesh Dodke, Sweta Kale," Cloud computing security", IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308.

[3] "Service Level Agreement and Master Service Agreement", http://www.softlayer.com/sla.html, accessed on April 05, 2009

[4] Meiko Jensen, J¨orgSchwenk, Nils Gruschka, Luigi Lo Iacono," Towards Secure Brokerage , Aggregation and Cloud Bursting", 2009 IEEE International Conference on Cloud Computing.

[5] Mehmet Yildiz, JemalAbawajy, TuncayErcan and Andrew Bernoth, "T-Broker: A Trust-Aware Service Brokering Scheme for Multiple Cloud Collaborative Services", 10th International Symposium on Pervasive Systems, Algorithms, and Networks, 2009 IEEE.

[6] P. T. Endo, "Resourcalocation for distrbuted cloud: Concept and Research challenges", IEE, pp. 42-46.

[7] "Virtualization and Cloud Computing: Optimized Power, Cooling, and Management Maximizes Benefits Adaptive Management of Virtualized Resources in Cloud Computing Using Feedback Control", First International Conference on Information Science and Engineering, **(2010)**.

[8] B. Oiza, "survey on reliable sla-based monitoring for billing scheme in cloud computing", International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622www.ijera.com, vol. 2, no. 1, **(2012)**, pp. 793-797 793.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details