Smart City's Security Model for Management of Image Data on Cloud

Pooja[1,*], Manish Kumar Mukhija[1], Satish Kumar Alaria[2]
[1]Department of Computer Science & Engineering, AIET, Jaipur, India
[2]Department of Electronics & Communication, AIET, Jaipur, India
Emails: poojasinghsfdc@gmail.com;manishkrmukhija82@gmail.com; satish.alaria@gmail.com

Abstract

In modern world of advancement, cloud technology is taking its grip. COVID-19 also enhance the use of the cloud services. The cloud concept comes with the new advancement of technology, but with that data breaches and data hacks are also increasing. In the cloud-based environment, we suggested the model of security enhancement which, make use pf role-based security model where the files are shared according to the role and the access of such file is controlled using TPA validation and apart for that the concept of authentication of user is also suggested using the Pattern Lock based graphical system for pattern formation. The pattern obtained are validated using the various of online password or pattern strength validation tools, results which are obtained proves that pattern obtained through the proposed concept performs better against the attack.

Keywords: Cloud Environment; Cloud Security; TPA; Role Based Access

1. Introduction

Cloud computing is an altogether flexible and smart establishment for running HPC, attempt an all-cloud climate portrays an association, affiliation or individual that utilizes a Web-based application for every task rather than presenting programming or taking care of data on a PC. All-cloud conditions are not ordinary, yet rather a development toward this is a somewhat long goal for cloud enrolling fans and cloud industrialists.[1]
There are various anticipated that benefits should an all-cloud climate, including the ability to get to all your work, programs and different information from any contraption. Regardless, an all-cloud environment is at this point a to some degree novel thought and there are numerous unanswered requests, similar to what happens if a cloud provider goes down or bankrupt. In actuality, the primary clients to enter an all-cloud environment will be individuals, as associations have more restrictive data to worry about. [1].

2. Literature Survey

S. R. Shree et.al 2020, [1] Optimization acknowledges a colossal part in different issues that anticipate the particular yield. Security of the informational collection away in distant experts forward obviously dependent upon secret key one which is then utilized with the end goal of encryption and furthermore then for the deciphering reason. Different bizarre key age assessments, for example, the RSA, AES are accessible to make the key. The key made by such estimationsshould be streamlined to give additional vital security to your information from unapproved clients comparably as from the TPA who will check their information for dependability reason. In this paper a method to overhaul the bewildering key by then utilizing cuckoo search calculation (CSA) is proposed.
A. Thakare, et.al 2020 [2] Duties are isolated inside a social occasion by utilizing the work-based acceptance control (RBAC) in the Azure Internet of Things (IoT) struc-ture, and basically a proper degree of access is given up to clients to perform unequivocal errands, reliant upon a given circumstance. Regardless, a near affirmation and

Doi: https://doi.org/10.54216/JCHCI.020101

Received: June 25, 2021 Accepted: November 25, 2021

underwriting structure is utilized for "kind of client," which develops the development over-inconvenience on the cloud worker. Additionally, taking into account its RBAC nature, the IoT structure is wasteful in managing a stunning circumstance where different clients demand equivalent sorts of assets, by making several re-hashed positions.

H. Belkhiria, et.al 2020 [3] In the area of cutting-edge genuine constructions, the im-prove-ment of Smart Living Spaces (SLS) plan offers individuals the chance to benefit with better philosophies for living. Such mechanical model that fuses a few pieces of bit-by-bit life, permits the inhabitants of the space to even more plausible adjust and control their current circumstance. SLS stresses, basically, energy preservation, accommodation and solace likewise as clinical thought concerns.

A. Suganthy and V. Prasanna Venkatesan, 2019 [4] With the ending up webbing and its related drives, the affiliations are more anxious in offering security to their assets. Access control models helps in giving very far to the clients when the assets are being gotten to by them and Role based enlistment control (RBAC) model is one such ac-cess control instrument in which the clients access the re-sources subject to the posi-tions they get in the framework.

3. Proposed work

The proposed concept in divided into two main segments,

1. Role Based Security
    a. According to the role-based security, the files are assigned for access for the particular role.
2. TPA Based Security
    a. TPA is the third party auditor which will cross check the user requests to access the file and generate OTP and Access Key.

A. New User Creation

[In order to access the services related to cloud sharing platform, first the user required to be registered using the platform, then the user can access the services.]

Step 1: First the user name , name of employee and role of employee are specified.

Step 2: Grid of the Pictures available for selection and the user has to select single image from it.

Step 3: The image is partitioned in small segments and the image in organized in the second grid.

Step 4: The size of the image selected is calculated and displayed in bytes.

Step 5: The use then select the segments of image , the selected segment turns gray and after all the desired image blocks are selected , click on the generate button.

Step 6: The Pattern will formed , on the basis of the selection of image block and the basis of pattern is ,

Image(ImageNumber)_part(partnumber1)_sizeofimage_
Image(ImageNumber)_part(partnumber2)_sizeofimage_

::::

Image(ImageNumber)_part(partnumberN)_sizeofimage_

Step 6: Save the pattern with the other details of the user in the database table meminfo , which contains the details of registered users.

Step 7: END.

B. Existing User Login

[Now, after the registration is done, the registered user can login using the procedure adopted for registration]

Step 1: Enter the user name.

Step 2: Grid of the Pictures available for selection and the user has to select single image from it.

Step 3: The image is partitioned in small segments and the image in organized in the second grid.

Step 4: The size of the image selected is calculated and displayed in bytes.

Doi: https://doi.org/10.54216/JCHCI.020101

Received: June 25, 2021 Accepted: November 25, 2021

Step 5: The use then selects the segments of image, the selected segment turns gray and after all the desired image blocks are selected, click on the generate button.

Step 6: The Pattern will formed , on the basis of the selection of image block and the basis of pattern is ,

Image(ImageNumber)_part(partnumber1)_sizeofimage_
Image(ImageNumber)_part(partnumber2)_sizeofimage_

::::

Image(ImageNumber)_part(partnumberN)_sizeofimage_

Step 6: If Details Correct then

Login Successful

Else

Login Failed

[End of If structure.]

Step 7: END.

C. File Upload

[This algorithm is used to uploading the file on the server, according to role.]

Step 1: Access username according to session variable

Step 2: Select the File to Shared.

Step 3: Select the role for which the file is to be shared.

Step 4: Store the details in the database table fuploads.

Step 5: Stop.

D. File Request

[This algorithm is used to request the file access from TPA]

Step 1: Select the name of file for which access to be requested.

Step 2: Save Details in the Reqdata which is table for user requests.

Step 3: Autoincrement based request ID is generated.

Step 4: Stop

E. TPA Grant Access

[This algorithm is used to grant the access to the user requesting the file.]

Step 1: Select the Request ID.

Step 2: Fetch the file details and user details

Step 3: Generate OTP which generated using 10 random numbers and each range from 30 to 126 and the character corresponding to these number will be combined in order to form the OTP.

Step 4: Generate Hash using SHA-512 algorithm for file which is requested and Hash of user name who requested the file. Now, extract 20 characters from Hash of File and 20 characters of Hash of Username to generate the access key.

Step 5: Save the details in the database table reqdata for the requested ID.

Step 6: End.

F. User Accessing File

[This algorithm is used access the file requested]

Step 1: Select the Request ID.

Doi: https://doi.org/10.54216/JCHCI.020101

Received: June 25, 2021 Accepted: November 25, 2021

Step 2: Fetch the file details.

Step 3: Enter OTP and Accesskey.

Step 4: If Details Correct then:

File Download

Else

Invalid Details

[End of If structure]

Step 5: End.

4. Implementation and Result Analysis

The proposed work is implemented using the Visual Studio Environment and SQL Server as the database for storage based simulation.

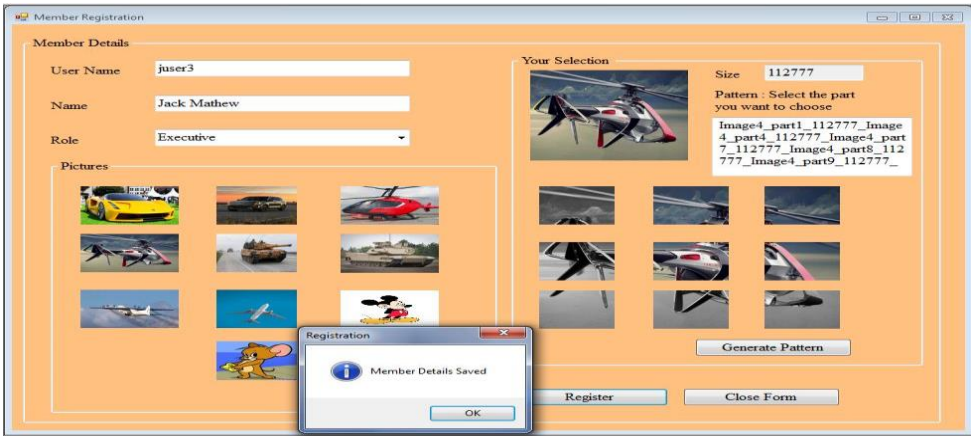

Figure 1: User Registration

In the fig 3, user registration process is shown in which the concept which we have shown for the purpose of authentication of users is depicted. In the registration process, new user has to specify their own role and as well from the set of the images provided have to select the image and then that image is partitioned in the nine equal parts and organized in the form of the grid and just like we form the pattern password in mobile we will slide over the images to select them and one the basis of the select the pattern will be formed. The patter includes the image number, then the part number of the image, then size and so on for all the part. After specification of the all the details, the new user's details will then be stored in the database.

Now when we have to talk about the access module then it requires the formation of the OTP with the request ID , The process of the generation of the OTP constitute the extraction of the SHA-512 Hash first 20 character and similarly the 20 characters of Hash of user name , which is then also combined with the range numbers which will then range from the 30-126 series.

Device 1: Rumkin Test

This secret word checker will measure your secret key and give it a score dependent on how great of a secret phrase it is.

Authentication Key:

Image5_part1_155666_Image5_part4_155666_Image5_part7_155666_Image5_part8__155666_Image5_part9_155666_

Access Key:

e026ea23e40021c0086fB0BE79A29AB853C20553

Doi: https://doi.org/10.54216/JCHCI.020101

Received: June 25, 2021 Accepted: November 25, 2021

TABLE 1. Analysis of Keys Test 1

	Authentication Key	**Access Key**
Proposed Approach	445.1	168.8

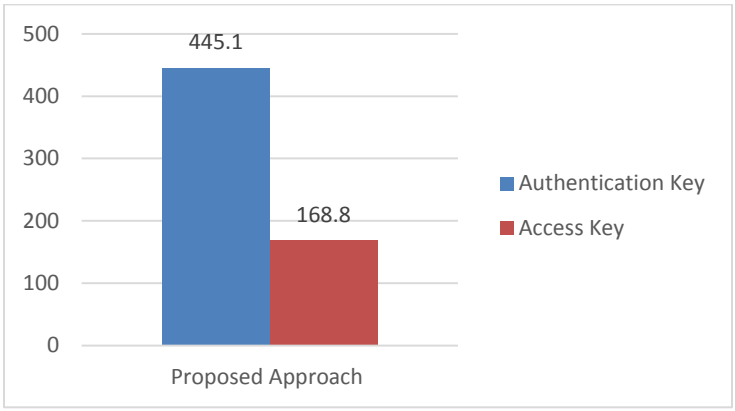

Figure 2: Key Analysis 1 Graph

Device 2: Cryptool

CrypTool is an open-source tools for examining password strength

TABLE 2. Analysis of Keys Test 2

	Authentication Key	**Access Key**
Proposed Approach	3.621	3.865

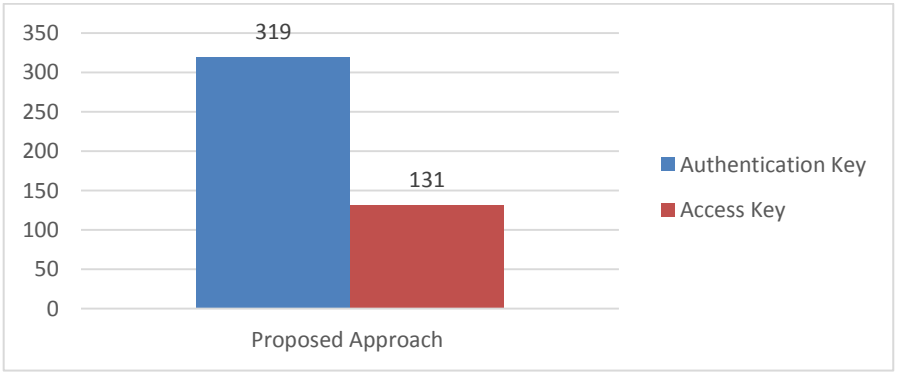

Figure 3: Key Analysis 2 Graph

TABLE 3. Analysis of Base Keys Test 2

	Access Key

Doi: https://doi.org/10.54216/JCHCI.020101

Received: June 25, 2021 Accepted: November 25, 2021

Base Approach	3.57

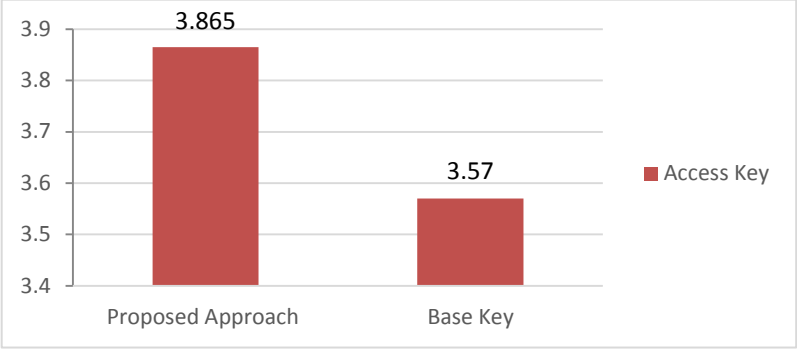

Figure 4: Analysis 2 Base and Proposed Graph

5. Conclusion

Two principle issues which is for the most part confronted, when information is partaken in cloud environment, first is confirming the client who can get to the information, and besides, the solid the actual information. Seeing the worry, we favorable to represent the half and half idea which includes the Role Based Security just as TPA based Security. The pattern obtained are validated using the various of online password or pattern strength validation tools, results which are obtained proves that pattern obtained through the proposed concept performs better against the attack.In future we will try to implement this model in the real-time environment and will try to suggest for its use in cloud based banking serves and more. Together with that we will also try to explore the new dimensions in the field of cloud based security.

6. References

1. Akkaoui, R., Hei, X., Guo, C., & Cheng, W. (2019). RBAC-HDE: On the design of a role-based access control with Smart contract for healthcare data exchange IEEE International Conference on Consumer Electronics—Taiwan (ICCE-TW), Yilan, Taiwan, 2019 (pp. 1–2).
2. Alaria, S. K., & Kumar, A. (2018). Implementation of new Cryptographic Encryption Approach for Trust as & Service (TAAS) in Cloud Environment. International Journal of Computers and Applications, 4(July–August)(8), (2250–1797).
3. Belkhiria, H., Fakhfakh, F., & Rodriguez, I. B. (2020). Resolving multi-user conflicts in a Smart building using RBAC IEEE 29th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Bayonne, France, 2020 (pp. 181–186).
4. Ghafoorian, M., Abbasinezhad-Mood, D., & Shakeri, H. (April 1 2019). A thorough trust and reputation based RBAC model for secure data storage in the cloud. In IEEE Transactions on Parallel and Distributed Systems,
5. Mu, Z., & Liu, M. (2019). Enterprise rights management system based on RBAC model International Conference on Robots and Intelligent System (ICRIS), Haikou, China, 2019 (pp. 234–237).
6. S.R. shree, A. Chilambu Chelvan and M. Rajesh. (2020). Optimization of Secret Key using cuckoo Search Algorithm for ensuring data integrity in TPA International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2020 (pp. 1–5).
7. Rao, K. R., Ray, I. G., Asif, W., Nayak, A., & Rajarajan, M. (2019). R-PEKS: RBAC enabled PEKS for secure access of cloud data. In IEEE Access, 7, 133274–133289. https://doi.org/10.1109/ACCESS.2019.2941560
8. Singh, V. P., Kumar, M., & Arora, H. (May/June 2020), ISSN: 0193-4120. Enhanced image security technique with combination of Arnold transformation and RSA algorithm. International Journal of Test Engineering and Management, 83, 30550–30560.

Doi: https://doi.org/10.54216/JCHCI.020101

Received: June 25, 2021 Accepted: November 25, 2021

9. Soni, K., & Kumar, S. (2019). Comparison of RBAC and ABAC security models for private cloud International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), Faridabad, India, 2019 (pp. 584–587).
10. Suganthy, A., & Prasanna Venkatesan, V. (2019). An introspective study on dynamic role-centric RBAC models IEEE International Conference on System, Computation, Automation and Networking (ICSCAN), Pondicherry, India, 2019 (pp. 1–6).
11. Thakare, A., Lee, E., Kumar, A., Nikam, V. B., & Kim, Y. (April 2020). PARBAC: Priority-attribute-based RBAC model for Azure IoT cloud. In IEEE Internet of Things Journal, 7(4), 2890–2900. https://doi.org/10.1109/JIOT.2019.2963794
12. Zou, Y., Deng, J., Xu, C., Liang, X., & Chen, X. (2019). Semantic rule based RBAC extension model for flexible resource allocation 12th International Symposium on Computational Intelligence and Design (ISCID), Hangzhou, China, 2019 (pp. 221–224)

Doi: https://doi.org/10.54216/JCHCI.020101

Received: June 25, 2021 Accepted: November 25, 2021