NOVEL SECURITY MODEL USING DUAL SECURITY AND USER ROLES

[1]Sukesh, Bhardwaj, [2]Surendra, Yadav

Abstract

Each and every organizations have to manage users for the efficient functioning of the organization. Organizations have data which make a relationship between users. In such an environment, data security is a major issue. For this type of issue, this paper proposes the dual security model involving the concept of using bio-metric and pictures. The concept of authentication used is not only interactive but also secure and dynamic. It works together with the dual security, the role assignment and role-based access on primary basis of the security model. The security analysis of the model using the online tools, so found the model to be very effective and promising.

Keywords: *Role Based Security, User authentication, Dual Security*

I. Introduction

Networks can once in a while be the frail connections in the cutting edge registering world. They are among the most defenseless and effectively captured segment of the whole arrangement. This is the reason various topologies and network security conventions put such a great amount of stress on the capacity to perceive any user attempting to make an association. The acknowledgment procedure does not really distinguish who the user is. It just checks the legitimacy of the accreditations (authorizations) on the user to decide whether that user is cleared to utilize the assets or not. [1]

A user authentication policy is a procedure whenever you check that somebody who is endeavouring to access administrations and applications gives permission who they guarantee to be. This can be practiced through an assortment of authentication techniques, for example, entering a password into your PC or telephone or a PIN number into the ATM. [1]

Authentication is utilized to check that you are who you state you are. After a user's role is affirmed, for example with a username and password, that personality (role) might be utilized in an approval policy to decide the proper access benefits. Associations today should guarantee that the correct users are offered access to the correct assets, regardless of whether it is physical or - progressively - digital. A user authentication policy might be utilized to help guarantee that just the target group is accessing an organization's sensitive resources. User authentication arrangements endeavour to guarantee that the individual requesting access to confidential data is the ideal individual to access that data. [1]

[1] School of Computer Science & System Studies, Career Point University, Alaniya, Jhalawar Road, Kota-325003, Rajasthan, India
[2] School of Computer Science & System Studies, Career Point University, Alaniya, Jhalawar Road, Kota-325003, Rajasthan, India

Received: 02 Dec 2019 | Revised: 24 Jan 2020 | Accepted: 16 Feb 2020

Role-based access control (RBAC) confines network access based on an individual's role inside an organization and has one of the fundamental strategies for advanced access control. The Roles in RBAC insinuate the degrees of access that delegates have to the network. Employees are simply allowed to get to the information essential to effectively complete their action commitments. Access can be based on a couple of factors, for instance, authority, commitment, and occupation competency. Also, access to PC resources can be obliged to express assignments, for instance, the ability to see, make, or change a record. As a result, lower-level laborers generally don't move toward secret information in the condition that they needn't mess with it to fulfill their commitments. This is especially helpful if you have various labourers and use third-parties and brief specialists that make it hard to intense lay screen arrange get to. Using RBAC will help in making certain that your organization’s confidential data and prominent applications are safe. [2]

Through RBAC, you can control what end-users can do at both wide and granular levels. You can assign whether the user is a head, a master user, or an end-user, and adjust roles and access consents with your representatives'(employees) situations in the organization. The Consents are assigned uniquely with enough access varying for representatives (employees) to carry out their responsibilities. [2].

II. Literature Review

Rohini Vidhate, and V.D. Shinde 2015, In this paper, authors proposed the idea of role-based encryption (RBE) scheme on which coordinates the kind of the cryptographic systems in relationship with the RBAC. The proposed RBE plan will permit the RBAC approaches to be applied for the encoded data which is placed in the open clouds. Authors present the safe RBE-based hybrid cloud storage engineering using which an organization can safely store date in the open cloud and together with that, keep the sensitive and confidential data, which is identified with the organization’s structure in the private cloud. In the wake of examining the paper, so as to accept it as the base paper we observed a few holes in it which are as per the following,

- Encryption and Decryption algorithm is required.
- Better access control policy is required.
- Better Coordination between the executive and User
- Improved Security with the Better time management

T. Phillips ET. Al 2019, this paper states that authors proposed the idea of the trust models so as to improve the degree of the security for the stored data in case of cloud storage systems utilizing the cryptographic RBAC plans. The trust models are intended to give another way to deal with the proprietors and additionally the roles to decide the dependability of individual roles and likewise for the users, separately, in the idea of the RBAC framework. The trust models which are proposed by the creators applies the role legacy and likewise the idea of the role progressive system in the execution of reliability of the roles.

C. Hahn ET. Al 2019, Attribute-based encryption (ABE) gives the constructive answer for the adaptable access control on the sensitive individual wellbeing records when managing the portable medicinal services framework which is on the open cloud foundation. Authors proposed a noteworthy answer for giving the compelling countermeasure plot so as to make sure about the asset constrained versatile medicinal services systems and likewise to give a thorough security proof in the standard model and to give protection from the different network assaults.

III. Proposed Approach

The proposed approach will depict the idea of the work give recommending for addressable issues which we have recognized.

The procedure contains the following tasks,

1. Registering the Users
2. Accessing the System
3. Encrypting of Messages by Owner.
4. Decrypting the Message by user structure specific role.
5. Assigning Registered User, the Role.

User Registration Algorithm

This algorithm will relate to the procedure of the deployment of the new user needs to access the System.

Step 1: Read the user name and Finger print of the user.

Step 2: The new user will supply the details required.

Step 3: If user details as of now exists Then Move to 10 else Move to Step 4.

Step 4: Creates the MD5 Hash design for Unique Mark for each user.

Step 5: If Hash Exists in Data Records, then Goto Step 10 Else Goto Step 6.

Step 6: Set UserName and MD5 code for the FingerPrint as worldwide factors.

Step 7: In the Second screen of the enlistment, 5X4 matrix of the pictures of Fruits and Flowers are given the multi-decision choice for decide choice and de-determination.

Step 8: The user needs to choose the photos which will be utilized for the second period of authentication.

Step 9: Generate the Pattern by using the Name of the Fruits or Flowers as a Pattern.

Step 10: The example which is created will be stored as the password with different details given by the user in the database.

Step 11: Stop.

User Validation

Received: 02 Dec 2019 | Revised: 24 Jan 2020 | Accepted: 16 Feb 2020

This algorithm is utilized for approval of existing users.

```
Step 1:     Read the user name and Finger print of the user.
Step 2:     The new user will supply the details required.
Step 3:     Read the code design made on the basis of the picture checked during the period of creating new user.
Step 4:     Creation of Hash Code for Finger Pattern.
Step 5:     If Details Validated Then Move To 6.
                Access Allowed
                Else
                Inaccurate Information
                [End of If structure]
Step 6:  End.
```

Encryption of the Message

This area is utilized by proprietor to encode the message which is to be exchanged in between two or more users of the specific role.

```
Step 1:     Read the Message M.
Step 2:     Define or Select the Role of users who can access the message.
Step 3:     Generate the SHA code for the Message M.
Step 4:     Generate the Pattern of Numbers containing the six digits randomly created numbers.
Step 5:     Generate the random number R for the quantity of characters to be extricated from the SHA design produced for Message M.
Step 6:     Extract R characters from SHA code and consolidate with the six random characters produced in Step 4, the resultant will be the key for the encryption, name it KeyM.
Step 7:     Encrypt the message M with KeyM utilizing AES algorithm.
Step 8:     With other data additionally store the role details.
Step 10:    Stop.
```

Decryption of the Message

This area is utilized by user of the specific role to decode the message which is to be shared by the properties for the specific role.

```
Step 1:     Read the figure message CM, Role, UserIdentity, KeyM.
```

Step 2: Check the Role of the user accessing utilizing UserIdentiy if user in the UserList for the particular role move to Step 3 Else Stop.

Step 3: Check the legitimacy of the KeyM which is the encryption key and is found to be legitimate, at that point move to step 4 in any other case stop.

Step 4: Decrypt the message utilizing KeyM.

Step 5: Stop.

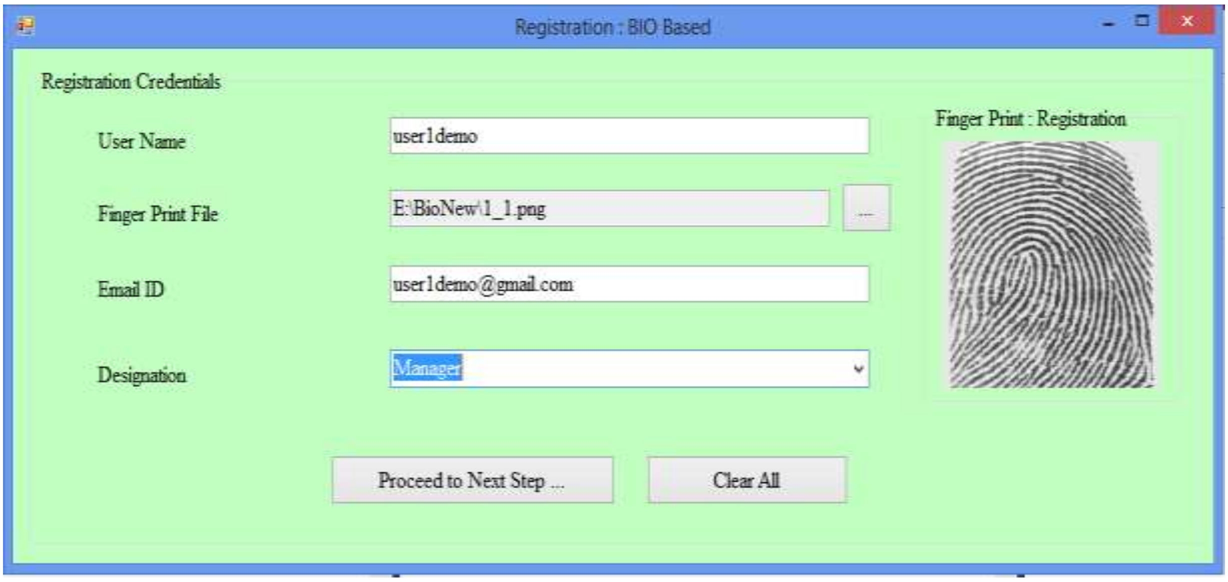
Role Granting Algorithm

This area will manage the confirmation of the role for the specific user.

```
Step 1:    Read the User Identity.
Step 2:    Read the Role for the rundown of the approved roles.
Step 3:    If the details coordinate in database for enlisted user at that point:
           Award role to the enlisted user.
           Else:
           Inaccurate Data
           [Condition Ends Here]
Step 4:    End.
```

IV. IMPLEMENTATION

The implementation is done using the software Visual Studio and database using the SQL Express Edition.



Registration : BIO Based

Registration Credentials

User Name: user1demo

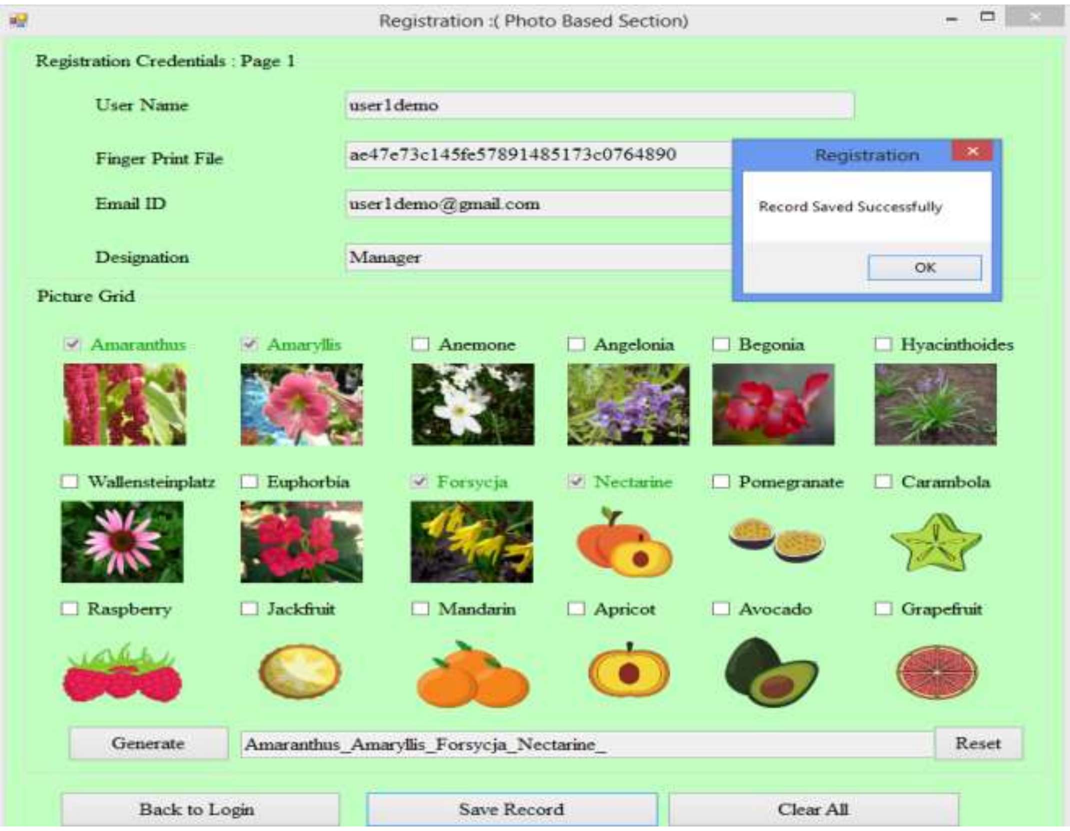
Finger Print File: E:\BioNew\1_1.png

Email ID: user1demo@gmail.com

Designation: Manager

Figure 1: Phase 1 Registration

Received: 02 Dec 2019 | Revised: 24 Jan 2020 | Accepted: 16 Feb 2020



Registration :(Photo Based Section)

Registration Credentials : Page 1

User Name: user1demo

Finger Print File: ae47e73c145fe57891485173c0764890

Email ID: user1demo@gmail.com

Designation: Manager

Registration

Record Saved Successfully

OK

Picture Grid

☑ Amaranthus ☑ Amaryllis □ Anemone □ Angelonia □ Begonia □ Hyacinthoides

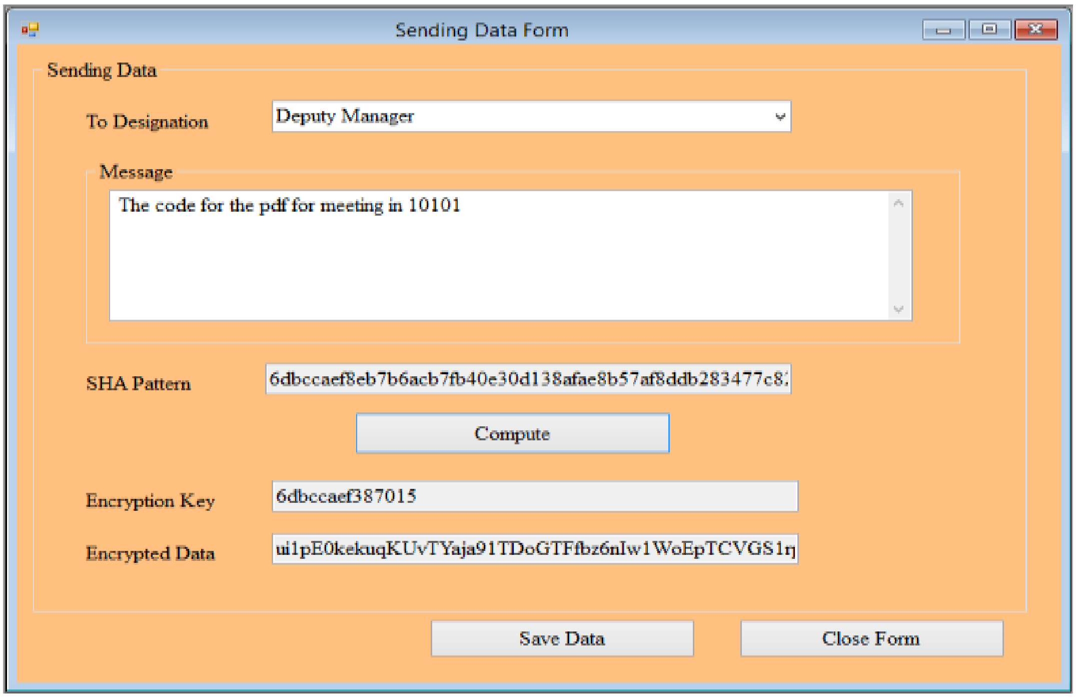
□ Wallensteinplatz □ Euphorbia ☑ Forsycja ☑ Nectarine □ Pomegranate □ Carambola

□ Raspberry □ Jackfruit □ Mandarin □ Apricot □ Avocado □ Grapefruit

Generate: Amaranthus_Amaryllis_Forsycja_Nectarine_

Figure 2: Phase 2 Registration

The implementation of proposed approach involves biometric and graphical selection of the images to form the basis of the password. The implementation is done using role-based concept for assigning the designation role to the users and data sharing is done using the role base access.



Sending Data Form

Sending Data

To Designation: Deputy Manager

Message

The code for the pdf for meeting in 10101

SHA Pattern: 6dbccaef8eb7b6acb7fb40e30d138afae8b57af8ddb283477c8:

Encryption Key: 6dbccaef387015

Encrypted Data: ui1pE0kekuqKUvTYaja91TDoGTFfbz6nIw1WoEpTCVGS1r

Figure 3: Role Based Access

V. RESULT ANALYSIS

The overall strength of a password is determined in order to verify that the strength is good enough to be protected from hackers' attempts to crack the password.

For testing purpose, we have used the following keys which are generated in the process of the simulation of the proposed work.

Finger Print Related Key:

133c2894089c54e3321b64d18f8347f7

Picture Based Key:

Euphorbia_Raspberry_Jackfruit_Mandarin_Apricot_Pomegranate_Begonia_Grapefruit_

SHA Based Transaction Key:

34a81b834c2bb12f2c4fde3044c404cf199

How Secure My Password

This is an online tool which accepts a password as an info and does some assessment based on applying the attacks on it and decides the evaluated time which will be required to break the password.

This password checker will measure your password and give it a score dependent on how great of a password it is. It will inform you as to whether you picked a typical password (don't do that!) and it will likewise consider the likelihood of letters landing near one another. For example, "Q" is quite often followed by "U", so your password's score won't increment much when you type in the "U".

Table 1: Strength Analysis Using Tool 1

	Finger Print Related Key	**Picture Based Key**	**SHA Based Transaction Key**
Years Required	138 X 10^{78}	22 X 10^{123}	2X10^{36}

We plotted the comparison graph on the basis of the power of 10

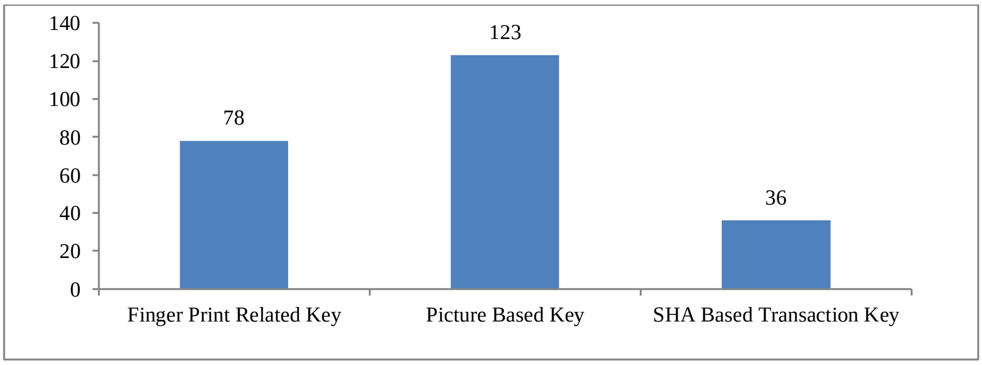


Figure 4: Graphs Based Analysis of Year According Tool1

Runkim Test

The Runkin tool likewise tests the password strength and computes the entropy together with deciding the length of the string.

Table 2: Strength Analysis Using Tool 2

	Finger Print Related Key	**Picture Based Key**	**SHA Based Transaction Key**
Length	32	78	35
Entropy (bits)	112.8	400.7	133.6
Character Size	36	74	36

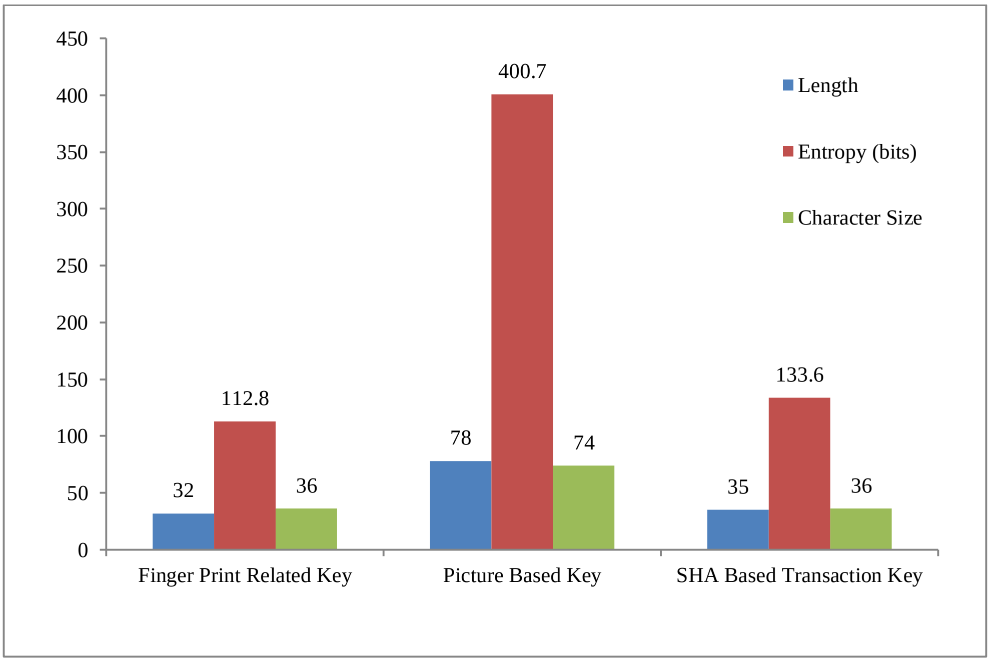


Figure 5: Graphs Based Parameters According Tool 2

CryptoTool 2

CrypTool is an open-source adventure. This will be used for calculating the entropy and strength of the pattern.

Table 3: Strength Analysis Using Tool 3

	Finger Print Related Key	**Picture Based Key**	**SHA Based Transaction Key**
Score	100	100	100

Received: 02 Dec 2019 | Revised: 24 Jan 2020 | Accepted: 16 Feb 2020

Bit Strength	101	221	97
Entropy	3.676	4.325	3.489

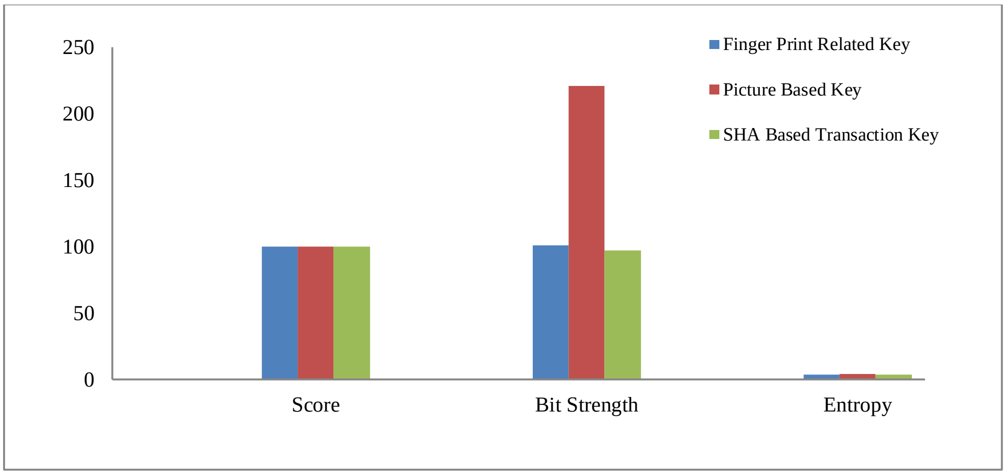


Figure 6: Graphs Based Analysis of Parameters according Tool 3

VI. CONCLUSION

Security is an important part when we are dealing with the data exchange or access in any organization big or small. The protection of data which is to be accessed by the user, is done in two segments. First is the proper authentication of the user and second one is to specify the portion of data which the authorized users can access. This paper handles both the issues. In the proposed work, the secure authentication is planned using the concept of the dual verification: first verification and then validation is done using the finger print and picture based pattern generation. The comparison of the finger print is done on the basis of hash code, whose result has better matching accuracy and it rremains faster as compared to the traditional finger print comparison methodology.

In the second section or part, the proposed work is focused over the role based security which specifies the access of the data on the basis of the role of the user. The proposed work makes use of the three keys where two keys, one based on the basis of the finger print and other on Picture selection, are used at the time of the authentication and login of the user and the third key and transaction id are used at the time of the transaction when a user tries to access the data which is allowed to be accessed as per the role. The results related to the strength of the keys are tested using various online and offline tools related to password strength and entropy testing and the results which are obtained are quite efficient and effective.

REFERENCES

[1] M. Afshar, S. Samet and T. Hu, "An attribute based access control framework for healthcare system," *J. Phy. Conf. Ser.* vol. 933, 2018, p. 012020.

[2] S. Chakraborty, R. Sandhu and R. Krishnan, "On the feasibility of attribute-based access contr.ol policy mining," in IEEE *20th Int. Conf. Inf. Reuse Integrat. Data Sci. (IRI),* July 2019, pp. 245-252.

[3] R. Vidhate and V. D. Shinde, "Secure Role-Based Access Control on Encrypted Data in Cloud Storage using Raspberry PI," *Int. J. Multidisciplinary Res. Develop.*, vol. 2, pp. 20-27, 2015.

[4] T. Phillips, X. Yu, B. Haakenson and X. Zou, "Design and Implementation of Privacy-Preserving, Flexible and Scalable Role-Based Hierarchical Access Control," *IEEE Int. Conf. Trust, Priv. Secu. Intel. Sys. App.*, pp. 46-55,2019.

[5] Y. Xue, K. Xue, N. Gai, J. Hong, D. S. Wei and P. Hong, "An attribute-based controlled collaborative access control scheme for public cloud storage," *IEEE Tran. Inf. Forens. Security,* vol. 14, pp. 2927-2942, 2019.

[6] Y. Xu, W. Gao, Q. Zeng, G. Wang, J. Ren and Y. Zhang, "A feasible fuzzy-extended attribute-based access control technique," *Sec. Comm. Net.*, 2018.

[7] C. Hahn, H. Kwon and J. Hur, "Trustworthy Delegation Toward Securing Mobile Healthcare Cyber-Physical Systems," *IEEE Internet Things J.*, vol. 6, pp. 6301-6309, 2019.

[8] G. V. Bandewar and R. H. Borhade, "Role Based Encryption with Efficient Access Control in Cloud Storage," *Int. J. Sci. Res.* (IJSR), 2016.

[9] N. Geetha and M. S. Anbarasi, "Role and attribute based access control model for web service composition in cloud environment," in *IEEE Int. Conf. Computat. Intelligenc. Data Sci. (ICCIDS)* June 2017, pp. 1-4.

[10] F. Yue-Qin and Z. Yong-Sheng, "Trusted Access Control Model Based on Role and Task in Cloud Computing," in *7th Int Conf. Inf. Tech. Med. Educ. (ITME),* Nov. 2015, pp. 710-713.

[11] A. Wójtowicz and K. Joachimiak, "Model for adaptable context-based biometric authentication for mobile devices," *Per. Ubiquit. Comput.*, vol. 20, pp. 195-207, 2016.

[12] W. C. Garrison, A. Shull, S. Myers and A. J. Lee, "On the Practicality of Cryptographically Enforcing Dynamic Access Control Policies in the Cloud," *IEEE Sym. Sec. Priv.*, pp. 819-838,2016.

[13] Y. Wang, Y. Ma, K. Xiang, Z. Liu and M. Li, "A Role-Based Access Control System Using Attribute-Based Encryption," in *IEEE Int. Conf. Big Data Artific. Intellig. (BDAI),* June 2018, pp. 128-133.

[14] I., Ray and I. Ray, "Trust-based access control for secure cloud computing," in *High Perform. Cloud Audit. Applicat.,* Springer, NY, pp. 189-213, 2014.