TEST Engineering & Management

July – August 2020
ISSN: 0193-4120 Page No. 646 - 649

Simulation Prototype of Novel Graphical Authentication and Role Based Security

Sukesh Bhardwaj, Dr. Surendra Yadav
Career Point University, National Highway 12, Alaniya, Rajasthan 325003.
+91-9958516487 and sr.sukesh22889@gmail.com

Article Info
Volume 83
Page Number: 646 - 649
Publication Issue:
July - August 2020

Article History
Article Received*: 06 June 2020*
Revised*: 29 June 2020*
Accepted*: 14 July 2020*
Publication*: 25 July 2020*

Abstract

Now days its trend of everything going online and the nature of cloud security is such that, the data from the unauthorized access has always been a big issue. Almost on A daily basis, online frauds, data loops, hacking are seen in the news. Thus, the nature of data insecurity pushes us to focus on developing some more innovative ways of user authentication so that it becomes more difficult for hackers to break in to the system or to break the security. The Authentication of users with bio-metric and role-based concept of security will enable us to overcome the security problems to an extent. This paper will focus on the explanation of the simulation work done for implementing the innovative concept for using the Role Based Security with the graphical organization of images along with fingerprint. The simulation is created using the Visual Studio 2010 and database-based simulation work is done using SQL Server Express edition. The simulation starts with the registration phase of the user where the registration is done through verification of the finger print and then proceeds with the selection of the pictures for the formation of the second phase, which is authentication. After the user is logged in with the proper verification, the role which was assigned at the time of the registration will form as the basis of the validation to decide whether the authorized user will have an access to the data or not. The user having an access of the data will again have to revalidate for accessing the data with some pattern generated for the validation of the authenticity for gaining access. So, this whole working of the proposed system, is shown in the simulation developed.

Keywords: *Role Based Security, User authentication*

I. Introduction

The paper with the Title "Groundbreaking Approach of Role Based Security using Fingerprint and Picture Password "which we have published is dedicated to the explanation of our innovative approach of using the role based security with the integration of the finger print and the arrangement of the graphical images for the formation of the pattern which will be used for the authentication of the user and is also involved in the transmission of the messages. [1]

The simulation of the proposed approach is done using the Visual Studio 2010, as creation of graphical forms, handling of the finger print and integration of the security algorithms can be done with ease using the VS 2010 and the database involved in the simulation work was created BY the Microsoft SQL Server 2009 expression edition and if there is need for more practical implementation we can easily migrate it to the other database. [2]

II. Simulation Explanation

As we have stated previously, the implementation is done in VS 2010 and SQL Server Database 2008. The proposed work implementation is done in order to simulate a work with secure data communication which is done using SHA and MD5 as the basis for the user registration and the data communication. [3]

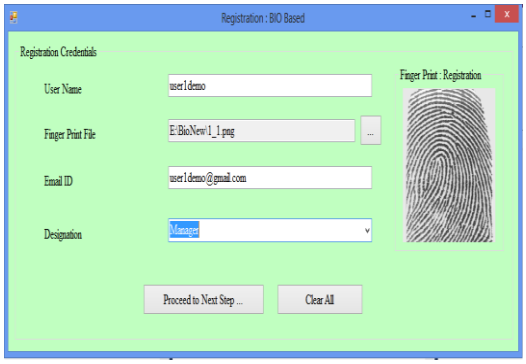

Fig. 1. Registration Section 1

TEST Engineering & Management

July – August 2020
ISSN: 0193-4120 Page No. 646 - 649

The fig 1 shows registration section 1, in which the registration process's first phase is explained. In this, a newly registering user has to specify his/her user name, select the finger print file and also specify his/her email id. The selection of the finger print by the user will enable the working of the MD5 algorithm which in the process first selects the image file corresponding to the finger print and then performs the MD5 algorithm and generates a fixed length HASH WHICH corresponds to the finger print. [4]

The designation of the user is selected from the combo box which is used for specifying the role condition for the user in the registration process. The details of the username and the MD5 hash generated corresponding to the fingerprint are checked in the database and if the user details already exist then an error is prompted. Otherwise, next screen similar to the screen shown in the fig 4.2 will get displayed. [5]

This is the second section of the registration phase. In this, we will generate the password pattern on the basis of the selection of the photos on the screen. In order to select the photos of the flowers and fruits we have to just click on the checkbox corresponding to that picture box. The pattern is generated on the basis of the concatenation of the scientific names of the fruits and flowers.

Now, after all the processing is done on the user part, just clicking on the save button will save the details if the following validations related to the data are successful: the user name entered by the user should be unique, the finger print selected and the correspondingly generated MD5 hash are also checked in the database for the validation SO that the other user is not registered with the same finger print and lastly the email id should also be unique.

Then all the details which are specified will then get stored in the database that is corresponding to the user registration. The database which is created for the proposed implementation is created in the Microsoft SQL Server 2008.

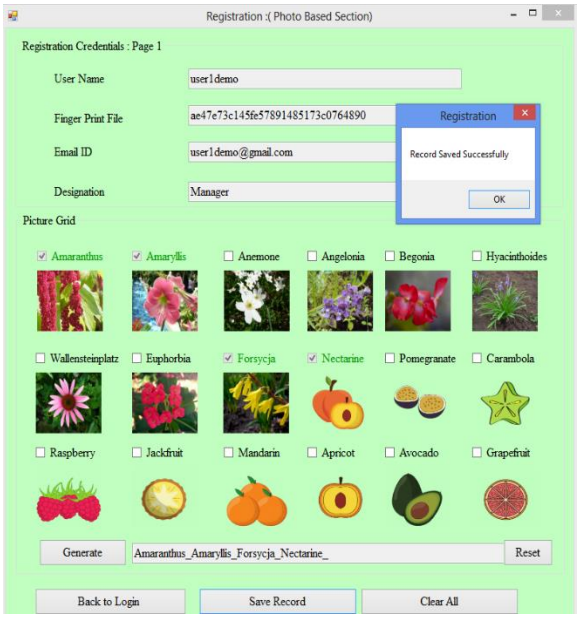

Fig. 2. Registration Section 2

uname	emailid	fiqmd5	password
amitjpr	amitjpr@gmail....	01b6bd2e2ffe91...	Amaranthus_Amaryllis_Anemone_Forsycja_Nectarine_
anilpr	anilpr@gmail.c...	f0ebf383bf1c11...	Amaranthus_Amaryllis_Anemone_Apricot_Avocado_Grapefruit_
datauser1	datauser1@gm...	2e2ffb7369d347...	Amaranthus_Amaryllis_Euphorbia_Jackfruit_Mandarin_Forsycja_Apricot_
user1demo	user1demo@g...	ae47e73c145fe5...	Amaranthus_Amaryllis_Forsycja_Nectarine_

Fig. 3. Registration Details in Table

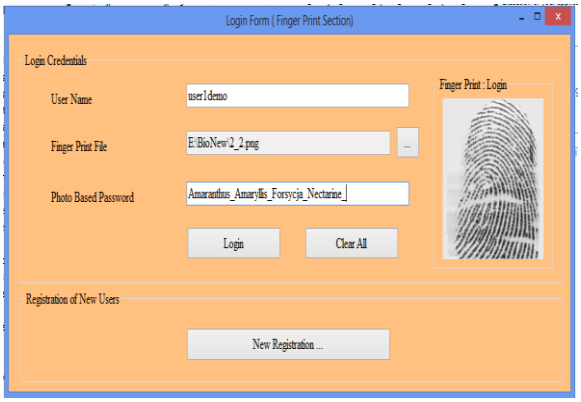

Fig. 4. User Login

The fig 4 shows the user login page of the proposed work. In this section, firstly we have to specify the user name. Then, we have to select the finger print which we have specified at the time of the registration process and lastly, the picture password which is generated by the selection of the pictures of the flowers and fruits is to be re-enacted. After all the details are entered by the user, the details are verified using the details which are stored in the database and the MD5 generation on the basis of the selected finger print is also performed in the process of the login. If all the credentials are found ok, the Main screen of the communication process is presented to the user. [6]

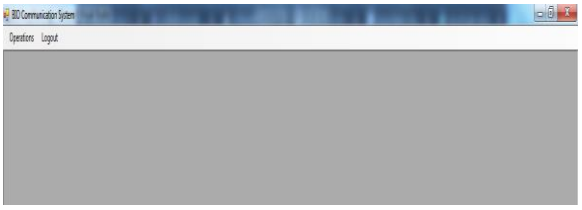

Fig. 5. Main Screen

The fig 5 shows the MDI form which is the main screen of the communication system. It contains a menu driven interface using which we can send data to the other user, receive the data shared by the other user and also access the list of the message which are received.

July – August 2020
ISSN: 0193-4120 Page No. 646 - 649

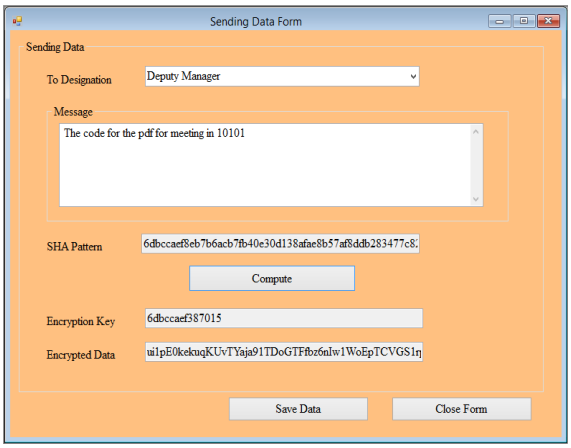

Fig. 6. Data Sending Form

Fig 6 shows the data sending form. In this form, data is shared on the basis of the role and will only be accessed by the users who are registered with that role. The process of the data encryption is as follows: first, an SHA code is generated for the data or the message to be sent using the SHA 256 algorithm. [7] Then a random number is generated, and the number of the characters which are equivalent to the random number are extracted from the generated SHA code. And then 6 random numbers are generated and combined with the extracted SHA to form the encryption key as shown in the fig 6. The data which is to be shared is then encrypted using the encryption key and with the help of the AES algorithm

Then, clicking on the Save data button will save the record. After the record is saved, a unique transaction id is generated which is unique for the data communication that is taking place between the sender and receiver. The details will be stored in the Data's table, where tid stands for the transaction ID which is an auto increment field in order to generate the unique ID for each record that is entered in the table.

Column Name	Data Type
tid	int
fuser	varchar(50)
tuser	varchar(50)
data	varchar(500)
shapass	varchar(500)

Fig. 7. Structure for Transaction Details

Now, as shown in the above section, the data is shared for the Deputy Manager and for the simulation purpose we have created another user with the role of the Deputy Manager and will try to access the data shared with that role. For this purpose, we have created another user with user name user2demo.

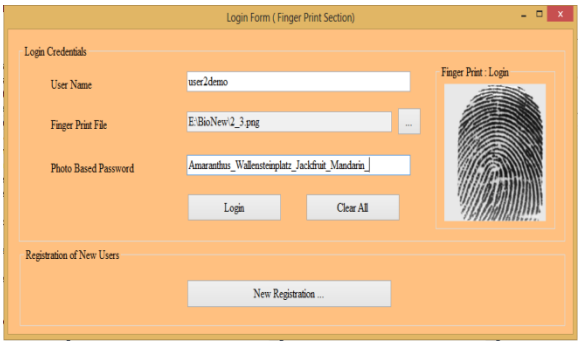

Fig. 8. Login for Deputy Manager

Fig 9 shows the data receiving form which is used for receiving the data. Here, the receiver has to enter the transaction ID received and the SHA password code for fetching the data. And the role is also checked in the background as only the users who have the role assigned with the message will be able to decrypt the data. [8]

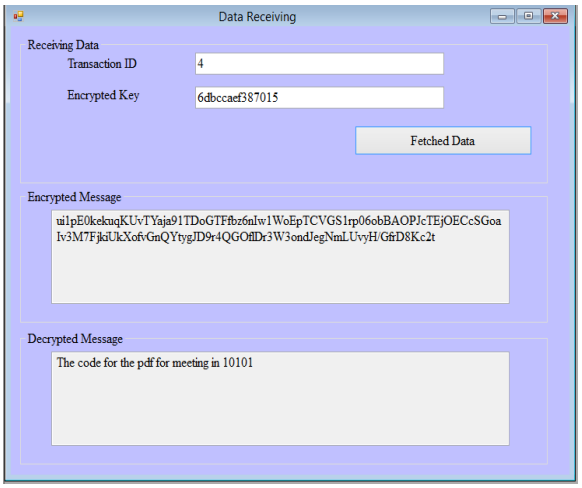

Fig. 9. Data Receiving

Fig 10 shows the form which shows the list of received messages. The form will show the transaction ID, sender information and the SHA code based password received for the fetching the data.

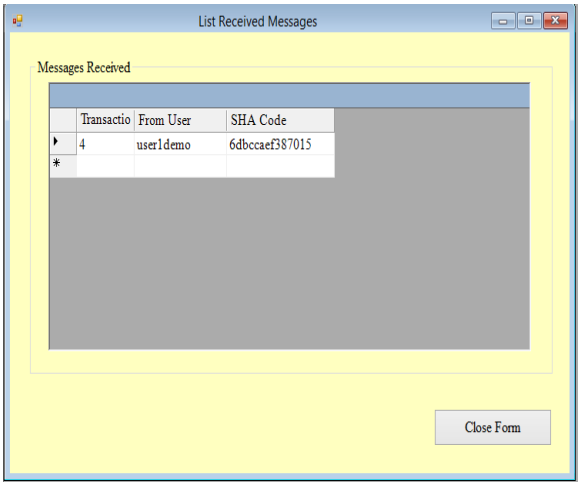

Fig. 10. List of Received Messages

July – August 2020
ISSN: 0193-4120 Page No. 646 - 649

III. Conclusion

This paper explains the overall working of the proposed approach using the simulation created using VS 2010 and SQL Server 2008 express edition. In the upcoming works, we will try to show the performance evaluation of our work using the various online and offline testing tools.

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 *20thInt. 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] L. Zhou, V. Varadharajan and M. Hitchens, "Trust Enhanced Cryptographic Role-Based Access Control for Secure Cloud Data Storage," *IEEE Tran. Inf. Foren. Sec.*, vol. 10, pp. 2381-2395,2015.

[5] 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.

[6] 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

[7] 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.

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

[9] 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.

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

[11] 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.