GROUNDBREAKING APPROACH OF ROLE BASED SECURITY USING FINGERPRINT AND PICTURE PASSWORD

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

Research Scholar

[1]Career Point University

[2]Career Point University

[1]sr.sukesh22889@gmail.com, [2] syadav66@gmail.com

[1]+91-9958516487, [2]+91-9982317251

ABSTRACT

Security and authentication of the user is one of the most important things when working in the cloud environment. The problem which is being faced by every organization working online or in cloud environment is the proper authentication of the user and also to share the information with the proper control, with a restriction of the type and extend to which the authorized user can access the data. This paper first reviews the concept of the base paper and then identifies the gaps in the current research and suggested the new concept of the authentication and explained the overall concept in terms of the role-based security, in order to filter the information access from the users in organization. The working of the concept which is proposed is providing the dual verification of the user identify, the bio-metric basis which is taken in the paper is the identification of the user using the finger print and the second phase of authentication deals with some sort of graphical image selection for the generation of the next authentication basis. Along with the dual authentication, the role specific data sharing is also performed to further enhance the security level. This paper we dedicated to the explanation of the concept and algorithms which we have designed for the proposed implementation of the system and with the explanation of the algorithms we also focus on the explanation of the utility or credibility of the work proposed. This work, not only aims for the proper authentication of user but also for the proper access of the information or data.

***Keywords*:** Role Based Security, Role Based Encryption, Role Based Access Control, User authentication

I. INTRODUCTION

User authentication is the process of the validation of a functioning human-to-machine move of the accreditations required for definite affirmation of a client's genuineness. [1] Validation is one such procedure which assumes a significant role in Cloud Computing security. [2] The different conceivable security assaults on the Cloud Service Providers (CSP) are forestalled by applying distinctive authentication components, which confirms a user's character when a user wishes to demand services from cloud servers. [4]

Role based security is a rule by which architects make structures that limit get as far as possible exercises according to a user's-constructed role inside a system. This is moreover every now and again called RBAC, since various associations and affiliations use this rule to ensure that unapproved clients don't get to advantaged information inside an IT architecture. [4] There are numerous approaches to build up a role-based security framework. Every one of them start with the meaning of different roles and what users allotted to those roles can and can't do or see. The subsequent degrees of usefulness must be coded into the framework utilizing explicit parameters.[5]

II. LITERATURE REVIEW

Rohini Vidhate, and V.D. Shinde 2015, [6] In this paper, authors proposed the concept of the role-based encryption (RBE) scheme on which integrates the sort of the cryptographic techniques in association with the RBAC. The proposed RBE scheme will allows the RBAC policies to be applied for the encrypted data on which is stored in the public clouds. [6] Author’s presents the secure RBE-based hybrid cloud storage architecture on which enables the functionality for the organization to store data securely in the area of the public cloud, together with that maintain the sensitive information on which is related to the organization’s structure in the private cloud. After studying the paper, in order to take it as the base paper we highlighted some gaps in it which are as follows,

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

O. Heinisuo, et. Al 2019, [7] In this paper, creators proposed the idea of the role-based encryption (RBE) plot on which incorporates the kind of the cryptographic procedures in relationship with the RBAC. The proposed RBE plan will permits the RBAC rules and regulations to be applied for the encrypted information on which is put away in the public clouds. [6] Author's available the protected RBE-dependent distributed storage design with respect to which empowers the usefulness for the association to store information safely in the region of the open cloud, along with that keep up the data confidentiality on which is identified with the association's structure in the private cloud.

C. Hahn et. al 2019, [8] Attribute-based encryption (ABE) gives the constructive answer for the adaptable access control on the delicate individual wellbeing records when managing the portable healthcare framework which is on the open cloud infrastructure. Creators proposed the noteworthy answer for giving the powerful countermeasure plot so as to make sure about the asset constrained portable health frameworks and furthermore to give the thorough security verification in the standard model, to give protection from the various network attacks. [8].

III. PROPOSED APPROACH

This section corresponds to secure file sharing over cloud the suggested technique will describes the conceptual work we are suggesting for the solution of the problems which we have identified.

The process contains the following operations,

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

User Registration Algorithm

This algorithm will corresponds to the process of the registration of the new user wants to access the System.

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

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

Phase 3: If user details already exists Then Move To 10 Else Move To Phase 4.

Phase 4: Corresponding to the finger print generates the MD5 Hash pattern.

Phase 5: If Hash Exists in Data Records Then Go to Phase 10 Else Go to Phase 6.

Phase 6: Set Username and MD5 code for the Fingerprint as global variables.

Phase 7: In the Second Screen of the registration, 5X4 grid of the images of Fruits and Flowers is presented with the multi-choice option of selection and de-selection.

Phase 8: The user has to select the pictures will be used for the second phase of authentication.

Phase 9: Generate the Pattern by coming the Name of the Fruit or Flowers as a Pattern.

Phase 10: The pattern which is generated will stored as the password with other details provided the user in the database.

Phase 11: Stop.

User Validation

This algorithm is used for validation of existing users.

```
Phase 1: Read the user name and Finger print of the user.
Phase 2: The new user will supply the details required.
Phase 3: Read the code pattern created on the basis of the image checked in the phase of
         creating new user.
Phase 4: Creation of Hash Code for Finger Pattern.
Phase 5: If Details Validated Then Move To 6.
         Access Allowed
         Else
         Incorrect Information
         [End of If structure]
Phase 6: End.
```

Encryption of the Message

This section is used by owner to encrypt the message which is to be shared in between the users of the particular role.

```
Phase 1:  Read the Message M.
Phase 2:  Define or Select the Role of users who can access the message.
Phase 3:  Generate the SHA code for the Message M.
Phase 4:  Generate the Pattern of Numbers containing the six digits randomly generated
          numbers.
Phase 5:  Generate the random number R for the number of characters to be extracted from
          the SHA pattern generated for Message M.
Phase 6:  Extract R characters from SHA code and combine with the six random characters
          generated in Phase 4, the resultant with be the key for the encryption, name it
          KeyM.
Phase 7:  Encrypt the message M with KeyM using AES algorithm.
Phase 8:  With other information also store the role details.
```

Phase 10: Stop.

Decryption of the Message

This section is used by user of the particular to decrypt the message which is to be shared by the owner for the particular role.

```
Phase 1:  Read the cipher message CM, Role, User Identity, KeyM.
Phase 2:  Check the Role of the user accessing using User Identity if user in the User list for
          the specific role move to Phase 3 Else Stop.
Phase 3:  Check the validity of the KeyM which is the encryption key if valid then move to
          Phase 4 otherwise stop.
Phase 4:  Decrypt the message using KeyM.
Phase 5:  Stop.
```

Role Granting Algorithm

This section will deals with the granting of the role for the particular user.

```
Phase 1:  Read the User Identity.
Phase 2:  Read the Role for the list of the authorized roles.
Phase 3:  If the details match in database for registered user then:
          Grant role to the registered user.
          Else
          Invalid Details
          [End of If structure]
Phase 4:  Stop.
```

IV. JUSTIFICATION OF PROPOSED APPROACH

The proposed work chapter is defined for overviewing the research gaps once again and then giving the explaining in coordination with the proposed work algorithms which can be applied for solving these gaps.

Now for the Gap: Improved Security with the Better time management.

For the improvement of the security, we have performed the concept of the dual authentication system. In the authentication system, first require the user registration, so we have created the module for the user registration.

a. Registering the users using the finger print

Now, the question arises that the users finger print concept is very old, so what new we are doing in this, so we are not validating the finger print using the line to line based traditional concept, we are improving this by making use of the SHA algorithm which generates the unique hash code which is of fixed length and also unique for the file which for which we are generating the hash code. [9]

So, the finger print is supplied as the image and the SHA code is generated on the basis of the image file. Now, what is the use of this concept, instead of using the traditional approach, first one is that it is unique, so no two fingerprint file can have the same hash code, now instead of the lines in the fingerprint, the SHA code [10] of the fingerprint file will be stored and matched, which in turn speed up the matching process.

b. Graphical Grid of the Pictures

The dual authentication of the user in this system is proposed, in which the second validation scenario is created on the basis of the selection of the pictures which is related to the fruits and flowers and the generation of the password pattern on the basis of the selection of the pictures.

The concept till now is fixed for 5X6 grid of pictures, we can further increase this grid or make it random to further increase the complexity level.

The pattern which is created on the basis of the images checked, will form the second phase password which will be utilized in the login phase.

Now, this dual authentication will help us in double verification of the user in the proposed system and this verification module is in the Login Module.

The question arises that, what is the user of taking the picture based verification, the answer to that is the pattern which are directly the text, like the name of the some personality, or some pattern related to some important dates are quite hard to remember and non-interactive, so taking the picture based concept of the pattern formation, not only give a ease for remembering the pattern but also in forms the possibilities of the number of the combinations, so will form the variety of different patterns which will be difficult for the hackers to break or crack.And to further increase the level of the security, we develop the concept, the SHA pattern generated using the fingerprint can be send via email id and the pattern generated from the selection of the pictures of fruits and flowers will be send as SMS.

Now for the gaps,

1. Encryption and Decryption algorithm is required.
2. Better access control policy is required.
3. Better Coordination between the administrator and User

For the implementation purpose of the Role Based Security [11], when creating the user the designation of the user is being taken which is latter utilized in the classification of the data.

As the topic rolls around the role based security, for this we have created the module for the admin purpose only, as in the base paper also controlled by the administrator. The module is "Assigning Registered User the Role"

In this the file which is shared the any user is visible to the administrator, and the administrator will assign which role [12] can access the file, so if any other role will try to decrypt the file, the access will not be granted..

V. CONCLUSION

The proposed approach provided the significant approach for overcoming all the gaps which are highlighted in the paper, the next Phase which we will proceed will be the implementation of the model proposed and for the simulation purpose, we are planning to done the implementation in Visual Studio and for the database required for that will be implemented in SQL Server.

REFERENCES

[1] Zhou, L., Varadharajan, V., & Hitchens, M. (2015). Trust enhanced cryptographic role-based access control for secure cloud data storage. *IEEE Transactions on Information Forensics and Security*, *10*(11), 2381-2395.

[2] Mui, L., Mohtashemi, M., & Halberstadt, A. (2002, January). A computational model of trust and reputation. In *Proceedings of the 35th Annual Hawaii International Conference on System Sciences* (pp. 2431-2439). IEEE.

[3] Chakraborty, S., & Ray, I. (2006, June). TrustBAC: integrating trust relationships into the RBAC model for access control in open systems. In *Proceedings of the eleventh ACM symposium on Access control models and technologies* (pp. 49-58).

[4] Feng, F., Lin, C., Peng, D., & Li, J. (2008, September). A trust and context based access control model for distributed systems. In *2008 10th IEEE International Conference on High Performance Computing and Communications* (pp. 629-634). IEEE.

[5] Toahchoodee, M., Abdunabi, R., Ray, I., & Ray, I. (2009, July). A trust-based access control model for pervasive computing applications. In *IFIP Annual Conference on Data and Applications Security and Privacy* (pp. 307-314). Springer, Berlin, Heidelberg.

[6] Vidhate, R., & Shinde, V.D. (July 2015). Secure Role-Based Access Control on Encrypted Data in Cloud Storage using Raspberry PI. *International Journal of Multidisciplinary Research and Development*, 2(7), 20-27.

[7] Deepika, G., Nesakumar, M. D., & Aruna, M. (2019). Trust Enhanced Secure Cloud Data Storage Using Cryptographic Role-Based Access Control Mechanism. International Journal of Computer Science and Mobile Computing, 8(9), 219-225.

[8] Hahn, C., Kwon, H., & Hur, J. (2018). Trustworthy delegation toward securing mobile healthcare cyber-physical systems. *IEEE Internet of Things Journal*, *6*(4), 6301-6309.

[9] Ferrara, A. L., Fuchsbauer, G., & Warinschi, B. (2013, June). Cryptographically enforced RBAC. In *2013 IEEE 26th Computer Security Foundations Symposium* (pp. 115-129). IEEE.

[10] Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006, October). Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM conference on Computer and communications security* (pp. 89-98).

[11] Garrison, W. C., Shull, A., Myers, S., & Lee, A. J. (2016, May). On the practicality of cryptographically enforcing dynamic access control policies in the cloud. In *2016 IEEE Symposium on Security and Privacy (SP)* (pp. 819-838). IEEE.

[12] Nabeel, M., & Bertino, E. (2013). Privacy preserving delegated access control in public clouds. *IEEE Transactions on Knowledge and Data Engineering*, *26*(9), 2268-2280.