International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 5, pp 150-155, May-2024

https://doi.org/10.47001/IRJIET/2024.805023

Authenticated E- Bank System Based on RBAC Model

[1]Alaa J. Mohammed, [2]Saja J. Mohammed

[1,2]Department of Computer Science, College of Computer Science and Mathematics, University of Mosul, Mosul, Iraq

***Abstract* - Electronic banking services have become increasingly popular in line with the development of information and communications technology because of the benefits and ease it provides for both financial institutions and consumers. It facilitates access to customers' bank accounts and carries out financial operations quickly and easily without the need to visit traditional banking branches. This reduces both time and effort for the customer. However, protection and security problems are considered one of the main issues facing electronic banking services. Hacking and online fraud have put these services' security at risk. For guarantee the security of electronic financial transactions and the preservation of customer data, this calls for strengthening security and implementing security measures. However, securing reliable identity verification for the customers is one of the main problems facing e-banks.**

Keywords: Information Security, Authentication Systems, Role Based Access Control, E-Bank Security, Multi-factor Authentication, Financial Data Protection.

I. INTRODUCTION

The rapid growth of technology and the increasing use of smart devices and the Internet, the need for strong authentication systems has become more important than previously. [1][2]. These systems guarantee the integrity and privacy of the data by preventing hackers and illegal use of sensitive, financial, and personal information. [3].

Robust authentication processes have further served to mitigate the likelihood of fraudulent cyberattacks, hence augmenting confidence between customers, corporations, and establishments. [4]. Updating these systems on a regular basis is an expenditure that is required to guarantee security in the age of technology [5]. Also, Authentication systems contribute to technical progress in the field of information confidentiality and digital security by developing and creating technologies and tools that protect information and ensure protected and secure electronic communications[6][7].

Verifying an online service user's identity is known as user authentication. To prevent unauthorized access to online accounts because unauthorized access has serious consequences, including financial loss or privacy violation, as both personal devices and online accounts contain vital private data [8]. Accordingly, user authentication is key to achieving complete protection of online accounts. It makes it possible to confirm users' validity before granting them access to system resources [9] [10].

Recent years have seen the proposal of several authentication systems using various methodologies; among them are text passwords, three-dimensional passwords, multi-factor authentication, third-party authentication and biometric scanning. Moreover, current research indicates that, among the approaches already mentioned, text-based passwords are the most popular [11] [12]. Nevertheless, despite its simplicity, the text-based password scheme is still a fairly weak authentication method because of its vulnerabilities to dictionary and brute-force attacks [13].

Technology has undergone a revolution thanks to the digital world, and this has had a significant impact on many facets of society, most notably the financial industry. Customers are increasingly choosing electronic banking, or "E-banking," as banks provide their services via internet platforms [14]. Customers can simply manage their finances at any time and from any location. Also Customers may use it to access their electronic bank accounts and carry out financial activities online, including making deposits, withdrawals, and transfers of funds [15].

Through the use of authentication techniques, such as identity verification, PIN verification, and Gmail verification, e-banks have improved customer's satisfaction and offered safer, more effective financial services. As a result, the security of bank accounts and online banking transactions has improved. [16] [17].

1.1 Role Based Access Control Authentication Method

Access refers to the capability of utilizing, editing, or observing a computer resource, the act of enabling activating or limiting the capability is known as access management [18] [19]. Due to its ability to reduce the complexity and cost of security management in large-scale networked systems, the Role Based Access Control (RBAC) model has emerged as an important standard for advanced access control [20] [21]. Fig. (1) explains the RBAC Model.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 5, pp 150-155, May-2024

https://doi.org/10.47001/IRJIET/2024.805023

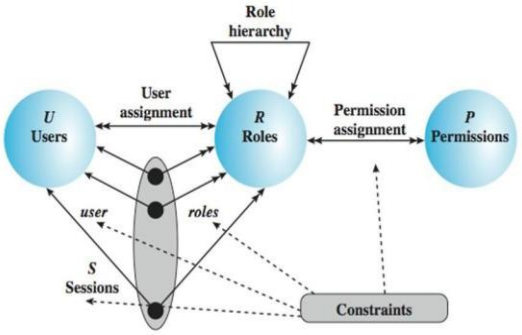

Figure 1: Role Based Access Control (RBAC) Model.

RBAC is a method that provides a sufficient level of security to user data as well as system resources through policies and rules that are implemented on the user in the form of password and registration [22]. Since the ability to create control policies for an organization that blend organically with its structure is the basic principle of the RBAC concept [23]. In other words, by designing a security policy that targets the organizational structure and targets independently, the RBAC method seeks to give the policy character [24]. By learning about the different jobs and the precise rights associated with each job. It will be explained how e-banks use RBAC algorithm to organize and control access to resources and information in a secure manner. Depending on their position within the company, users are given different roles, and these roles decide what rights they are allowed to access. Such as, regular electronic banking personnel can access customer data and perform basic financial transactions, while risk management personnel can access more sensitive data and perform larger financial operations. The e-bank will be able to ensure control and security of access to information, and not grant any user excessive power [25] [26].

II. E-BANK AUTHENTICATION MODEL

In this paper a high priority on security and client data protection is placed. In the context of e-banking, RBAC model is an essential tool for organizing and monitoring access to data and resources.

E-banks can reduce security risks and enhance access control by assigning roles and defining the permissions that accompany them. Although senior management employees may access sensitive data and make important choices, day-to-day operations employees may carry out their normal duties and access vital data. RBAC is therefore a crucial tool for enhancing security in an environment involving electronic banking because it helps to increase security and protection and facilitate access regulation and monitoring. The RBAC approach in an e-banking environment provides many other benefits, by reducing human error and simplifying management and monitoring procedures, RBAC helps increase efficiency. In addition, it helps to better manage reports and permissions, which helps facilitate monitoring and compliance with banking legislation and laws.

In this paper, RBAC will be created and implemented in the e-banking by defining the roles and authority that fit each role. First, the main roles in the system will be identified. These roles are:

1. The general supervisor.
2. The human resources employee.
3. The financial employee.
4. The information management employee.
5. The customer.

After that, the Authorizations will be organized and distributed to each role according to the needs and responsibilities of each role. The contribution of this paper is to enhance the security, efficiency and privilege management of e-banking.

The basic roles that should be included and implemented in an electronic banking system will be explained.

1. Administrator: He will be given the authority of the system administrator, where he will be responsible for managing users and roles, accessing to all roles, and Assigning roles to every user who enters the system.
2. Human Resources Manager: The human resources employee has the authority to deal with clients, verify their identity, and manage their requests regarding modification or addition to the client's personal data. Likewise, customer data cannot be modified unless approval is requested from this role.
3. Financial Management: The financial manager has the authority to create bank accounts for new customers in the system, as well as verify and monitor financial transactions, including withdrawals and deposits, by clients.
4. Information Manager: One of the responsibilities of the information manager is to monitor users' activities in the system and their requests on a regular basis, and to record all operations that take place in the system through periodic reports. As well as invalidating any suspicious roles that affects the security and safety of the system.
5. The client will have access to its personal and banking information, making changes to the personal information after obtaining the approval of the human resources employee, as well as conducting banking transactions that include deposits, withdrawals, and transferring funds to other clients.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 5, pp 150-155, May-2024

https://doi.org/10.47001/IRJIET/2024.805023

The operating process of the system is illustrated in the diagram in figure 2.

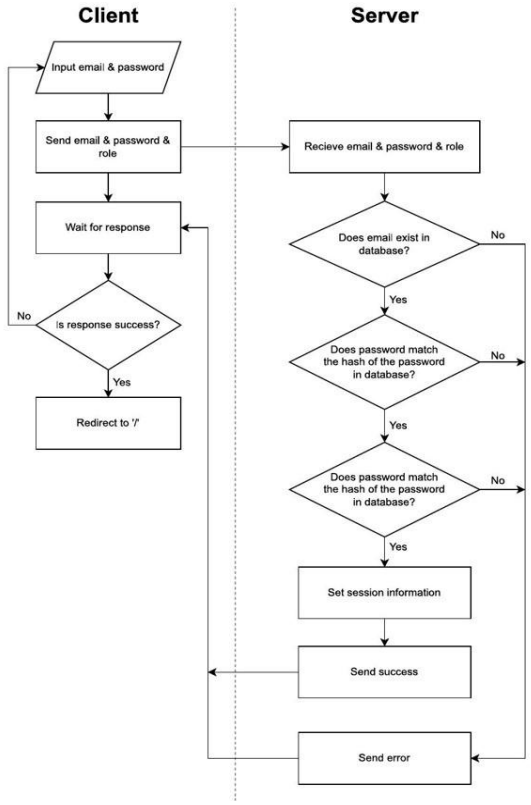

Figure 2: The system function

III. RESULTS AND DISCUSSIONS

The following subsections describe the fundamental concept of the suggested scheme shown in Figure 2:

1. User Registration and Email Confirmation:

When a new user visits the /register endpoint to create an account, he/she must complete registering and filling out a list containing his/her personal data, an email with a confirmation link is sent to the user's email address. The user then clicks on the confirmation link to verify their email address.

2. User Login and Access Control:

After confirming the email, the user logs in using the /login endpoint. Upon successful login, the user is redirected to the /home endpoint, where they can access their dashboard.

Access to certain endpoints is restricted based on the user's role.

For example:

- Regular users can access basic functionalities like viewing their account details (/users/me) and uploading an image (/users/image).
- Human Resource (HR) managers can perform additional actions such as creating new users (/users/new) and update user information's (/users/<user_id>/roles).
- Admins have access to all functionalities, including managing roles (/roles) and accounts (/accounts).

3. Role Verification:

When a user requests access to certain functionalities that require a specific role, such as creating a new user or managing roles, their request is checked against their assigned role. If the user's role hasn't been verified by an admin or information manager, they are redirected to /deactivated and prompted to contact the appropriate authority for role verification.

4. Account Management:

Users with appropriate permissions, such as finance managers, can create new accounts (/accounts/new) and manage existing accounts (/accounts/<account_id>). They can also perform actions like activating/deactivating accounts and managing transactions (depositing and withdrawing funds).

5. Request Management:

Users with roles like HR managers, information managers, and finance managers can view and manage requests. They can accept or reject requests based on their nature, such as role verification requests or account creation requests.

Login Scenario: During the login process, the user follows these actions:

Step 1: The user begins the login process when he enters his username in the designated field. This is followed by entering the secret password that was previously set.

Step 2: After receiving the login request, the application checks the credentials entered against the user information that is kept in the database of E-bank system and then authenticates the user if the credentials are correct.

Step 3: It is checked whether the user has validated his email address after successful authentication. We move to the next stage if the email is verified. The user receives a notification alerting them that they must verify their email before they are sent to the login page if the email is not verified.

Step 4: It is checked whether the administrator or information manager has validated the user's role after verifying his email. The user moves to the next stage if the task is confirmed. The user is asked to contact the relevant authority to verify the role and is redirected to /deactivated if the role is not validated.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 5, pp 150-155, May-2024

https://doi.org/10.47001/IRJIET/2024.805023

The user is authenticated after completing all the mentioned verification processes. Depending on the user roles and permissions granted to them, the user will be able to access the functions and features of the application.

The user can access additional features such as managing accounts and users and performing other administrative duties if he has the necessary rights.

Logout Scenario: Ending the session correctly and the steps the client follows to exit the system safely to ensure data integrity are explained in this section

Step 1: After receiving a request to log out of the application, all user information and session data, including any unique authentication tokens that may have been retained, are deleted.

Step 2: The application asks the user to log in again if he wants to continue using it after terminating his session and redirects him to the login page. To verify that the logout was successful, a flash message may appear after you are redirected to the login page. "You have successfully logged out".

Register Scenario: The following actions are taken by the user during the registration process

Step 1: To create a bank account for a new user, the new user navigates to /register. The user completes the registration list by entering all required fields, including password, email address, and user name. After that, the application form is sent to the application.

Step 2: After receiving the request, the data entered by the user is verified. Verify the strength of the password, ensure that the user name and email are unique, and check any other mandatory fields.

Step 3: An email containing a special link for verification is generated by the application. The email provided by the user during the registration process is the recipient of this email.

Step 4: After receiving the email notification, the user verifies his email address by click on the verification link.

Step 5: After completing the request for email notification, the application updates the database with the user's confirmed email address. The user's registration is deemed successful if the email address is correctly verified and the verification link is legitimate.

Resource Access Scenario: This scenario illustrates how authorization works within the application to control access to resources such as user details, accounts, and role

1. User Role Determination:

When a user logs into the application, their role is determined based on their credentials and stored information in the database. The role is typically assigned during registration or managed by an administrator.

2. Accessing User Information:

After logging in, a user with the role of an HR manager wants to view the details of other users in the system.HR manager navigate to the /users endpoint. the application checks the user's role to determine if they have the necessary permissions to view user information. Since the HR manager role is authorized to view user details, the access is granted. After that The HR manager can now see a list of users, including their usernames, email addresses, and roles.

3. Limited Access for Regular Users:

A regular user without administrative privileges tries to access the /users endpoint to view user details. However, since the user's role does not match any of the authorized roles for accessing user information, the application denies access. The user receives a flash message indicating that they do not have permission to access the requested resource and is redirected to the homepage.

4. Accessing Account Information:

A finance manager logs into the application and wants to create a new account for a user. He navigates to the /accounts/new endpoint, which is restricted to users with roles of “finance manager". Upon accessing the /accounts/new endpoint, the application checks the user's role to determine if they have the necessary permissions to create a new account. Since the finance manager role is authorized to perform this action, the access is granted. The finance manager fills out the necessary information to create a new account and submits the form. The application processes the request and creates the new account in the system.

5. Unauthorized Access Attempt:

An unauthorized user tries to access the /accounts/new endpoint directly by entering the URL in the browser. Since the user's role does not match any of the authorized roles for creating accounts, the application denies access and the user receives a flash message indicating that they do not have permission to access the requested resource and is redirected to the homepage.

ISSN (online): 2581-3048
Volume 8, Issue 5, pp 150-155, May-2024
https://doi.org/10.47001/IRJIET/2024.805023

IV. CONCLUSION

In this paper, a novel strong authentication scheme for authenticate e-banking system is proposed based on two-factor authentication scheme which involving a strong password and verification via a link sent to a Gmail account for user, that is considered an effective way to improve the security of electronic bank accounts. When users trying to access their accounts, the users must enter the right password, after that a special link is sent to their Gmail account for verification. This procedure lowers the possibility of unwanted access and electronic breaches by enabling the user to confirm their identity and authority to use the account, according to the principal of "something you have and something you know" is the main goal of this approach, which strengthens security.

ACKNOWLEDGEMENT

The resources provided by the University of Mosul/College of Computer Science and Mathematics are much appreciated by the writers, as they enhanced the caliber of their work.

REFERENCES

[1] Kiljan, Sven, Harald Vranken, and Marko van Eekelen. "Evaluation of transaction authentication methods for online banking." Future Generation Computer Systems 80 (2018): 430-447.

[2] Mohammed, Saja J., and Dujan B. Taha. "From cloud computing security towards homomorphic encryption: A comprehensive review." TELKOMNIKA (Telecommunication Computing Electronics and Control) 19.4 (2021): 11521161.

[3] Barkadehi, Mohammadreza Hazhirpasand, et al. "Authentication systems: A literature review and classification." Telematics and Informatics 35.5 (2018): 1491-1511.

[4] Wang, Xuerui, et al. "Attacks and defenses in user authentication systems: A survey." Journal of Network and Computer Applications 188 (2021): 103080.

[5] Alsaadi, Israa M. "Physiological biometric authentication systems, advantages, disadvantages and future development: A review." International Journal of Scientific & Technology Research 4.12 (2015): 285-289.

[6] Baig, Ahmed Fraz, and Sigurd Eskeland. "Security, privacy, and usability in continuous authentication: A survey." Sensors 21.17 (2021): 5967.

[7] Sharma, Uttam, et al. "Optimized authentication system with high security and privacy." Electronics 10.4 (2021): 458.

[8] Mathias, Craig. "Why mobile user authentication is more important than ever." (2014).

[9] Shah, Syed W., and Salil S. Kanhere. "Recent trends in user authentication–a survey." IEEE Access 7 (2019): 112505112519.

[10] Dasgupta, Dipankar, Arunava Roy, and Abhijit Nag. Advances in user authentication. Cham, Switzerland: Springer International Publishing, 2017.

[11] Mohammed, Saja J. "Using biometric watermarking for video file protection based on chaotic principle." International Journal of Computer Science and Information Security (IJCSIS) 15.12 (2017): 201-206.

[12] MOSTAFA, Ehab Younis, and Saja J. MOHAMMED. "THE LANDSCAPE OF AUTHENTICATION SYSTEMS: A COMPREHENSIVE SURVEY.", MINAR International Journal of Applied Sciences and Technology, 5 (4), 1-16.

[13] Bošnjak, Leon, J. Sreš, and Bosnjak Brumen. "Brute-force and dictionary attack on hashed real-world passwords." 2018 41st international convention on information and communication technology, electronics and microelectronics (mipro). IEEE, 2018.

[14] Karim, Nader Abdel , et al . " Online Banking User Authentication Methods : A Systematic Literature Review." IEEE Access (2023).

[15] Chaimaa, Belbergui, Elkamoun Najib, and Hilal Rachid. "E-banking overview: concepts, challenges and solutions." Wireless Personal Communications 117 (2021): 1059-1078.

[16] P. A. Aidonojie, O. O. Ikubanni, and N. Okuonghae, "The prospects, challenges, and legal issues of digital banking in Nigeria," Cogito: Multidisciplinary Res. J., vol. 14, p. 186, 2022.

[17] K. Matthews, J. Thompson, and T. Zhang, "Economics of Banking, The," World Scientific, 2023.

[18] N. Agrawal and S. Tapaswi, "A trustworthy agent-based encrypted access control method for mobile cloud computing environment," Pervasive Mobile Comput., vol. 52, pp. 13-28, Jan. 2019.

[19] R. El Sibai, et al., "A survey on access control mechanisms for cloud computing," Transactions on Emerging Telecommunications Technologies, vol. 31, no. 2, p. e3720, 2020.

[20] J. Yang, et al., "A model study on collaborative learning and exploration of RBAC roles," Wireless Communications and Mobile Computing, vol. 2021, pp. 1-9, 2021.

[21] J. Xu, et al., "Role-based access control model for cloud storage using identity-based cryptosystem," Mobile Networks and Applications, vol. 26, pp. 1475-1492, 2021.

[22] Mohammed, A. J., & Mohammed, S. J. (2024). Securing Cloud Computing Using Access Control

ISSN (online): 2581-3048
Volume 8, Issue 5, pp 150-155, May-2024
https://doi.org/10.47001/IRJIET/2024.805023

Systems: A Comprehensive Review. ", Book series: Lecture Notes in Networks and Systems, Springer".

[23] R. Ghazal, et al., "Intelligent role-based access control model and framework using semantic business roles in multi-domain environments," IEEE Access, vol. 8, pp. 12253-12267, 2020.

[24] A.S. Alshamsi, Z. Maamar, and M.-A. Kuhail, "Towards an approach for weaving Open Digital Rights Language into Role-Based Access Control," in Proc. 2023 International Conference on IT Innovation and Knowledge Discovery (ITIKD), IEEE, 2023.

[25] L. Dongdong, et al., "Role-based access control in educational administration system," in MATEC Web of Conferences, vol. 139, EDP Sciences, 2017.

[26] F. Li, et al., "Customer satisfaction with bank services: The role of cloud services, security, e-learning and service quality," Technology in Society, vol. 64, p. 101487, 2021.

[27] A.A. Shaikh and H. Karjaluoto, "Mobile banking adoption: A literature review," Telematics and Informatics, vol. 32, no. 1, pp. 129-142, Feb. 2015.

Citation of this Article:

Alaa J. Mohammed, Saja J. Mohammed, "Authenticated E- Bank System Based on RBAC Model", Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 8, Issue 5, pp 150-155, May 2024. Article DOI https://doi.org/10.47001/IRJIET/2024.805023

****

