International Journal of Scientific & Engineering Research Volume 9, Issue 7, July-2018
ISSN 2229-5518

Design and Implementation of authentication model for the Iraqi AMS Web-based Management System

Ahmed Qassim Hadi
Informatics Institute for Postgraduate Studies
Iraqi Commission for Computers and Informatics
Baghdad, Iraq
ahmedkh082@gmail.com

Shaimaa Hameed Shaker
Computer Science Department
University of Technology
Baghdad, Iraq
120011@uotechnology.edu.iq

Amer S. El-Ameer
Informatics Institute for Postgraduate Studies
Iraqi Commission for Computers and Informatics
Baghdad, Iraq
amerelameer@yahoo.com

Abstract— this work aims to specify appropriate authentication controls based on power essential for Web-based applications that recognized by operators, to have a high possible for impression. It is also required to increase the body of knowledge of information security on proper authentication controls to decrease threats of impression in applications, though search for accurate and legalize level of authentication strength, to each of the various events lead in such applications.

Keywords—authentication; authentication model; authentication design; web application; password; MD5 algorithm

I. Introduction

Formerly, the Internet was shaped as a communication instrument. It was established to allow publics to transfer information, data and messages. Currently, publics can interconnect with family or friends in another side of the world rapidly. Operators from everywhere can easily share information using the internet[1]. Nevertheless, since the expansion of the Internet, there is a growth in the size of cybercrime happenings always[2]. When Criminals commits a crime, no longer they need to be actually present. In this way, an extreme challenge to have digital security [3]. In current technology, to verify a user's ID, the Web applications including password logins as essential authentication. The first line of defense against attacker exploitation is the passwords [4].

The most common weaknesses in Web based apps are common, it is finally lead to severe security threats[5]. From there, the hackers exploit these failings in Web based apps with some tool supporting[6]. These security threats[7] produces a necessity to use authentication mechanisms in Web based apps. Therefore, passwords were founded to prove the identity of user throughout the authentication. If a password keeps valued data, including sensitive information and assets of an organization, then they are frequently the main target of a hacker. If a password is stolen, pinched or guessed, the hacker can block a user to login into his account, and he will access his sensitive information. Actually, most web applications store passwords plain text in the database[8]. Hashing the password was presented because of these situations[9]. Applying hash techniques to convert the passwords from plain text to hash values, that is not readable in databases.

Hashing is a one way technique that used to scrambling data via an algorithm. Most data is removed throughout the hashing process, and a moderately small hash value is produced compared to the original data. Since hash a one-way process, it is a non-reversible function. Therefore, it is difficult to reverse hash values back to the original inputs[10]. MD5 (message digest algorithm) is an essential algorithm of digital signature; detect authentication and data encryption of user account of its special ability of strong one-way encryption and irreversibility. Therefore, MD5 is commonly used in login and authentication part in which password is encoded by MD5 algorithm. The idea of login method is to match the scrambled password value with the password that stored in database which is no longer the original password match or not[11].

Lin-Lai [12] proposed a structure based on EIGamal crypto-system but their structure is failed to deliver mutual authentication and later suffers from server spoofing attack.

Hwang and Li [13] and Khan and Zhang [14] also offered a system based on EIGamal crypto-system, but suffers from time management.

Liao and Hwang and many others proposed a remote authentication system based on multi server environment [15, 16].

The section II describes the proposed system, the section III discuss the design of authentication model of the proposed system.

II. The proposed system

The Academic Monitoring System (AMS) is a proposed management system of a web based application for monitoring the Iraqi academic research activity, it aims to put the Iraqi scientific research in one place and extract the required statistics to calculate the rank of researchers and the rank of universities, it is an attempt to create main and complete database system to discover the scientific and activities for the Iraqi academics in the world classifications according to their universities. The (AMS) is an interactive web-based application that permits Iraqi researchers to insert their scientific productions and publications, and let them to review and download other researches. It is designed to facilitate the academic research activity monitoring for the ministry of higher education. The aim of this proposed system is to design and implement Academic monitoring System for the ministry of Iraqi higher education, calculate the rank of academic researchers, and Iraqi university rank based on researchers productions. The proposed system provides a framework for the Iraqi academics and their scientific productions; it offers a user friendly interfaces, well-designed web pages and high security to save user data.
In AMS case, there are three types of users (Main Admin, Sub Admin, Researchers) and the unregistered users. The main admin and sub admin has the capability to read and confirm the data of the researchers in the database, while the researchers can read, update and write in their profiles. The unregistered users (visitors) can only read data of the researchers in the database.
There are two needs affect the design of the authentication for the system. First, it should be safe. Second, it should be suitable for the user. There is not a solution can achieve all the needs because there are many users and a huge different between user groups. This system covers three kinds of authentications, figure (1).

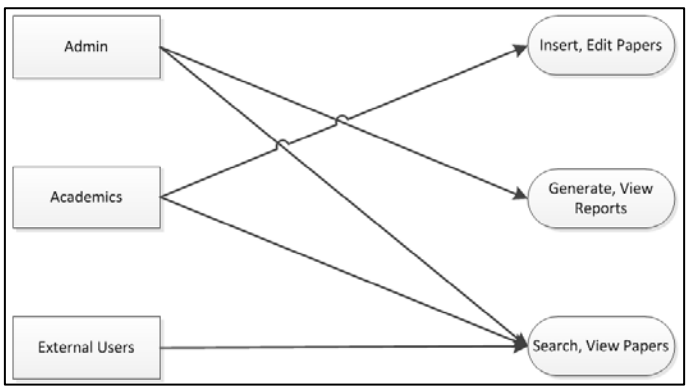

Figure (1) Kinds of authentication in proposed system

1. Central authentication system (CAS).
2. E-mail authentication system.
3. Secure ID.

III. The proposed design of authentication model

This system is created to observe and register scientific papers of the academics, make a number of papers for every registered. So, can observe all the details and change them with the special access rights. The application includes three authentication related classes as mentioned earlier.
In the AMS, data must be encrypted for the objective of security; this is done to avert information hacking or forced intrusion. MD5 cryptography algorithm is applied to this purpose to encrypt user passwords. When a user's password is preserved to the database, it is encrypted so if an attack has truly happened the data saved in the database turn into worthless because it is encrypted.
The next is the stages of creating hash value employing MD5 figure (2):

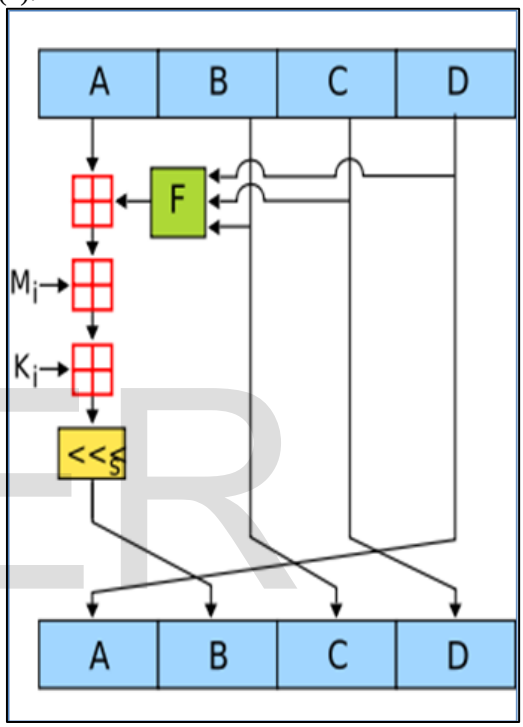

Figure (2) MD5 Algorithm

1) Data Padding: The message is padded in order to its length in bits is 64 bits short of being a multiple of 512 bits long.
2) Append length: A 64-bit impersonation of the real message length is appended to the consequence of the former step.
3) MD buffer Initialization: A four-word buffer, called MD buffer, is employed to compute the message digest. This buffer is started with fixed hexadecimal values.
4) Operation the message in 512-bit blocks.

The authentication mechanisms in the proposed system are divided to two phases, first phase contains several steps as in figure (3), and they are:

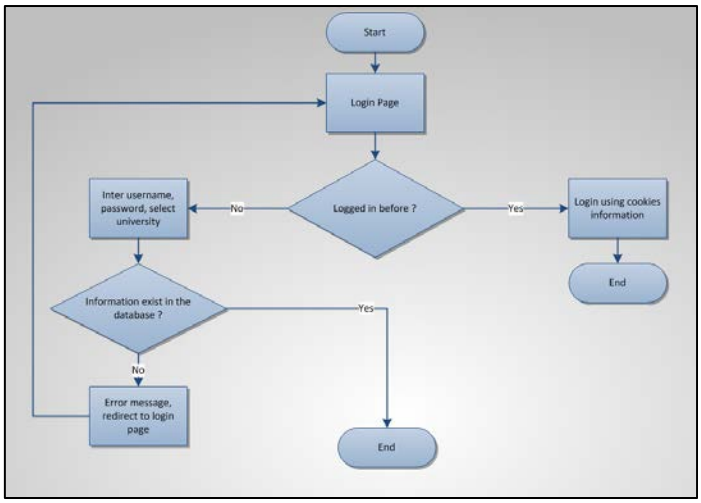

Figure (3) first phase in proposed authentication model

- Step one: check if the user have logged in before, then use the cookies to login.
- Step two: if the user is not logged in before, then force the user to insert (email address as a user name, password, and select university).
- Step three: determine if the database contains this username and password, if it return true then go to second level, else redirect the user to login page with error message as shown in figure (4).

Figure (4) error message in login web form

After check whether the user name and password are exist, the second phase also contain several steps which it shown in figure (5), it is:

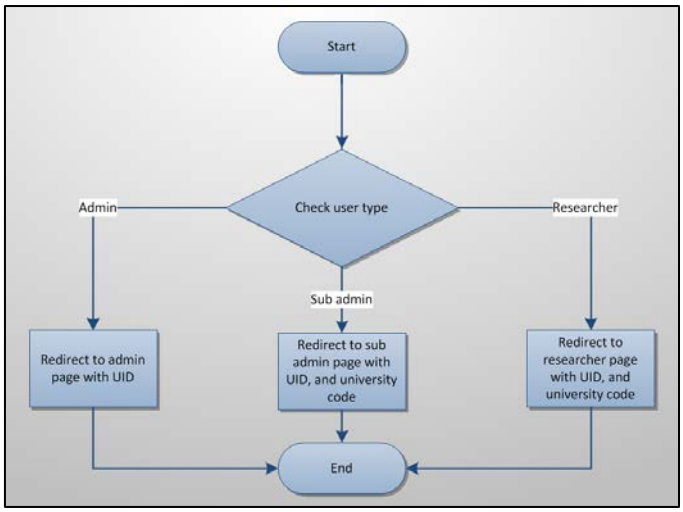

Figure (5) second phase in proposed authentication model

- Step one: in this step the system read the user type from the database.
- Step two-A: if the user type is a researcher, then create a session and a session ID between server and user, redirect user to (researcher home page) to view his profile, with a string that contains user's unique information, which contain UID (Unique Identification Number) and university code ID.
- Step two-B: if the user is a sub admin (university admin), then create a session and session ID between the user and the server, and redirect user to (university home page), with a string that contains university's unique information, which contain UID (Unique Identification Number) and university code ID.
- Step two-C: if the user is a main admin (MOHE admin), then create a session and session ID between the user and the server, and redirect user to (main admin home page), with a string that contains unique information, which contain UID (Unique Identification Number), this time there is no university code needed because the main admin has permission to access to all universities.

IV. Discussion:

MD5 (message digest algorithm) is an essential algorithm of digital signature; detect authentication and data encryption of user account of its special ability of strong one-way encryption and irreversibility. Therefore, MD5 is commonly used in login and authentication part in which password is encoded by MD5 algorithm. The idea of login method is to match the scrambled password value with the password that stored in database which is no longer the original password match or not. This technique takes message of random length as input, and creates a 128- bit "fingerprint" or "message digest" as output. It is estimated that it is computationally impossible to create two messages having the same message digest, or to create any message having a given pre-specified target message digest. It is very resistant to collisions.

The proposed system is created to observe and register scientific papers of the academics, make a number of papers for every registered. So, can observe all the details and change them with the special access rights. The application includes three authentication related classes figure (6):

- Long term users: is the major user group for instance system. They are use the system a few years.
- Short term users: is the active user group for instance system. They are use the system a few months.
- One time users: this instance system is used largely, but rarely for one time or a few times.

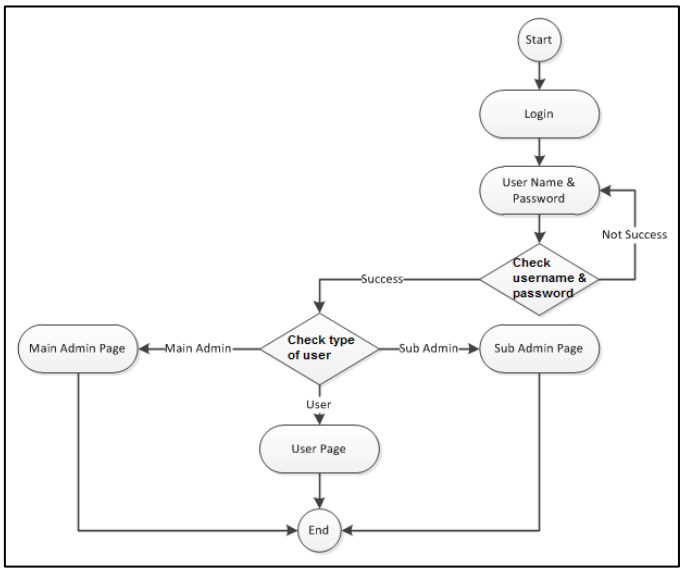

Figure (6) the system Authentication Process

V. Conclusion

The proposed system provides a suitable authentication model for the Iraqi academic monitoring system; it offers a user access control, well-designed authentication mechanism and high security to save user data. It provides a suitable authentication controls to reduce threats of impersonation in systems and to validate the right level of authentication strength.

References

1. Ahmed, A.A., A. Jantan, and M. Rasmi, *Service violation monitoring model for detecting and tracing bandwidth abuse.* Journal of network and systems management, 2013. **21**(2): p. 218-237.
2. Elejla, O.E., A.B. JANTAN, and A.A. AHMED, *THREE LAYERS APPROACH FOR NETWORK SCANNING DETECTION.* Journal of Theoretical & Applied Information Technology, 2014. **70**(2).
3. Ahmed, A.A. and N.A.K. Zaman, *Attack Intention Recognition: A Review.* IJ Network Security, 2017. **19**(2): p. 244-250.
4. Ahmed, A.A. and L.M. Khay. *Securing user credentials in web browser: Review and suggestion*. in *Big Data and Analytics (ICBDA), 2017 IEEE Conference on*. 2017. IEEE.
5. Mostardi, R.E., et al., *A HIGH-RESOLUTION HUBBLE SPACE TELESCOPE STUDY OF APPARENT LYMAN CONTINUUM LEAKERS AT $z\sim 3$.* The Astrophysical Journal, 2015. **810**(2): p. 107.
6. Teh, J.S., A. Samsudin, and A. Akhavan, *Parallel chaotic hash function based on the shuffle-exchange network.* Nonlinear Dynamics, 2015. **81**(3): p. 1067-1079.
7. Belfedhal, A.E. and K.M. Faraoun, *Fast and efficient design of a PCA-based hash function.* International Journal of Computer Network and Information Security, 2015. **7**(6): p. 31.
8. Kumar, R. and G. Mahajan, *A novel framework for secure file transmission using modified AES and MD5 algorithms.* International Journal of Information and Computer Security, 2015. **7**(2-4): p. 91-112.
9. Ora, P. and P. Pal. *Data security and integrity in cloud computing based on RSA partial homomorphic and MD5 cryptography*. in *Computer, Communication and Control (IC4), 2015 International Conference on*. 2015. IEEE.
10. Dobbertin, H., *Secure hashing in practice.* Information Security Technical Report, 1999. **4**(4): p. 53-62.
11. Zhong, L., W. Wan, and D. Kong. *Javaweb login authentication based on improved MD5 algorithm*. in *Audio, Language and Image Processing (ICALIP), 2016 International Conference on*. 2016. IEEE.
12. Lin, C.-H. and Y.-Y. Lai, *A flexible biometrics remote user authentication scheme.* Computer Standards & Interfaces, 2004. **27**(1): p. 19-23.
13. Hwang, M.-S. and L.-H. Li, *A new remote user authentication scheme using smart cards.* IEEE Transactions on consumer Electronics, 2000. **46**(1): p. 28-30.
14. Khan, M.K. and J. Zhang, *Improving the security of 'a flexible biometrics remote user authentication scheme'*. Computer Standards & Interfaces, 2007. **29**(1): p. 82-85.
15. Lin, I.-C., M.-S. Hwang, and L.-H. Li, *A new remote user authentication scheme for multi-server architecture.* Future Generation Computer Systems, 2003. **19**(1): p. 13-22.
16. Liao, Y.-P. and S.-S. Wang, *A secure dynamic ID based remote user authentication scheme for multi-server environment.* Computer Standards & Interfaces, 2009. **31**(1): p. 24-29.