**A WEB BASED HTTP CLIENT-SERVER WITH ENCRYPTION, SMTP PROTOCOL, TOKENIZATION COOKIES AND IP AUTHENTICATION IN HUMAN RESOURCE MANAGEMENT SYSTEM**

**Literature Review**

**Members:**

***Salman Ahmed Khan (19K-1043)***

***Khizar Jilani (19K-1057)***

***Hasnain Abbas (19K-1059)***

***Sadeem Sattar (19K-1102)***

***Abdullah Tilal Khan (19K-1103)***

**Presented To:**

***Miss Atifa Batool***

**Technical Business Writing (FAST NUCES)**

**Dated: December 23, 2021**

**Abstract**

The Human Resource Management System (HRMS) aims to facilitate the management operation in an organization. It focuses on the communication of three entities including Admin, HR and Employee. Its objective is to automate the daily activities carried out by these activities. The HRMS is based on HTTP Client-Server that allow clients to make http request to fetch their respective page portal whereas the data is send by the server as per client request. The security feature is also implemented in password with Bcrypt encryption of RSA Algorithm and SHA-256 Algorithm. The SMTP protocol is implemented for sending email alerts from server to client. The Client IP authentication is also carried out to ensure the user connectivity within the organization. The respective client session is also maintained with the tokenization and cookies to control the access by server making it a state-full server. Through this the transparency between the entities is ensured with the privacy and with relevant data submission.

**Introduction**

For the past decade, the human resource management has evolved and developed into different areas and disciplines. The process in the HRMS has been went through trials and errors of the communication between the entities associated with the HRMS.

The Human Resource Management System (HRMS) is concerned with the activities and processes carried out within an organizational entity to easily communicate with each other with respect to their duties and process. The changing organizational need in the marketplace have raise concerned for the improvement and efficiency of the human resource discipline with the development in the networking domain of the system.

The Human Resource Management System focuses on the main entities associated with the system which include Administration, HR and Employee that will communicate with each other with the system. The HRMS will follow the automation process rather than manual that will save the users time rather than investing their precious time on the system.

The HRMS is composed on the Client Server Architecture. The users of the system provide the request to the web based HRMS system to fetch their respective data and page portal [1]. It will generate the HTTP client request that will be accepted by the server with the TCP Protocol to assess the HTTP request [2]. The server then provides with the accurate result as per the client request and respond with the HTTP response.

The HRMS ensure the data privacy of its users by implanting the security feature in the password generation of the user using Hashing of Bcrypt which include RSA Algorithm and SHA-256 Algorithm that prevent illegal access of attacker to breach the system to access the user data and make it more secure for the consultancy of the user.

The HRMS also provide SMTP Protocol to send the email to the employee associated with the system when it is registered with the system ensuring the updated information is provided that create validation with the system. The SMTP protocol forward the header packet to the remote server using IMAP or POP3 to download the mail stored in local mail server [3].

The user connectivity session with the system is maintained by storing the cookies of the user in the system and perform tokenization using JWT tokenization to identify the specific request of the user currently logged and associated with the system.

The employee Client IP is also authenticated with the system to prevent illegal access of the user to attempt their attendance until the user reside with the premises and connected with the IP of the organization.

**Background**

The Human resource management plays an important role in the workforce of an organization. Due to the non-authentication, non-automation, single based system without HTTP request and response, a centralized system cost heavily to the organization with a poor networking in the system. Moreover, the email sending is not implemented in the systems that does not notify to the employee of the system that its details are encapsulated in the system.

The old HRMS system provide the attendance feature to employee that can be marked by employee at from anywhere without residing within the organization. This feature cause unauthorize access to the employee which can be used in illegal manner.

Similarly, the user’s privacy is at risk due to non-encrypted password in the system catalogue that is a fatal flow and is opened and welcomed to the attackers and hackers to breach and log in any user’s system.

Therefore, there is a need of such a system that can secure the users information from the outside world, which is non centralized implemented in HTTP protocol, maintain user’s sessions through tokenization and cookies, provide Email and IP authentication within the system.

**Features**

The HRMS consist on three entities that include Admin, HR and Employee with their respective dashboards and functionalities which are mentioned below:

**Admin:**

The following are the functionalities of Admin:

* Add HR Details
* Update HR Details
* Delete HR Details
* Manage Departments
* Manage Designation
* View its respective details

**HR:**

The following are the functionalities of HR:

* Manage Employees
* Approve Leave
* Approve Resignation
* Generate Payroll
* View Details

**Employee:**

The following are the functionalities of Employee:

* View Details
* Add Attendance
* Apply Leave
* Submit Resignation
* Receive Payroll

**HTTP Client – Server**

The HRMS is based on the client – server architecture in which the information and data of the respective client is submitted to the server to get the desired result. With the assistance of client-server rather than running on top of UDP, HTTP uses TCP as its underlying transport protocol[9]. The HTTP client sets up a TCP connection with the server initially. Once the connection is established, the browser and server processes use their socket interfaces to access TCP. The client server is rapidly evolving and with high level of uncertainity it envolve decision making[10].

The client creates a HTTP request to the sever[2]. This is carried out by the TCP handshaking connection between the client and server. The HTTP request either GET, POST, PUT or DELETE request is then transmit to the server to perform the client request. The server is then transmitted a HTTP respond back to the client containing the desired result as per client request.

**Bcrypt Encryption**

The HRMS provide the security feature to its users by saving their catalogue from outside world from hacker. The encryption is implemented in the login feature of the system. In the login feature, password is the part in which encryption is implemented. The bcrypt hashing is based on the Blowfish block cipher [7]. Encryption is used at several levels in the service, and it is enabled by default for all clients. Data access is enabled first through encrypted tunnels using Hypertext Transfer Protocol Secure (HTTPS), then it uses Perfect Forward Secrecy (PFS), which scrambles data as it moves between their and other companies' servers, and it uses SSL/TLS (Transport Layer Security) for connectivity, with the 256-bit TLS looking at the encryption enforceme [15].

It is encrypted by using hashing mechanism that include RSA Algorithms and SHA-256 Algorithm which could calculate byte-wisely just a modulo check of the block, whereas a stronger mixing function like SHA-256 that calculate the complex of block of hash[6] encrypt the user’s password, therefore, with encryption, the breaching of the system is reduced and it become impossible for the hackers and it ensure the protection of the users from illegal access.

**Cookies and Tokenization**

Cookies can be collected, altered, or embezzled since they are maintained and transported as in form of text. Cookies that safeguard them from security concern[11]. Despite their broad use, little work has been performed on their characteristics, such as standard attributes, placement standards, and the information that may be acquired through third-party cookies[12].The HRMS implement the cookies and tokenization. The cookies are used to save and store the user’s session within the system to provide a healthy connectivity to the users so that a user’s session could be maintained with the system. The cookies are implemented to track the activities of the users to prevent the breach of privacy of the users in the system [5].

Moreover, the process of tokenization is implemented to secure the users data and authorization in the login system of the respective users.

**SMTP Protocol**

The HRMS provide the feature on mailing the notification to the employees’ email when its details are attached in the system by HR. The E-mail message is sent to the sender's E-mail server using the SMTP protocol after the TCP connection between the E-mail client and the E-mail server is established. The E-mail server sends the email message to another E-mail server or directly toward the recipients' E-mail server using the same protocol[13].Additionally, it is done on communications between SMTP servers using transport layer security rather than end-user security or end-to-end encryption. It examine the cypher suites[14].

An auto generated email is send from HR to employee to notify about its entry. This mechanism is carried out by using SMTP Protocol over HTTP client response from client to the server. The SMTP server then uses DNS to fing the mail address and resolving the domain name of email to their respective IP address[4].

The SMTP mail is forwarded from HR to employee using the node-mailer that encapsulated the smtp protocol.

**Client IP Authentication**

The Attendance feature in employee dashboard implement the IP authentication. The employee cannot mark itself present until it is connected with premises in which the system is attached within the organization.

The client IP is fetched through the HTTP request send by the client to the server for requesting the attendance landing page.

The client IP is then authenticated with the organization’s IP to check whether the client is connected with the organization network and is within the premises of the organization and disallowing links to the site that leaves the premises[8]. If the IP is matched then authentication process is successful and attendance page is enabled and responded to the client by server by a HTTP response, else the authentication will be failed and the server will respond back with HTTP response of disabled attendance.

**Conclusion**

The HRMS provide the automated functionality for the organization management to carry out their day-to-day activities with the system. The system provides client-server implementation on HTTP, it also secure and preserver the users privacy through bcrypt encryption and tokenization. The clients’ sessions are also maintained to provide reliable access to the client through cookies. Also, the mailing process is autogenerated using SMTP Protocol and lastly the client IP authentication is also done to prevent illegal and faulty attendance in the system. Thus, making our HRMS a reliable and secure system.

**References**

[1] Sulyman, Shakirat. (2014). Client-Server Model. IOSR Journal of Computer Engineering. 16. 57-71. 10.9790/0661-16195771. Available: htttps://www.researchgate.net/publication/271295146\_Client-Server\_Model

[2] Davis, P.T.(Editor) (1996). Securing Client/Server Computer Networks. McGraw-Hill, USA

[3] Riabov, Vladimir. (2007). SMTP (Simple Mail Transfer Protocol). 10.1002/9781118256114.ch26.

[4] Campbell, P., B. Calvert, and S. Boswell.2003. *Security + Guide to Network Security Fundamentals.* Boston: Cisco Learning Institute.

[5] Cahn, Aaron & Alfeld, Scott & Barford, Paul & Muthukrishnan, Senthilmurugan. (2016). An Empirical Study of Web Cookies. 891-901. 10.1145/2872427.2882991.

[6] Smiatacz, Maciej & Wiszniewski, Bogdan. (2021). Just look at to open it up:. Multimedia Tools and Applications. 80. 1-36. 10.1007/s11042-021-10533-8.

[7] Malvoni, Katja & Designer, Solar & Knezovic, Josip. (2014). Are Your Passwords Safe: Energy-Efficient Bcrypt Cracking with Low-Cost Parallel Hardware. 10.13140/2.1.3267.0081.

[8] Kharade, Kabir & Kharade, Shraddha & Katkar, Smita. (2019). Cyber Security -A Method of Generic Authentication of Data with Ip Security. 9.

[9] Natesan, Abirami N. (2019). A Detailed Study of Client-Server and its Architecture.

[10] Sawyer, Steve & Southwick, R.. (1996). Distributed work and client/server computing: issues from the field. 10.1007/978-0-387-35085-1\_20.

[11] B. Li, S. -j. Lv, Y. -s. Zhang and M. Tian, "The application research of Cookies in network security," PROCEEDINGS OF 2013 International Conference on Sensor Network Security Technology and Privacy Communication System, 2013, pp. 152-155, doi: 10.1109/SNS-PCS.2013.6553855.

[12] Aaron Cahn, Scott Alfeld, Paul Barford, and S. Muthukrishnan. 2016. An Empirical Study of Web Cookies. In <i>Proceedings of the 25th International Conference on World Wide Web</i> (<i>WWW '16</i>). International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 891–901. DOI:https://doi.org/10.1145/2872427.2882991

[13] Ramadass, Sureswaran & Bazar, Hussein & Abouabdalla, Omar & Manasrah, Ahmad & El-Taj, Homam. (2009). Active e-mail system SMTP protocol monitoring algorithm. 257 - 260. 10.1109/ICBNMT.2009.5348490.

[14] L. Baumgäertner, J. Höchst, M. Leinweber and B. Freisleben, "How to Misuse SMTP over TLS: A Study of the (In) Security of Email Server Communication," 2015 IEEE Trustcom/BigDataSE/ISPA, 2015, pp. 287-294, doi: 10.1109/Trustcom.2015.386.

[15] Nisha, Shireen & Farik, Mohammed. (2017). RSA Public Key Cryptography Algorithm – A Review. International Journal of Scientific & Technology Research. 6. 187-191.