Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.5, No.12, 2015
www.iiste.org

Design and Implementation of Multilevel Secure Database in Website

Hind S. Harba
Al-mostansaria university college of sciences

Abstract
Multi-tier web server systems are used in many importantcontexts and their security is a major cause of concern.Such systems can exploit strategies. In this paper, a model was present based onthree-tier architecture (Client tier, Server tier and Database tier) and applying multilevel security on it. The database server tier consists of the DBMS or the database management system and the database and we built it off-line to reduce unauthorized access to sensitive data. The Client tier, which is usually a web browser, processes and displays HTML resources, issues HTML requests and processes the responses. These web browsers are HTTP clients that interact with the Web servers using standard protocols. The Middle or application server tier consists most of the application logic. Inputs receives from the clients and interacts with the database but only the results sent to application server then to client. This achieved by using multilevel of security to protect database, using Authorization, Password Encryption. The process of authorization done by allowing the access to proposed system pages depending on authorized level; Password encrypted using bcrypt with fallbacks on sha-256/512 with key stretching to protect it from cracking by any types of attack. Client-to-Application Server Protocol (CAP) uses the RC4A algorithm to provide data confidentiality to secure transmitted information from application server to client.
Keywords: Authentication, Multi-tier model, Multi-Tier Security, Security, Data protection, Internet security.

1. Introduction

Internet applications such as online news, retail, and financialsites have become commonplace in recent years. Modern Internetapplications are complex software systems that employ a multi-tierarchitecture and are replicated or distributed on a cluster of servers.Each tier provides a certain functionality to its preceding tier andmakes use of the functionality provided by its successor to carryout its part of the overall request processing. For instance, a typicale-commerce application consists of three tiers a front-end Webtier that is responsible for HTTP processing, a middle tier,Java enterpriseserver that implements core application functionality, anda backend database that stores product catalogs and user orders. [1]

The three-tier architecture pattern provides a means of structuring and decomposing applications into three tiers or layers, where each tier provides a different level of responsibility. One tier deals with the presentation part of the system (user and system interfaces), another handles the business logic, being the core of the system, and the last tier is representing the data storage. Enterprise applications are typically implemented as three-tier architectures that consist of clients in the front tier, servers that perform the application business logic processing in the middle tier, and databases that store the application data in the back-end tier. [2]

This paper describes a method for design three-tier system and protecting its streamed data from possible security attacks. The main feature of the suggested design is its ability to provide a secure environment for real-time data or file downloading watching. One of security parts is to secure pages content, this done by used authorizing and authentication. Secondly, is to make password hashing very strong to prevent the password cracking by attacker. Thirdly, secure communication between Web browsers and servers this done by used RC4A with Secure Sockets Layer/Transport Layer Security (SSL/TLS).

2. Related Work

Most of the existing work of Web services performance modeling is confined to the front-end Web server. Wells et al. [3] made a performance analysis of Web servers using colored Petri nets. Their model is divided into three layers, where each layer models a certain aspect of the system. The model has several parameters, some of which are knownand the remaining unknown parameters that are determined by simulations. Doyle et al.[4] presents a simplified analytical model to predictthe response time of Web services. Their model is acombination model of server CPU and storage I/O.Still, the model only applies to single tier and is validonly for static content requests

Rykowski, and Wieczerzyck [5] propose a new architecture for web servers. This architecture is of three-tier type, and it is composed of a query language interpreter as the interface to the server, a specialized object-oriented database of resources as an engine, equipped additionally with semi-transaction and user managers, and an XML wrapper as a gateway to data repositories.

He Liduo and Chen Yan [6] provide a J2EE-based three-tier architecture technology for the construction of Web Content Management System, which aims to improve the effectiveness of development, management, and maintenance in web applications. Leite et al.

3. Background

Multi-tier architectures are traditionally used for database applications. The middle tier separates presentation and business functions and its services allow communication between programs based on different technologies and programming languages. Different technologies for realization of the middle tier exist (e.g. transaction processing, message-oriented, object-oriented, and Web-based). They differ in communication protocols and service allocation [7].

Multi-tier architecture provides many benefits over traditional client/server architecture [8]:

- Installing and deploying the user interface is virtually instantaneous - only the Web interface in the middle tier needs to be updated.
- Without a "thick" client interface, it is easier to deploy, maintain, and modify applications - no matter where the client is located.
- Because the application itself is server-based, users always access the most up-to-date version.

Modern Web services providers use a multi-tiered architecture to provide required services. While some Web applications use two tiers Web server and database server high volume sites typically add a third tier: application server to support complex business logic. As a consequence, the most widely deployed infrastructure of Web services is the 3-tiered architecture which is shown in Figure 1. This 3-tiered architecture provides both high level of scalability and reliability [9].

In this 3-tiered architecture, on the front line of atypical Web site is the Web server that acts as thepresentation layer. This tier has three functionalities:(1) Web server receives requests from the clients,service static Web requests; (2) at the same timeforwards complex dynamic content requests to the2nd tier; (3) receives responses from the 2nd tier andsends them back to the clients. Typical Web serverincludes Apache and Microsoft Internet InformationServer (IIS). [10]

4. Architecture of the Proposed System

The system is constructed from three-tier (client-server architecture) to specify the application as shown in figure (1).

- Client tier: a web browser runs in any computer which is responsible for handling the information representation for user request.
- Application server tier: it resides in middle tier, where it handle the initialization and the updated information. It is responsible for receiving client request, processing the data contained in request and applying the client response for updating the demand information.
- Database tier: the backend database reside on web server side and stores the data for system, which is required by the middle tier.

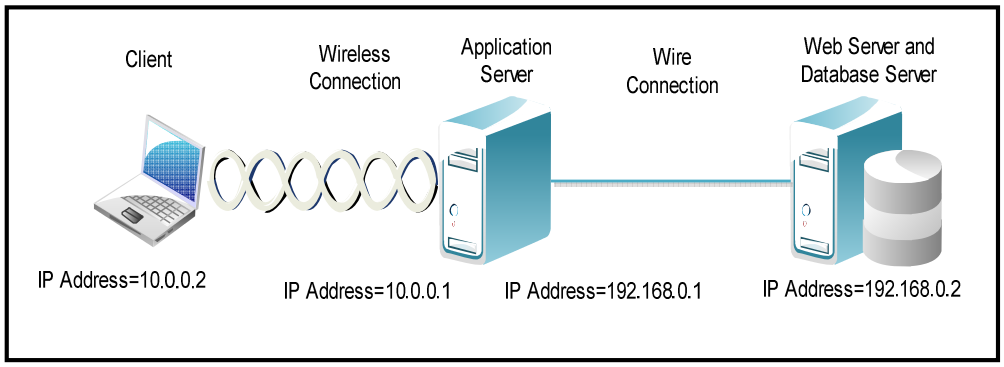

Figure (1): Implemented network for the proposed model

All three tiers (in this model) are connected with special network which consist of wired and wireless networks.

The application server is the important part of the network which contain two interface card for interfacing with client computer in one side and with the database in other side.The client computer (IP= 10.0.0.2) connected with server computer (IP= 10.0.0.1) in wireless network with special group.But the server computer used wired network for connecting with database server as (server comp. IP= 192.168.0.1) and (database server comp. IP= 192. 168.0.2) in other group.

4.1Client

In the client side the user of a web application can view data across the internet and into the web application. For

the sake of simplicity, the assumption of a browser-based web application will be made. Static HTML pages are manipulated by the user and the data is submitted via an HTML request into the web application. Data specific to the user is submitted within this request through the use of HTML page. After the client is connected to web application the user identifies himself to the system by sending secret password. To ensure the authentication of this password hashing algorithm is used. Only authorized user can enter the system and view home page to request specific page (such as view order table) the user request is sent to web application and the client is waited a response which is encrypted by using RC4A algorithm therefore the client must decrypt the encrypted page using the same algorithm to enable user to view data.

4.2 Application Server

Application server is a program that handles all application operations between users and an organization's backend business applications or databases. An application server is typically used for complex transaction-based applications. In this work, the middle tier is usually split recursively into three tiers again. The Client applications that run inside the browser submit requests to the web server using HTTP protocol/ The 'presentation layer' on the server transforms the request and passes it to the 'business layer' which will perform some computation by interacting with the 'data layer'. The results from the 'business layer' are then transformed into HTML by the 'presentation layer' and returned as the response to the client. The most popular way of generating HTML responses in the middle tier is by using the server pages (shadow files). The server page is a special HTML page that contains embedded scripts.

4.3 Database

The whole idea of a database driven web site is to allow the content of the site to reside in a database, and for that content to be pulled from the database dynamically to create web pages for people to view with a regular web browser.

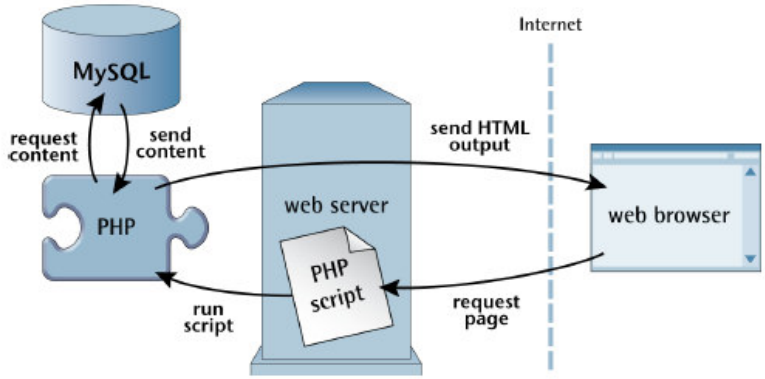

Figure (2) PHP retrieves MySQL data to produce web pages.

As shown in Figure 2, the PHP scripting language is the go-between that speaks both languages. It processes the page request and fetches the data from the MySQL database, then spits it out dynamically as the nicely formatted HTML page that the browser expects. When a person visits a page on database, driven web site the flowing steps is happen:

1. The visitor's web browser requests the web page using a standard URL.
2. The web server software (typically Apache) recognizes that the requested file is a PHP script, so the server fires up the PHP interpreter to execute the code contained in the file.
3. Certain PHP commands connect to the MySQL database and request the content that belongs in the web page.
4. The MySQL database responds by sending the requested content to the PHP script.
5. The PHP script stores the content into one or more PHP variables, and then uses echo statements to output the content as part of the web page.

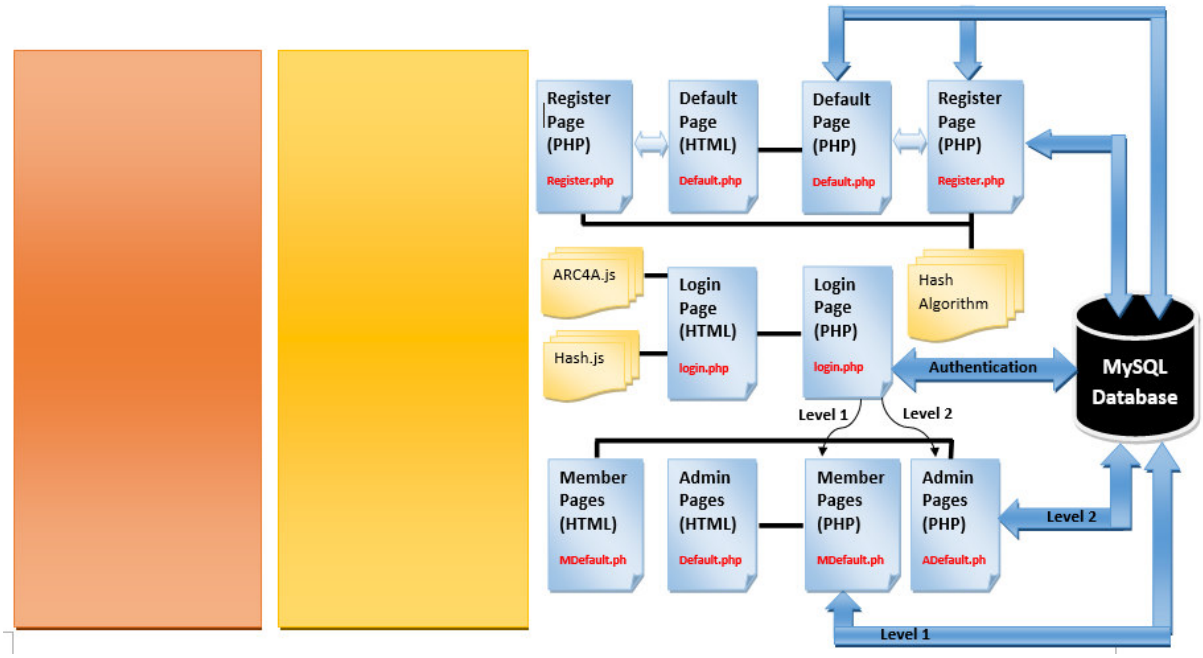

Figure (3): System architecture

5. System security

The security of system can be described as follows:

1- **Data Confidentiality:** The Client-to-Application Server Protocol (CAP) provides a standard method for transporting multi-protocol datagrams over Client to application server links. The CAP uses the RC4A algorithm to provide data confidentiality. The process of sending encrypted information is from application server to client to configure secure channel and this information is decrypted in client.

2- **User Authentication and Authorization:** Site Authorization is used to determine the level of user (visitor, member or administrator). The visitor can view the books content but cannot view or buy books but only the activated members have ability to view allowable books or buying not allowable books. In order to view member library user needs to enter authentication process to redirect to the member library.

3- **Password Encryption:** This method is used to encrypt user password transfer from client to server and then storied in MySQL database to protect them from being stolen or attacked from different attacks (SQL injection, Dictionary and Brute-Force Attack, Lookup Tables, Reverse Lookup Tables Rainbow Table, etc.), this is done by hashing password using BCrypt and salt.

4- **Disabling Browser Caching:** The Method used to bypass, clear, and disable browser cache so that each time client visit a page all the files are freshly downloaded.

5- **HTTP over Secure Sockets Layer (HTTPS):** HTTPS provides authentication of the web site and associated web server that one is communicating with, which protects against Man-in-the-middle attacks. Additionally, it provides bidirectional encryption of communications between a client and server, which protects against eavesdropping and tampering with and/or forging the contents of the communication. This provides a reasonable guarantee that one is communicating with precisely the web site that one intended to communicate with (as opposed to an impostor), as well as ensuring that the contents of communications between the user and site cannot be read or forged by any third party.

5.1Data Confidentiality

The Client-to-Application Server Protocol (CAP) provides a standard method for transporting multi-protocol datagrams over Client to application server links.

Cryptography is the only practical means to provide security services in many applications. Research into cryptography has exploded in the last 18 and a variety of cryptographic algorithms and techniques have emerged .RC4A is one of them.RC4A, an RC4 family algorithm designed by Ron Rivest for RSA Data Security, Inc. in 1987, developed by S. Paul and B. Preneel which attempts to increase security without decreasing efficiency. Their approach essentially takes two RC4 instances and crosses information between them. RC4A stream cipher works in two phases, KSA (Key Scheduling Algorithm) phase and PRGA (Pseudo Random number Generation Algorithm) phase. During PRGA two successive outputbyte are generated. The goal behind RC4A was to increase security primarily by increasing the internal complexity of the algorithm.RC4 used in the Secure Sockets

Layer/Transport Layer Security (SSL/TLS) standards that have been define for communication between Web browsers and servers. [11]

In proposed The CAP uses the RC4A algorithm to provide data confidentiality. The length of the session key to be used for initializing encryption tables can be negotiated. CAP currently supports 256-bit session keys. RC4A is a stream cipher, symmetric key algorithm. The same algorithm has been use for both encryption and decryption as the data stream is simply XORed with the generated key sequence. The key stream is completely independent of the plaintext used. It uses a variable length key from 1 to 256 bit to initialize a 256-bit state table. The state table has been use for subsequent generation of pseudo-random bits and then to generate a pseudo-random keystream which is XORed with the plaintext to give the ciphertext.

The sequence of bytes generated is not random since the output is always the same for a given input but it has to approximate random properties to make it harder to crack. The process of sending encrypted information is from application server to client to confm igure secure channel and this information has been decrypt in client.

5.2 User Authentication and Authorization

The proposed system offers three main user levels:

- *Visitor Level*, which allow all user to enter the site and view book content but not have the ability to view or buy books.
- *Member Level*, allow just for member users to show the full allowable books and the ability to buying not allowable books, but cannot access administrator pages.
- *Administrator Level*, which has the ability to access to all site content beside the ability to manage the site (i.e. add or remove members and edit his information) or books content

5.2.1Passwords Hashing

Passwords are a notoriously weak authentication mechanism. Users frequently choose poor passwords. An adversary who has stolen a file of hashed passwords can often use brute-force search to find a password p whose hash value H (p) is equal to the hash value stored for a given user's password, thus allowing the adversary to impersonate the user. [12]

Storing passwords as direct md5 hashes is not recommended [13]. MD5 is an older algorithm, the hash-pool is smaller (32 characters, but not all combinations are possible). The use of SHA1 is a lot better. It is a new algorithm, supposedly has less collision, and has a larger pool (40 characters and a higher percent of possible combinations).

In the proposed system, PHP hash (bcrypt) Passwords with random Salt have been used.

5.2.2Bcrypt Algorithm Scheme

Bcrypt is a hashing algorithm, which is scalable with hardware (via a configurable number of rounds). Its slowness and multiple rounds ensures that an attacker must deploy massive funds and hardware to be able to crack passwords. Add to that per-password salts (bcrypt REQUIRES salts) and have been sure that an attack is virtually unfeasible without either ludicrous amount of funds or hardware.

Bcrypt uses the Eksblowfish algorithm to hash passwords. While the encryption phase of Eksblowfish and Blowfish are the same, the key schedule phase of Eksblowfish ensures that any subsequent state depends on both salt and key (user password), and no state can be precomputed without the knowledge of both. Because of this key difference, bcrypt is a one-way hashing algorithm. It cannot retrieve the plain text password without already knowing the salt, rounds and key (password).

5.2.3System Password Algorithm Scheme

The proposed system uses a new, informative post on proper implementation of encryption using bcrypt with fallbacks on sha-256/512 with key stretching.

Password Encryption Algorithm

Input:	Password Characters ($password)
Output:	Encrypted Password Characters
Step 1:	Start.
Step 2:	Create hash using Blowfish hashing with a salt is as follows: $2a$" + a two digit cost parameter + "$" + 22 digits from the base64 alphabet "./0-9A-Za-z" + "$"
Step 3:	Create a new salt string which conforms to the requirements of CRYPT_BLOWFISH.
Step 4:	Fall-back SHA512 hashing algorithm with stretching.
Step 5:	Generates the password and verifies functions.
Step 6:	End.

In other word, after a user enters their ID and password, proposed system needs to take the user's ID

address and perform a database lookup to determine if a user account exists matching the supplied ID address. If an account exists, it needs to return the user's encrypted password and salt from the matching database row. With the returned salt, it need to run the encryption over the user supplied password to generate an encrypted password. It use this encrypted password and compare it to the returned encrypted password from the database to check for equality. If the two encrypted passwords are the same, the user supplied the correct password and we can log him in. It's up to you to implement the database calls and login; it's only been pseudo-coded in for completeness.

5.3 Disabling Browser Caching

The stored files are load from the hard drive instead of having to be downloaded from the Internet. This is a useful feature because it makes your Web surfing much faster. Sometimes, however, browser caching is undesirable – it may cause you to miss updates on a Web page that changes frequently. . If the cache is disabled, the browser is instructed to not save page content and will request it anew from the server. From a security perspective the cache should be disabled, so the browser does not store sensitive data and will always request pages from server if the URL changes.

There way used around this. You can bypass, clear, or even disable your browser cache so that each time you visit a page all the files are freshly downloaded.

- **Meta Expires**

  The following tag is used to expire the content immediately:

  <META HTTP-EQUIV="expires" CONTENT="0">

The above tag is also said to disable caching so that search engines will load a new copy of the site from the server every time an end user visits the site.

5.4 Secure Sockets Layer Authentication

Secure Sockets Layer (SSL) is a developer's tool for securing the transmission of data. A trusted certificate installed on the Web server offers visitors that good feeling of a secure environment. In the proposed system, a client (web browser) was authenticating themselves to server (website or server application) and that server also authenticating itself to the client through verifying the public key certificate/digital certificate issued by the trusted Certificate Authorities (CAs). From a high-level point of view, the process of authenticating and establishing an encrypted channel using SSL involves the following steps: (as show in figure 3.8)

Step 1: Satrt
Step 2: A client requests access to a protected resource.
Step 3: The server presents its certificate to the client.
Step 4: The client verifies the server's certificate.
Step 5: If successful, the client sends its certificate to the server.
Step 6: The server verifies the client's credentials.
Step 7: If successful, the server grants access to the protected resource requested by the client.
Step 8: End.

This SSL authentication has to great advantage that even hackers try to attack server he/she cannot access to the certified pages (like login page and member ship pages) without having the digital certification. In addition, the big advantage of using SSL is that all that data are protected (like passwords, information, videos, etc…).

6. Possible Attacks on Passwords and Their Solution

It has long been a common practice to store user passwords in a hashed form instead of the clear, human readable form. For years, hash-algorithms such as MD5 and SHA-1 have been the preferred methods, but these days neither should be used for any security related purpose as they have well-known vulnerabilities. Instead many recommend that these days SHA-2 should be used, as it has no known exploitable vulnerabilities (apart from inept and lazy people who are using passwords that are too short and simple to stand against educated guess).

A function is a one-way cryptographic algorithm that takes a variable length input and calculates a value that is unique for the specific set of data (e.g. file or string). It is not possible to reverse given hash value to reveal what the original value was. So when applied to passwords the way to verify if the given password matches with the hashed password in the database, the given password is hashed with the same algorithm and if the two hash values are identical it means that the right password was given and use may login. For example, if the password is 'secret' the hash value (SHA-256) is '2bb80d537b1da3e38bd30361aa855686bde0eacd7162fef6a25fe97bf527a25b'. User databases get hacked all too often.

6.1 Cause of Problem

While hashing is a good way to protect a password against the eyes of unauthorised mortals, they can be vulnerable against brute force attacks. Modern computer components are simply so fast and efficient that brute force attacks

(where each and every possible combination is tried until the right combination of characters is found) have become quite reasonable option for attackers.

A modern brute force attack utilises GPU instead of more traditional CPU. Consider this: while a CPU based password recovery tool might take about a year to crack an eight-character password, a similar GPU based password recovery tool could do the same trick in less than a day. In another words, a 13-year old with a gamer's desktop computer and simple software tool could crack a list of typical hashed passwords within hours or days, if not in minutes. Now consider for a moment about what a well-resourced and determined professionals would do to passwords in the user database of your favourite web site should they gain access to it (For example, a dirt cheap ATI Radeon HD 5450 can handle about 52 million SHA1 or 126 million MD5 hash computations per second. Upgrade to ATI Radeon HD 5970 and it would be doing about 2320 million SHA1 or 5631 million MD5 calculations per second, and that is with just a single GPU. Most desktops can have two linked GPUs, including the one I have under my desk that I have dedicated just for gaming and LAN-parties.

To put things into perspective, ATI Radeon 5770 can crack a five-character password under one second while a typical CPU might be do the same in about 24 seconds or so. A six-character password would take about four seconds for 5770 to crack, and a seven-character password would be sorted in about 17 minutes. The respective times for a typical CPU would be around 90 minutes and four days, or so.

6.2 System Solution to prevent password attacks

Obviously there are no guarantees but there are ways to frustrate most attackers to a point when the reward just isn't worth the trouble. For a common user the best protection is not to use overly cryptic and hard to remember passwords with caps, numbers and special characters (e.g. #fK1~2) but simply to use longer passwords. For example, if the system is using ASCII that has 95 printable characters, each new character in the password multiplies the number of possible combinations by 95. On the other hand, if your password is just a common word then you are wide open for dictionary based attacks and guesses of people who know you. Go for the middle ground.At the same time software architects and developers should ditch the ye olde SHA-2 variants and similar algorithms and move to BCRYPT.

Bcrypt is a Blowfish variant that has one very important aspect that sets it apart from most other hash algorithms: it can be made very expensive to use in a world where cheap equals bad. Most hash algorithms have been optimised to calculate a hash value for large sets of data as fast as possible (for example, an AMD64 CPU can calculate MD5 hash for 335 MB of data in one second) which is great when one needs to find out if two large data sets are identical, but bad when dealing with common <10 character passwords, as shown earlier.

Bcrypt on the other hand is designed to be slower instead of faster when calculating the hash thus making it easy to increase the expense of brute force attack as a single hash calculation would take milliseconds (or even seconds) instead of microseconds. Combined with properly long unobvious passwords bcrypt can seriously frustrate GPU based brute force attacks while attackers relying on CPU should not even bother.

It is important to put this into proper context: it is perfectly fine for a password hashing to take about a second during registration and login as these happen fairly rarely: a typical user registers only once and might login to service few times a day whereas a hacker would need to go through as many individual passwords in as short time as possible. Another thing about using bcrypt is that it can be adapted to match Moore's Law: it has a work factor that can be freely increased as computers become faster as well as to tweak the balance between performance and security. Bcrypt is available for most programming languages and for example the Grails Spring Security Core -plugin by Burt Beckwith makes the using of bcrypt practically trivial.In addition proposed system increase encryption strength using bcrypt with fallbacks on sha-256/512 with key stretching.

7. Conclusion

This work has reached to the following conclusions

1- The three tier architecture of the proposed system plays the basic role of database security because the client does not have a direct access to the database server connect to it across the middle application server (active server) especially when using LAN network (off-line connection) between the two servers.
2- Using disable caching is more important because the stored files areloaded from the hard drive instead of being downloaded from the Internet. This is a useful feature because it makes the Web surfing much faster.
3- The Client-to-Application Server Protocol (CAP) provides data confidentiality by using the RC4A algorithm.
4- Using bcrypt to that per-password saltsmake attacked much more difficult, because it have been sure that an attack is virtually unfeasible without either ludicrous amount of funds or hardware.
5- Password encrypted using bcrypt with fallbacks on sha-256/512 with key stretching to protect it from cracking by any types of attack.

References

[1] Bhuvan U., Giovanni P., Prashant S., Mike S., and Asser T.,"An Analytical Model for MultitierInternet Servicesand Its Applications",SIGMETRICS'05, Banff, Alberta, Canada, June 2005.
[2] Mumtaz A. and Sarmad H.,"Developing a Three-Tier Web Data Management Application for Higher Education Admission Environment",International Arab Journal of e-Technology, Vol. 2, No. 4, June 2012.
[3] Wells L., Christensen S., L. Kristensen M., and Mortensen K. H., "Simulation Based Performance Analysisof Web Servers", 9th International Workshop on PetriNets and Performance Models, 2001.
[4] Doyle R., Chase J., Asad O., Jin W., and Vahdat A.,"Model-Based Resource Provisioning in a WebService Utility", presented at USITS, 2003.
[5] Te-Kai L., Santhosh K., and Jen-Yao C.," Performance Engineering of a Java-based e-Commerce System" Proceedings of the 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE'04), Taipei, Taiwan, pp.33-37, 2004.
[6] He L. and Chen Y., "Design and Implementationof Web Content Management System by J2EE- based Three-tier Architecture",2nd IEEE International Conference on Information Managementand Engineering (ICIME), Zhengzhou, China, pp.513-517, 2010.
[7] Diane C. and Sajal D., "Smart Environments: Technology, Protocols and Applications",Wiley Inc.,ISBN: 0471544485, pp. 101-127, 2004.
[8] Oracle Technology Network, http://java.sun.com/products/jsp/ JavaServer Pages.
[9] Ramesh N., Robert S., Rima P. S., "Developing Java Web Services: Architecting andDeveloping Secure Web Services Using Java",Wiley, ISBN: 0471236403, 2005.
[10] Douglas K. B., "Web Services, Service-Oriented Architectures, and Cloud Computing: The Savvy Manager's Guide",Elsevier ScienceInc, ISBN: 9780123983572.
[11] Abdullah A., Roslina S. and Abdul Rahman R.,"Hardware Implementation of RC4A Stream Cipher",International Journal of Cryptology Research 225-233, 2009.
[12] Kevin J., "What is hashing", Thycotic Software Ltd., (2007).
[13] Chi-Chaochang and Tzonelih H., "Modular Design for Round-Oriented PasswordAuthentication Protocols", Journal of Information Science and Engineering 22, 1295-1308, (2006).