A

Project Report

on

MINDMETRICS : AN APPROACH FOR UPGRADING SECURITY

Submitted in Partial Fulfillment of
the Requirements for the Degree
of

Bachelor of Engineering

in

Computer Engineering

to

North Maharashtra University, Jalgaon

Submitted by

Prajakta Yuvraj Patil
Anil Pradipkumar Chaudhari
Bhushan Ravindra Badgujar
Kuldip Anilsinh Rajput
Shraddha Vinodrao Patil

Under the Guidance of

Mr. Ashish T. Bhole

DEPARTMENT OF COMPUTER ENGINEERING
SSBT's COLLEGE OF ENGINEERING AND TECHNOLOGY,
BAMBHORI, JALGAON - 425 001 (MS)
2016 - 2017

SSBT's COLLEGE OF ENGINEERING AND TECHNOLOGY, BAMBHORI, JALGAON - 425 001 (MS)

DEPARTMENT OF COMPUTER ENGINEERING

CERTIFICATE

This is to certify that the project entitled *Mindmetrics : An approach for upgrading security*, submitted by

Prajakta Yuvraj Patil
Anil Pradipkumar Chaudhari
Bhushan Ravindra Badgujar
Kuldip Anilsinh Rajput
Shraddha Vinodrao Patil

in partial fulfillment of the degree of *Bachelor of Engineering* in *Computer Engineering* has been satisfactorily carried out under my guidance as per the requirement of North Maharashtra University, Jalgaon.

Date: October 9, 2016
Place: Jalgaon

Mr. Ashish T. Bhole
Guide

Prof. Dr. Girish K. Patnaik
Head

Prof. Dr. K. S. Wani
Principal

Acknowledgements

The project on Mindmetrics : An approach for upgrading security is standing on the pillars of contribution of many people. We would like to express our gratitude towards beloved Principal, Prof. Dr. K. S. Wani for introducing us to this research work. We would also like to thank HOD Prof. Dr. Girish K. Patnaik for encouraging us to enthusiastically accomplish this project. We would also extend our gratitude towards Guide Mr. Ashish T. Bhole for guiding us and showing the right path to successfully reach our destination. Also, We would like to thank all the faculty and staff members for extending their helping hand directly or indirectly. Last but not the least, We would also like to thank our dear parents and friends for having their blessings on us and motivating us endlessly.

Prajakta Yuvraj Patil
Anil Pradipkumar Chaudhari
Bhushan Ravindra Badgujar
Kuldip Anilsinh Rajput
Shraddha Vinodrao Patil

Contents

List of Figures

Abstract

Exposure of the password files is a critical security concern making millions of user susceptible to cyber attacks. Password hash files are stolen quite often and cracked by hacker. Password cracking attack is a statistical attack, and some of the weak passwords can be broken through a dictionary attack or a hybrid attack. After the attackers crack some passwords, they can access the system using the known login IDs for the cracked passwords. The attack against passwords is a serious threat to current systems. Many methods have been proposed to improve it but they require specialized devices or they may not be always reliable. Proposed method augments the current password based system by strengthening the identification and verification process. It utilizes personal private data instead of a login ID to identify a user uniquely, called as mindmetrics. After the several login attempts attacker will be blocked by the identification server. Thus it may stop or slow down attackers.

Chapter 1

Introduction

Introduction chapter will introduce the work, It will focusses exactly on what is the area of project and explains what is actually be done in the work. All ideas about project work are cleared here.

Chapter is of 7 sections. First section describes introductory part of the project. Background and need of the project will discuss in section 1.2. Section 1.3 presents the motivations behind the project. Scope of the project is defined in section 1.4. Section 1.5 gives objectives of the project. Organization of the whole project is given in section 1.6 .The last section gives the Summary.

1.1 Background

Computer systems employ an authentication mechanism to allow access only to legitimate users. From the perspective of most of the users, the mechanism provides a better security. The initial perception fails to take into account security as exposure of the password file is a critical security concern making millions of user susceptible to cyber attacks. Password hash files are stolen quite often and cracked by hacker. After the attackers crack some passwords, they can access the system using the known login IDs for the cracked passwords. By improving the identification part and a verification part together, the overall authentication process can be strengthened, in which utilization of the personal secret data takes place instead of login id to identify user uniquely.

1.2 Motivation

Password hash files are stolen quite often and cracked by hackers. Password cracking attack is a statistical attack, and some of the weak passwords can be broken through a dictionary attack or a hybrid attack. After the attackers crack some passwords, they can access the system using the known login IDs for the cracked passwords. The attack against passwords

is a serious threat to current authentication systems, and additional security measures are needed to mitigate the threat. Once an account is breached, the cost from the damage is high for both victims and the companies. In 2013, the average organizational cost of data breaches in US was $5.4 million and the average per capita cost was $188 in US. While passwords are supposed to be random characters, login IDs are not random. They are used for communication or accounting purposes, and must carry a meaningful pattern. It may be part of users first and/or last names, part of social security number, combination of names and numbers, account number, or email addresses. Thus login IDs are publicly known or can be guessed easily. In other words, obtaining the login ID is generally not a barrier for the attackers, and the success of an attack depends on the difficulty of the password. While a great emphasis was given to the verification, i.e. password system, somewhat less attention was given to the identification, i.e. login ID. By fortifying the identification part, the overall authentication system can be strengthened.The goal of the research is improving the security of the authentication system by supplementing it with a secure identification process.

1.3 Problem Definition

Mindmetrics is a method that augments the current password-based system by strengthening the identification and verification process. It utilizes secrete data instead of a login id to identify a user uniquely. The secret is referred as Mindmetrics token. Without the secret knowledge, the attackers cannot pass the identification stage before they can even try the password. The process of identification in mindmetrics uses something in users mind. There are two parts in the mindmetrics based method. First, mindmetrics token is requested in the login page. A user then specifies the token with which a computing system can identify a user account. Then the identification server looks up the registered access tokens to find a matching token and login id. Second, the server presents multiple login IDs to the user, with one of the login IDs being the correct login id for the user account and some more real or fake IDs. To prevent the attackers from recognizing the login IDs, the login id‘s are partially obscured. Among these partial login IDs, a legitimate user can still recognize the correct login id and choose it. That completes the identification stage, and also verification stage can be improved by encrypting the passwords of users.

1.4 Scope

The present scope of the project involves securing the authentication systems to employ an authentication mechanism that allows access only to legitimate users. The authentication mechanism identifies the user not by using the login id instead it uses mindmetrics token

for identification purpose and the password for verification purpose. If the login credentials are correct then the user gets access to the system. The framework captures application level requirements of users trust to better reflect reality. Many of the website could use that system to keep data secured.

1.5 Objective

The main objective of the proposed system is to improve the security of the authentication system by supplementing it with a secure identification process. To make false login attempts difficult, proposed method does not use a publicly known login ID for identification. Instead it uses private information known only to the computer system and the user. The process makes the stolen password files unusable for the attackers. And also prevents system form dictionary and brute force attack.

1.6 Organization of the Report

The system provide more security to client data which protect data from unauthorized access or attack. Firstly,Chapter 1 describes an Introduction. Chapter 2 describes System Analysis for gathering and interpreting facts, diagnosing problems and using the facts that improve the system. Chapter 3 describes Software Requirement Specification through the various hardware, software, functional and non-functional requirements of the system. Chapter 4 describes System Design to provide understanding and procedural details necessary for implementing the system recommended in system study. Chapter 5 describes the conclusion that integrate the various issues, research etc.and future scope for making the new changes requests considered to modify project scope.

1.7 Summary

In this chapter, introduction of project is described. In the next chapter System Analysis is described.

Chapter 2

System Analysis

System analysis is the study of states of interacting entities, including computer system analysis. The field closely related to requirement analysis or operation research. The chapter briefly discuss "System analysis" of Mindmetrics system with is's related work.

The related work and attempts are reviewed in section 2.1. The proposed system of the project is describe in section 2.2. Section 2.3 explains the different feasibility studies related to the project. All risk involved in project are given in section 2.4. Section 2.5 gives the project scheduling. Effort allocation is explained in section 2.6. Last section gives Summary.

2.1 Literature Survey

Computer systems use an authentication mechanism to allow access only to legitimate users. The authentication process is consisting of two parts, identification and verification. Identification process is used to verify who the user is? and verification process is used to verify if the user is legitimate or not. Traditionally the identification was performed by a username or login ID and the password for verification. In a password based system, the plain text passwords are transferred into hash values is generated from the newly entered password, and compared with the stored hash values in the password hash file. If the hash value matches, access is granted. The password verification process is the heart of the most authentication systems.

The Alon Schclar and Lior Rokach describes that the user authentication based on username and password is the most common means to enforce access control. It introduces a novel approach for user authentication based on the keystroke dynamics of the password entry. A classifier is tailored to each user and the novelty lies in the manner by which the training set is constructed. That concept reduces the possibility of overfitting, while allowing scalability to a high volume of users. Specifically, only the keystroke dynamics of a small subset of users, which is referenced as representatives and it is used along with the password entry keystroke dynamics of the examined user. The contribution of the approach is two fold

it and reducing the possibility of overfitting, while allowing scalability to a high volume of users. Alon Schlar and Loir Rokach propose two strategies to construct the subset for each user.The first selects the users whose keystroke profiles govern the profiles of all the users, while the second strategy chooses the users whose profiles are the most similar to the profile of the user for whom the classifier is constructed. Results are promising reaching in some cases 90% area under the curve. In many cases, a higher number of representatives deteriorate the accuracy which may imply overfitting. An extensive evaluation was performed using a dataset containing over 780 users [6].

The Bin B. Zhu and Jeff Yan focuses on Using hard AI problems for security. They presented that many security primitives are based on hard mathematical problems. Using hard AI problems for security is emerging as an exciting new paradigm, but has been under-explored. Bin B. Zhu and Jeff Yan presents a new security primitive based on hard AI problems, namely, a novel family of graphical password systems built on top of Captcha technology, which is called as Captcha as graphical passwords (CaRP). CaRP is both a Captcha and a graphical password scheme. CaRP addresses a number of security problems altogether, such as online guessing attacks, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. Notably, a CaRP password can be found only probabilistically by automatic online guessing attacks even if the password is in the search set. CaRP also offers a novel approach to address the well-known image hotspot problem in popular graphical password systems, such as PassPoints, that often leads to weak password choices. CaRP is not a panacea, but it offers reasonable security and usability and appears to fit well with some practical applications for improving online security [2].

The Mariusz Rybnik and Marek Tabedzki mainly describes that On-the-fly keyboard user authorization is certainly an interesting option for standard security procedures for high-security computer systems. Unauthorized access to logged-in workstation could threaten the security of data and systems. Conventional authorization methods (passwords, fingerprint scans) verify user identity only during logging process, leaving system vulnerable to user replacement afterwards. Procedures overcoming that peril are often invasive or uncomfortable. A possible solution for constant authorization without these drawbacks is to identify the keyboard user while typing. The ap propose method is based on two extracted keystrokes features flight and dwell. It have tested the suggested solutions on individual group resembling a medium-sized company. The obtained results are promising[7].

The Bob Zhang et al. focuses on authentication system based on Palm-Print Classification by Global Features. Three-dimensional (3-D) palm print has proved to be a significant biometrics for personal authentication. Three dimensional palm prints are harder to counterfeit than 2-D palm prints and more robust to variations in illumination and serious scrabbling

on the palm surface. Previous work on 3-D palm-print recognition has concentrated on local features such as texture and lines. Three novel global features of 3-D palm prints which describe shape information and can be used for coarse matching and indexing to improve the efficiency of palm-print recognition, particularly in very large databases. The three proposed shape features are maximum depth of palm center, horizontal cross-sectional area of different levels, and radial line length from the centroid to the boundary of 3-D palm-print horizontal cross section of different levels. These features are treated as a column vector and use orthogonal linear discriminant analysis to reduce their dimensionality. Then two schemes are adopted

1) coarse-level matching

2) ranking support vector machine to improve the efficiency of palm-print recognition.

A series of 3-D palm-print recognition experiments are conducted using an established 3-D palm-print database, and the results demonstrate that the proposed method can greatly reduce penetration rates[8].

The Joseph Bonneau et al. focuses on The Quest to Replace Passwords A Framework for Comparative Evaluation of Web Authentication Schemes. It presents that they evaluate two decades of proposals to replace text passwords for general-purpose user authentication on the web using a broad set of twenty-five usability, deployability and security benefits that an ideal scheme might provide. The scope of proposals surveyed is also extensive, including password management software, federated login protocols, graphical password schemes, cognitive authentication schemes, one-time passwords, hardware tokens, phone-aided schemes and biometrics. A comprehensive approach leads to key insights about the difficulty of replacing passwords. Not only does no known scheme come close to providing all desired benefits none even retains the full set of benefits that legacy passwords already provide. In particular, there is a wide range from schemes offering minor security benefits beyond legacy passwords, to those offering significant security benefits in return for being more costly to deploy or more difficult to use. So, it can be conclude that many academic proposals have failed to gain traction because researchers rarely consider a sufficiently wide range of real-world constraints[1].

Many schemes have been proposed to improve the whole authentication process but they may require specialized devices or they may not be always reliable.

User authentication is done in two steps, identification and verification. The traditional password-based verification system has been challenged by sophisticated attacks, but new schemes are being made to cover the weaknesses of the password-based systems. However, the identification part is still based on a public login ID. The proposed scheme called mindmetrics to strengthen the identification process with personal secret information. In

proposed systems, a login ID will not be asked instead, a user must provide the correct token to pass the identification stage. In case the password file gets stolen, the login attempts by attackers will be blocked by the identification server. Thus it may stop or slow down attackers, and account holders can change their account credentials before attackers can gain access. Mindmetrics can simulate biometrics with its high security level where true two factor authentication with biometrics is not feasible[5].

2.2 Related Work

The term Mind metrics is coined with the concept of Biometrics as it is similar to biometrics. Biometrics is a field of study which aims to identify or recognize people based on traits they have. Given these traits, a system can be trained to recognize certain people, with a certain probability. Biometrics refers to metrics related to human characteristics. Biometrics authentication is used in computer science as a form of identification and access control. Mind metrics uses some secret data instead of human characteristics as a token to identify the user. It utilizes personal secret data instead of a login ID to identify a user uniquely, hence mind metrics.

Examination between Biometrics and Mindmetrics :

- Some extraordinary equipment gadget (e.g.: thumb scanner) is required in biometrics. Then again no unique equipment is required in mindmetrics and can be effectively actualized. So mindmetrics can be utilized for getting to nearby or remote figuring frameworks from any customary private or open PCs.
- Biometrics is expensive and can't be effortlessly actualized on open e-business sites. Mindmetrics is savvy and can utilized for open e-business sites.

Mindmetrics is a deterministic procedure, and therefore there is no vulnerability. Hence mindmetrics is more user friendly, less expensive, and can be utilized by any open sites, for example, e-business sites[3].

2.3 Proposed System

The proposed system augments the current password-based system by strengthening the identification process. It utilizes personal secret data instead of a login ID to identify a user uniquely, hence mindmetrics. It then asks the user to choose a correct login ID among multiple choices of partially obscured IDs. Since it does not accept a login ID during the authentication process, a stolen or cracked password cannot be used for gaining an access to the computing system unless the attacker provides a correct identification material, i.e.,

mindmetrics token. It is the additional step which raises the security of an authentication system considerably over single or double password systems. Since the stolen passwords cannot be used immediately by the attackers, account holders can have extra time to change their passwords before the attackers gain an access. Mindmetrics scheme separates the identification server and the verification server, thus it is scalable to a large system. the proposed system is expected to work in 5 stages :

1. Token Registration
2. Token submission
3. Identification
4. Verification
5. Login

In First Stage, user will have to register first i.e user will enter all his details like Token ,Login ID , password which will be minimum 8 character long. In the second stage User will have to submit all the credentials that he have entered earlier. In that stage the user account will get created. In the third stage user needs to be identified among the number of users.In fourth stage user needs to be verified, user verification is performed on the basis of the users password. In final stage user gets logged in to the system[3].

2.4 Feasibility Study

A feasibility study is a formalized, written approach to evaluating your idea and can help you identify. The section shows the all the aspects of the project and it can be known that whether the project is practically possible to develop worth limited resources and time. The feasibility study is an evaluation and analysis of the potential of a proposed project which is based on extensive investigation and research to support the process of decision making. Feasibility studies aim to objectively and rationally uncover the strengths and weaknesses of an existing business or proposed venture, opportunities and threats present in the environment, the resources required to carry through, and ultimately the prospects for success.

2.4.1 Economical feasibility

The study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development

of the system is limited. The expenditure must be justified. Thus the developed system as well within the budget and that was achieved because most of the technologies are freely available for use. Only the customized products had to be purchased.

The project is economically feasible as it requires open source softwares meaning most of the resources required for the development of proposed system are free to use. This makes it very much feasible in accordance to economy.

2.4.2 Operational feasibility

Operational feasibility is a measure of how well a proposed system solves the problems. Operational feasibility means users should support the project.

The proposed system needs no involvement of end user. It only implements security at back end servers maintaining password hash files and uses addition server. No additional components other than these are required, thus the proposed system is operationally feasible.

2.4.3 Technical feasibility

The technical feasibility deals with the technology and the tools used to develop the system. Technical feasibility refers to the ability of the process to take advantage of the current state of the technology in pursuing further improvement.

The proposed system can be implemented using current technologies available which are also open source hence free to use. It can also be improved by the technologies thus making it technically feasible.

2.5 Risk Analysis

Risk analysis and management are a series of steps which are help a software team to understand and manage uncertainty. Many problems can plague a software project. A risk is a potential problem it might happen, it might not. But, regardless of the outcome, it's a really good idea to identify it, assess its probability of occurrence, estimate it's impact, and establish a contingency plan should be the problem actually occur. Actually Project Risk Analysis and Management is a process which enables the analysis and management of the risks associated with a project. Properly undertaken it will increase the likelihood of successful completion of a project to cost, time and performance objectives. The risk associated with the proposed system lies in the number of Login ID's generated. Another risk depends on length of token entered. Theoretically the proposed model enables 2 raise to(-n) risk factor while guessing actual Login ID from generated set of Login ID's . Practically, it is advised to generate minimum 6 Login ID per user for assuring more than 95% security;

as probability of guessing acual Login id out of 6 Login id is equal to 5%, thus secutity is 95% in this case. However, the risk cannot exceed 50% even in worst case scenario where token consists of a single character. The problems or risks that are commonly faced are listed as follows :

- **Project Risks**
  Threaten the project plan which is, if project risks become real, it is likely that project schedule will slip and the costs will increase project risks identify potential budgetary, schedule,personnel, resource,customer and requirements problems and their impact on a software project.In the project, project risk occurs if requirement of technical member means technical team is unavailable according to the project plan and estimation and if the project is not completed within time then situation project risk can occur.

- **Technical Risks**
  Threaten the quality and timeliness of the software to be produced. If a technical risk becomes a reality, implementation may become difficult or impossible. Technical risks identify potential design,implementation,interface,verification and maintenance problems. Technical risks occur because the problem is harder to solve than thought it would be. In the project if any module doesn't worked properly according to developer expectations then technical risk may occur.

2.6 Project Scheduling

Software project scheduling is an activity that distributes estimated effort across the planned project duration by allocating the effort to specific software engineering tasks. It is important to note that the schedule evolves over time. During early stages of project planning, a macroscopic schedule is developed. That type of schedule identifies all major software engineering activities and the product functions to which they are applied. As the project gets under way, each entry on the macroscopic schedule is refined into a detailed schedule. Here, specific software tasks required to accomplish an activity are identified and scheduled. Scheduling for software engineering projects can be viewed from two rather different perspectives. In the first, an end-date for release of a computer based system has already and irrevocably been established. The software organization is constrained to distribute effort within the prescribed time frame. The second view of software scheduling assumes

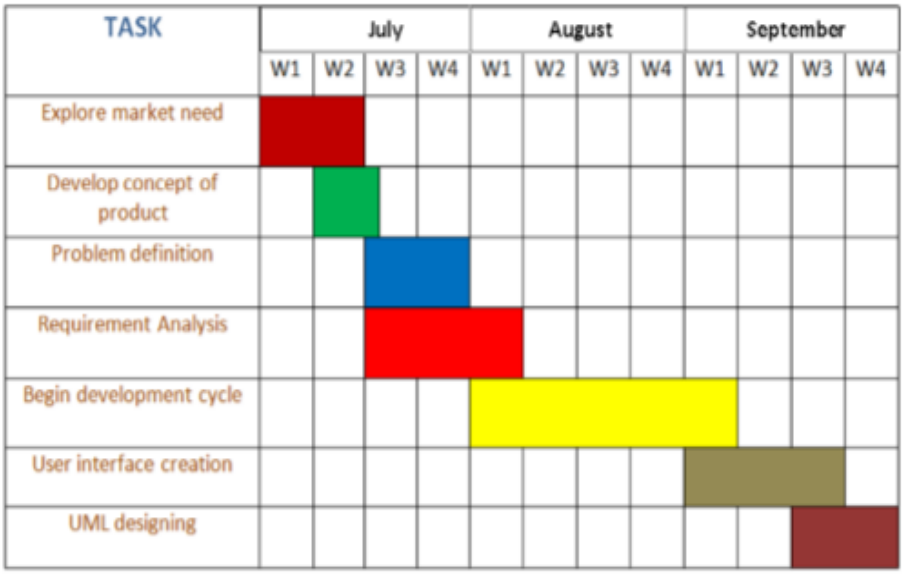

Figure 2.1: Gantt chart

that rough chronological bounds have been discussed but that the end-date is set by the software engineering organization. Effort is distributed to make best use of resources and an end-date is defined after careful analysis of the software. Unfortunately, the first situation is encountered far more frequently.

2.7 Effort Allocation

Project means team work; Project is developed by combination of effort of team. So whole project is divided into modules and number of modules is allotted to team members. After completion of each module, it will be link from one module to another module to form a complete project. That effort allocation should be used as a guideline only. The characteristics of each project must dictate the distribution of effort. Work expended on project planning rarely accounts for more than 23 percent of effort, unless the plan commits an organization to large expenditures with high risk. Requirements analysis may comprise 10 to 25 percent of project effort. Effort expended on analysis or prototyping should increase in direct proportion with project size and complexity. A range of 20 to 25 percent of effort is normally applied to software design. Time expended for design review and subsequent iteration must also be considered.

Activity	Prajakta	Bhushan	Anil	Shraddha	Kuldipsinh
Project Planning	25%	19%	20%	18%	18%
Requirement Gathering	20%	20%	19%	21%	20%
Design	22%	21%	21%	20%	15%

Table 2.1: Effort Allocation

2.8 Summary

In this chapter system analysis of project is described briefly. In the next chapter system requirement specification is described.

Chapter 3

System Requirement Specification

System requirement Specification is the official statement of what is required of the system developers. It include both user requirements and a detailed specification of the system requirements. Requirement analysis is done in order to understand the problem the software system is to solve.

The chapter focuses on the various requirements of the system. Section 3.1 describes the hardware requirements of the system. The software requirements of the system are discussed in section 3.2. Section 3.3 describes the functional requirements of the system. Non-functional requirement of system are discussed in 3.4. Section 3.5 describes other requirements and constraints of system. Finally the last section is of summary.

3.1 Hardware Requirements

The hardware requirement includes a system with following configurations:

- Processor : Pentium IV and above.
- Display Type : VGA and above.
- Memory(RAM) : 256MB.
- Storage Memory :1GB.

3.2 Software Requirements

The various software requirements of the system are summarized as below:

- Operating system : Windows 7/8.
- System Type : 64-bit/32-bit operating system.
- Front end : Java.

- Java version : Jdk1.6.0
- Back end :mysql.
- Web server : Apache Tomcat 6.0

3.3 Functional Requirements

Requirement Analysis is dependent on three aspects (Data, Function and Behavior).Requirement Analysis of data is a process of inspecting, cleaning, transforming, and modeling data with the goal of highlighting useful information, suggesting conclusions, and supporting decision making. Data analysis has multiple facts and approaches, encompassing diverse techniques under a variety of names, in different business, science, and social science domains. Requirement Analysis of function is providing services to user as they expect in the sense of Java Integrated Environment. Function Analysis is one of important aspect of any project to determine project efficiency, integrity, user friendliness etc.

3.4 Non-Functional Requirements

In Non-functional requirements of the project implements those functions which does not effect on function and behavior of project for desired goal and objective of project. Non-functional requirement just provides user friendliness and notifications that are not most necessary for the project.

3.5 Other Requirement and Constraints

It defines performance and design requirements.

- Simple look and feel.
- Allow only the authorized user to interact with the data.
- Fast response time.
- Security to user accounts.
- Easy enhancement.

3.6 Summary

In this chapter, System Requirement Specification is provided. In the next chapter, Design of the project is presented.

Chapter 4

System Design

Design is an activity concerned with making major decisions, often of a structural nature. It shares with programming a concern for abstracting information representation and processing sequences, but the level of detail is quite different at the extremes. Design builds coherent, well planned representations of programs that concentrate on the interrelationships of parts at the higher level and the logical operations involved at the lower levels. Software design is the first of the three technical activities-designs, Coding and test which are required to build and verify the software.

In this chapter Section 4.1 describes the system architecture of the proposed system. E-R Diagrams are discussed in section 4.2. Section 4.3 describes the database design of the project. Data flow diagrams are discussed in section 4.4. The UML diagrams are discussed in section 4.5. Finally, the last section is of summary.

4.1 System Architecture

Fig 4.1 shows a schematic view of the architecture of entire system. The architecture consist of two server first is identification server and second is verification server. Both of these performs authentication process by dividing it in two parts i.e Identification and verification. As mentioned earlier there are two parts in the mindmetrics based authentication process.

- Firstly, Mindmetrics token is requested in the login page. A user specifies the token with which a computing system can identify a user account. Then the identification server looks up the registered access tokens to find a matching token and login ID.
- Secondly, the server presents multiple login IDs to the user, with one of the login IDs being the correct login ID for the user account and some more real or fake IDs. To prevent the attackers from recognizing the login IDs, the login IDs are partially obscured. Among these partial login IDs, a legitimate user can still recognize the correct login ID and choose it.

- Lastly, the given password will be encrypted and is compared with the already stored encrypted version of password. If match is found then and then only user will be allowed to access web server.

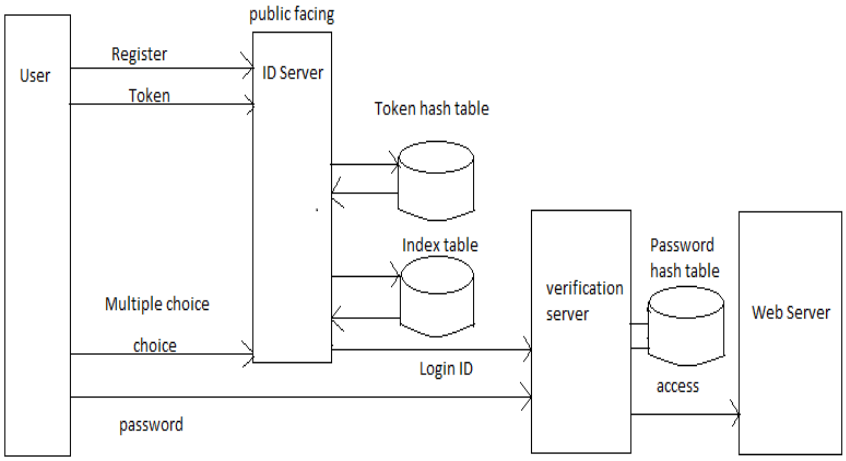

Figure 4.1: Mindmetrics system architecture

4.2 E-R Diagram

In software engineering, an entity relationship model (ER model) is a data model for describing the data or information aspects of a business domain or its process requirements, in an abstract way that lends itself to ultimately being implemented in a database such as a relational database. The main components of ER models are entities (things) and the relationships that can exist among them.

Entity-relationship modeling was developed by Peter Chen and published in a 1976 paper. Variants of the idea existed previously, and have been devised subsequently such as super type and subtype data entities and commonality relationships. ER diagram shows the relationship between various entities involved in the system. Fig 4.2 shows Entity relationship diagram for mindmetrics.

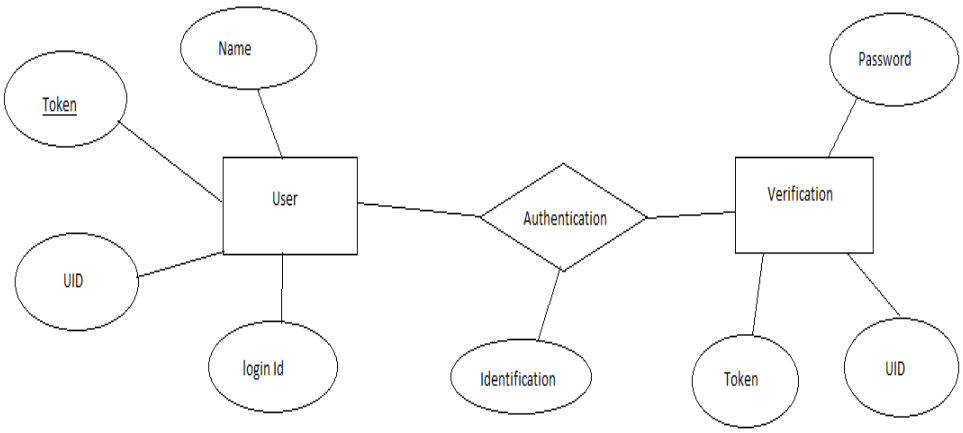

Figure 4.2: E-R Diagram for Mindmetrics System

4.3 Data Flow Diagram

A DFD is a graphical technique that depicts the information flow and the transformation that have been applied as the data moves from input to output. The data flow diagram also known as data flow graph or bubble chart. A data flow diagram may be used to represent a system or software at any level of abstraction.

The data flow diagram can be completed using only four simple notations i.e. special symbols or icons and the annotation that with a special system. Named circles show the processes in DFD or named arrows entering or leaving the bubbles represent bubbles and data flow. A rectangle represents a source or sink and is not originate or consumer of data. Data flow diagrams are the basic building blocks that define the flow of data in a system to the particular destination and difference in the flow when any transformation happens. It makes whole procedure like a good document and makes simpler and easy to understand for both programmers and non-programmers by dividing into the sub process. The data ow diagram serves two purposes:

- To provide an indication of how data are transform as the moves through the system.
- To depict the function that transforms the data flow.

A level 0 DFD, also called a fundamental system model (FSM) or a context model. It represents the entire software elements as a single bubble with input and output data indicated by incoming and outgoing arrows respectively. Figure 4.3 shows the Level 0 DFD of the proposed system.

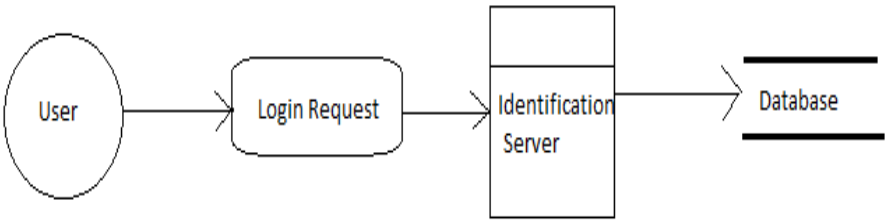

Figure 4.3: Level 0 Data Flow Diagram

Level 1 DFD contains additional processes and information ow paths, as the level 0 DFD is partitioned to reveal more detail. Level 1 DFD might contain 5 - 6 bubbles with interconnecting arrows.Figure 4.4 shows the Level 1 DFD of the proposed system.

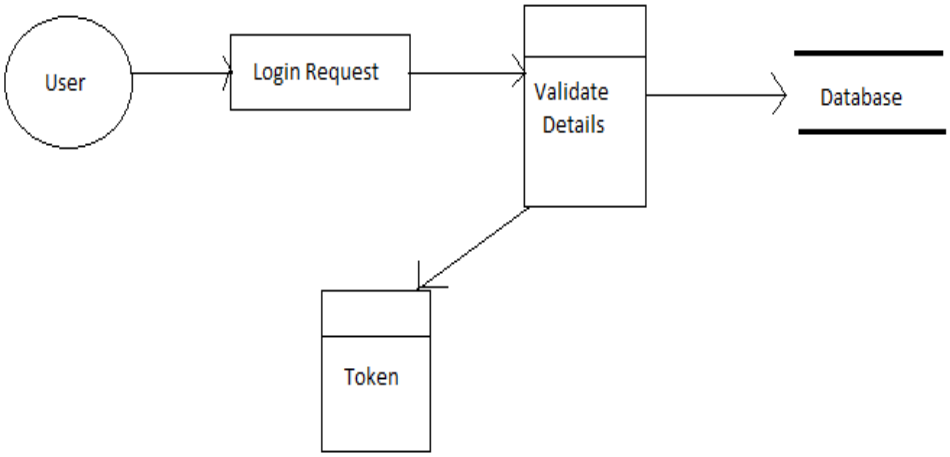

Figure 4.4: Level 1 Data Flow Diagram

4.4 Interface Design

The interface design describes how the software communicates within itself, with systems that inter operate with it, and with humans who use it. An interface implies a flow of information (e.g., data and control) and a specific type of behavior. Therefore, data and control flow diagrams provide much of the information required for interface design.

4.4.1 User Interface design

The overall process for designing a user interface begins with the creation of differen models of system function (as perceived from the outside). The human- and computer-oriented tasks

that are required to achieve system function are then delineated; design issues that apply to all interface designs are considered; tools are used to prototype and ultimately implement the design model; and the result is evaluated for quality.

4.5 UML Diagrams

The UML is a language for Visualizing, Specifying, Constructing, documenting a software intensive system. Visualizing refers to structures which are transient can be represented using the UML. Specifying addresses the specification of all the important analysis, design and implementation decisions that must be made in developing and deploying a software intensive system. Constructing the UML is not a visual programming language, but its models can be directly connected to a variety of programming languages. Documenting addresses the documentation of a system's architecture and all of its details.

4.5.1 Usecase Diagram

A Use case diagram shows a set of use cases and actors and their relationships.

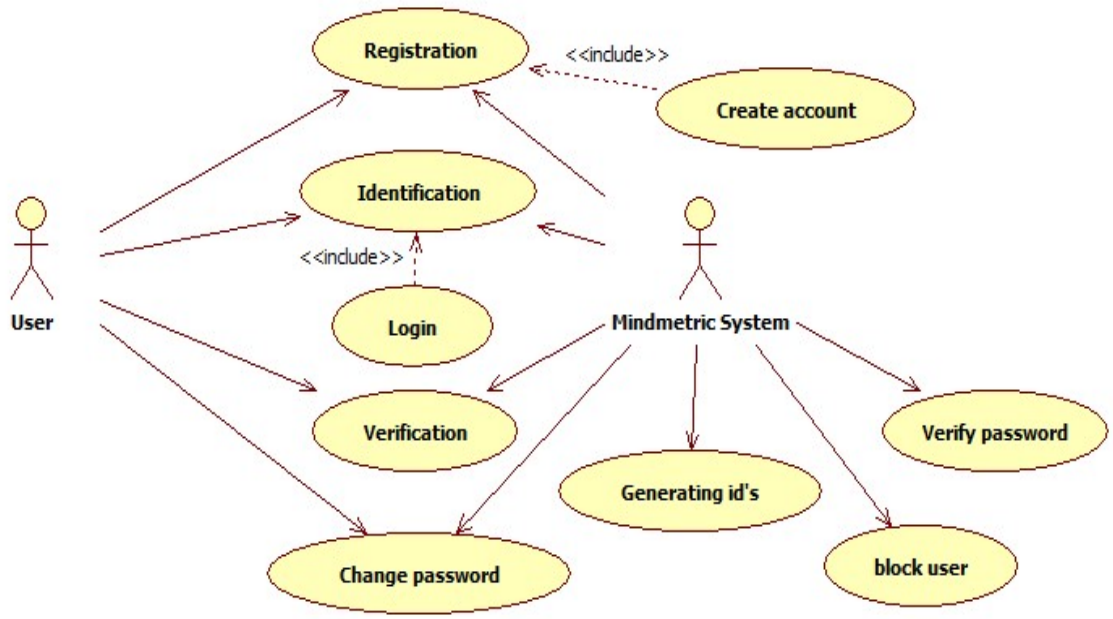

Figure 4.5: Usecase Diagram for Mindmetrics : An approach for upgrading security

Use case diagrams address the static use case view of a system. These diagrams are especially important in organizing and modeling the behaviors of a system. The Use Case diagram of the proposed system is shown in Figure 4.5.

4.5.2 Class Diagram

A Class diagram shows a set of classes, interfaces and collaborations and their relationships. These diagrams are the most common diagram found in modeling object-oriented systems. Class diagram address the static design view of a system. Figure 4.6 shows the class diagram for the proposed system.

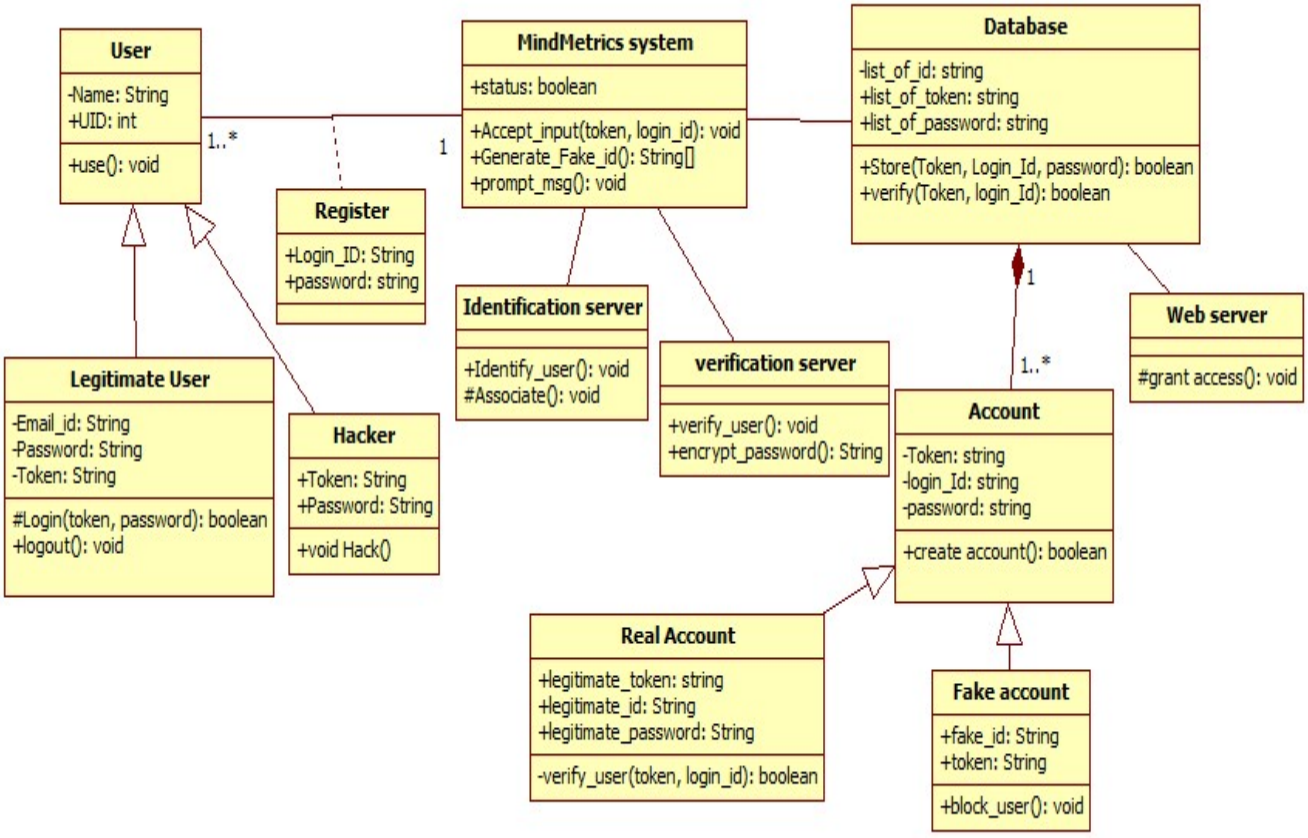

Figure 4.6: Class Diagram for Mindmetrics : An approach for upgrading security

4.5.3 Sequence Diagram

Both sequence and collaboration diagrams are kinds of interaction diagrams. An interaction diagram shows an interaction, consisting of a set of objects and their relationships. They address the dynamic view of a system. Figure 4.7 and 4.8 shows the sequence diagram for the proposed system.

- A sequence diagram is an interaction diagram that emphasizes the time-ordering of messages.
- A collaboration diagram is an interaction diagram that emphasizes the structural organization of the objects that send and receive massages. Sequence diagram and collaboration diagrams are isomorphic i.e one can be transformed into other.

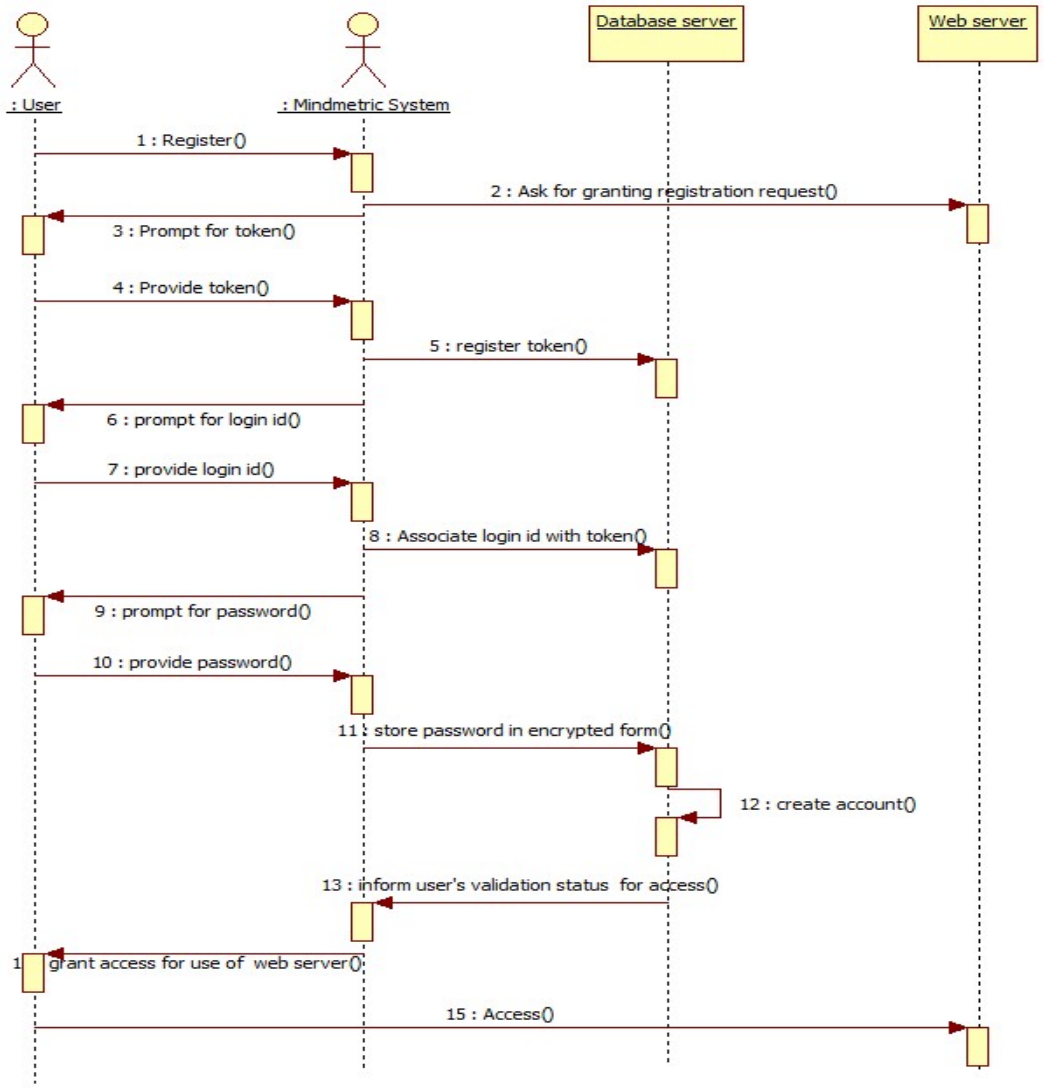

Figure 4.7: Sequence Diagram for create account Usecase of Mindmetrics : An approach for upgrading security

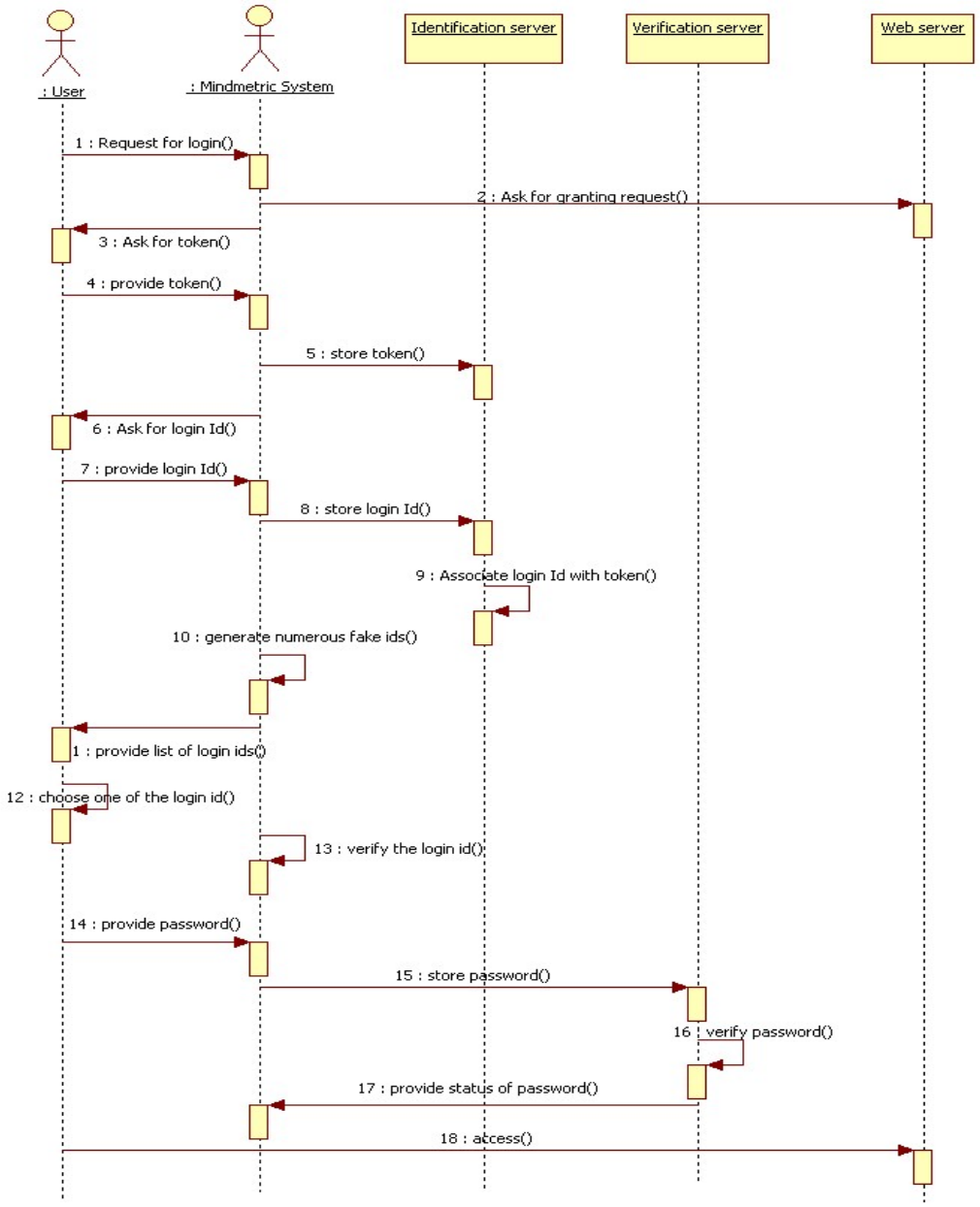

Figure 4.8: Sequence diagram for verification Usecase of Mindmetrics : An approach for upgrading security

4.5.4 Component Diagram

A component diagram shows the organization and dependencies among a set of components. Component diagrams address the static implementation view of a system. They are related to class diagram in that a component maps to one or more classes, interfaces or collaborations.The component diagram for the proposed system is shown in Figure 4.9.

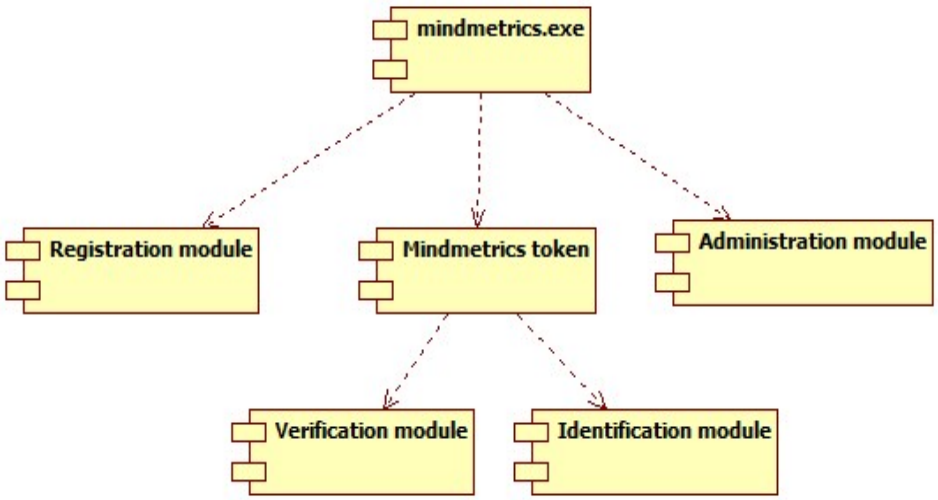

Figure 4.9: Component Diagram for Mindmetrics : An approach for upgrading security

4.5.5 Deployment Diagram

A deployment diagram shows the configuration of run-time processing nodes and the components that live on them. Deployment diagram address the static deployment view of an architecture. Figure 4.10 shows the deployment diagram for the proposed system.

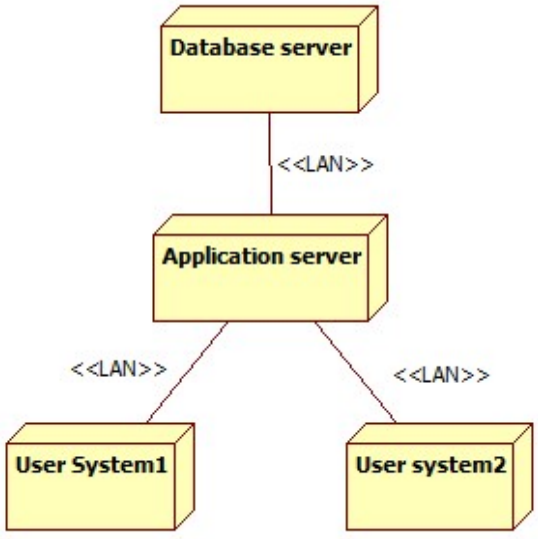

Figure 4.10: Deployment Diagram for Mindmetrics : An approach for upgrading security

4.5.6 State chart Diagram

A state chart diagram shows a state machine, consisting of states, transitions, events activities. State chart diagram addresses the dynamic view of system. It is especially important in

modeling behaviour of an interface, class or collaboration and emphasize the event ordered behaviour of a object which is especially useful in modeling reactive systems. Figure 4.11 shows the state chart diagram for the proposed system.

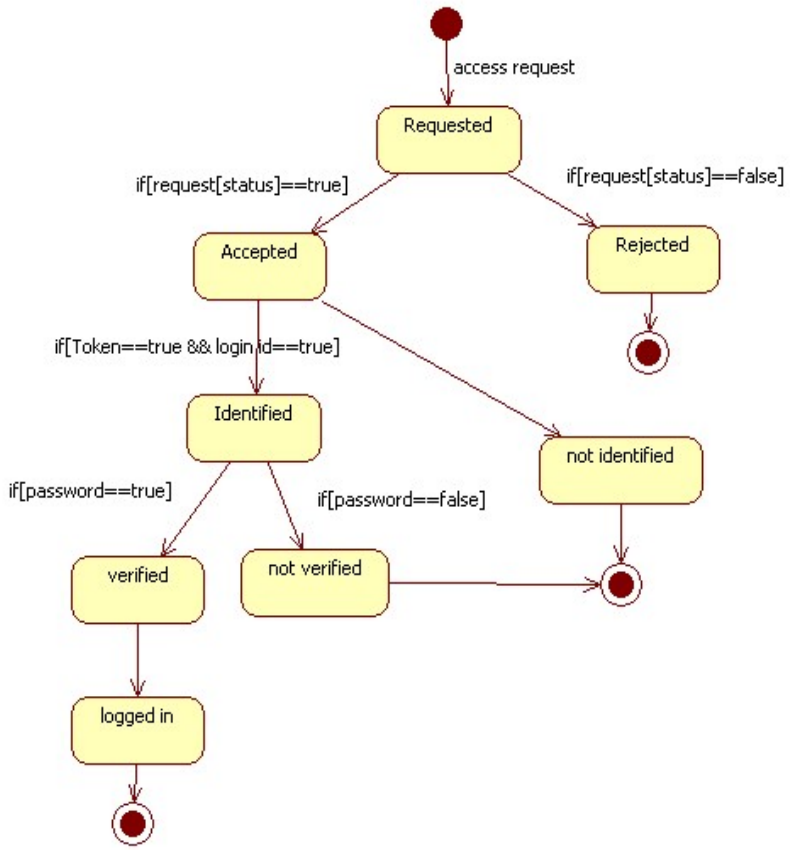

Figure 4.11: State Chart Diagram for Mindmetrics : An approach for upgrading security

4.6 Summary

In this chapter, System design is described. In the next chapter conclusion is presented.

Chapter 5

Conclusion

The proposed system overcomes all the drawbacks of conventional password based system. A new concept called mindmetrics is used to strengthen the identification process with the personal secret information. Mindmetrics is more advantageous than biometrics as it does not require any hardware device and is cost effective. System makes false login attempts difficult and increase in login attempts by attackers is blocked by identification server. The user is not allowed to enter the verification phase till it clears the identification phase. The proposed system makes use of symmetric protocol for two-server password authentication and key exchange. The proposed system is very efficient as compared to the traditional authentication protocols implemented on single server.

Bibliography

[1] Joseph Bonneau, cormac Herley, Paul C van Oorschot, and Frank Stajano, The Quest to Replace Passwords : A Framework for Comparative Evaluation of Web Authentication Schemes, 2012 IEEE Symposium on Security and Privacy, Vol. 7, pp. 553 - 567

[2] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu,"Captcha as Graphical PasswordsA New Security Primitive Based on Hard AI Problems, IEEE Transactions on Information Forensics And Security, Vol. 9, No. 6, June 2014, pp. 891 - 904

[3] Emmanouil Georgakakis, Nikos Komninos, Christos Douligeris, NAVI: Novel Authentication with Visual Information, IEEE Symposium on Computers and Communications, 2012 , pp. 588 - 595

[4] Juyeon Jo, Yoohwan Kim, and Sungchul Lee, Mind metrics: Identifying users without their login IDs, IEEE International Conference on Systems, Man, and Cybernetics, 23-October -2015, vol. 5-8, PP. 448-161.

[5] M. Alzomai, A. Jsang, A. McCullagh, E. Foo, Strengthening SMSBased Authentication through Usability, International Symp on Parallel and Distributed Processing with Applications, 2008, pp. 683 - 688

[6] Alon Schclar, Lior Rokach, Adi Abramson, and Yuval Elovici, User Authentication Based on Representative Users, IEEE Transactions On Systems, Man, And CyberneticsPart C: Applications And Reviews, Vol. 42, No. 6, November 2012, pp. 1669 1678

[7] Mariusz Rybnik, Marek Tabedzki, and Khalid Saeed, A Key stroke dynamics based system for user identification, 7th Computer Information Systems and Industrial management Applications, 2008 pp. 225 230

[8] Bob Zhang, Wei Li, Pei Qing, and David Zhang, Palm-Print Classification by Global Features, Ieee Transactions On Systems, Man, And Cybernetics: Systems, Vol. 43, No. 2, March 2013, pp. 370 378