Open password system with press time and inner time

Gaddam S Sai Veena\textsuperscript{1}, Tadepalli Sivani\textsuperscript{2}, Sravani Bandi\textsuperscript{3}, Nisha Gajjala\textsuperscript{4} Vemula Sharanya \textsuperscript{5}

\textbf{Author1:} Gaddam S Sai Veena, Department of Information Technology, Bhoj Reddy engineering college, Hyderabad, Andhra pradesh, India. Pursuing B.TECH fourth year.

\textbf{Author2:} Tadepalli Sivani, , Department of electronics and instrumentation engineering, CVR college of engineering,Ibrahimpatnam, Andhra pradesh,India. Pursuing B.TECH fourth year.

\textbf{Author3:} Sravani Bandi, Department of Information Technology, Bhoj Reddy engineering college, Hyderabad, Andhra pradesh, India. Pursuing B.TECH fourth year.

\textbf{Author4:} Nisha Gajjala, Department of computer science engineering, ACE engineering college, Hyderabad, Andhra pradesh, India. Pursuing B.TECH fourth year.

\textbf{Author5:} Vemula Sharanya , Department of Information Technology, Bhoj Reddy engineering college, Hyderabad, Andhra pradesh, India. Pursuing B.TECH fourth year

\textbf{Abstract}

The deficiencies of traditional password-based access systems have become more acute as these systems have grown in size and scope. Researchers are actively investigating ways to improve the security of password systems or offer replacements. One category of improvements uses keystroke biometrics, an approach which seeks to identify an individual by their typing characteristics. Since 1980, a number of techniques have been proposed for accurately harnessing keystroke dynamics for system authentication and other novel uses. But do these systems deliver on their promise to increase system security and simultaneously ease the burden of logging into systems and remembering passwords? And do databases of users’ keystroke profiles present additional privacy concerns?

The keystroke bio metrics is used with the application in news reporting system. It will detect the person who send the news is the reporter or some other person who hacked the user name and password of the system. First the pattern of the reporter is stored with the server system. Server after receiving the text then it matches with the text pattern information in it. The main purpose of the system is to develop a secure, cheap and effective security system for securing the computer applications and data based on typing biometrics called typing patterns.

\textbf{Scope of the System}

The scope of the system includes developing an application that can detect the user not only based on the password but also based on the typing biometrics by the typing patterns. The scope includes the following implementations.

- To develop data collector module which access the data from DBMS
- To develop cryptography module which can encrypt the password
- To develop password check module which can check the password entered
- To develop key stroke recognition module which calculate time between keystrokes.
- To develop pattern matching module which checks the patterns which matches the existing patterns with the current one for authentication.
- To develop decision module which can grant the permission.

\textbf{Current System}

The traditional way to authenticate the user to access the computer systems is password based authentication. Many cases noted based on the stealing passwords and information theft leads to huge losses. In this way the user will have two things with him the username every one knows it and the password which the user only knows. The user will logs into the system by using the user name and the secret password.

\textbf{Proposed System}

The proposed system will be efficient, low cost, scalable security system based on typing bio metrics. It uses the Artificially Intelligent neural networks to identify the persons. After the decision making is completed it will authorize the user.
1. Introduction

The main purpose of the system is to develop a secure, cheap & effective security system for securing the computer applications and data based on typing biometrics called typing patterns. If users are extra paranoid about security it's tough to go wrong with an open-source solution knowing that user (or the concerned community) can pore over the code. KeePass is open-source, free, and available for everything from a portable Windows installation to an implementation for iPhones, PocketPCs, and Android phones. KeePass supports a variety of features including automatic password generation, field and icon customization, secure notes, and login and password entry through clipboard copying, drag and drop, or auto fill-in. KeePass supports a wide range of import and export formats as well as printing for hard copy backup or secure offline storage LastPass is one of the newest password managers on the market but it has quickly gained a following for ease of use, hiccups-free integration across operating systems, browsers, and mobile platforms, and an extremely reasonable premium-model that costs only a $1 a month. Because LastPass is available for every major operating system and phone platform it's difficult to imagine a combination of operating system, web browser, and phone it doesn't cover, meaning you'll use your password manager more. LastPass has gone to extraordinary lengths to cover the bases when it comes to running a web-connected password management service including the ability to use two-layer authentication and setting up one-time use passwords for those times you want to access your online password database but you're not sure if the connection you're on is really secure.

SplashID is a multi-platform password manager. Available on the desktop for Windows and Mac OS X it also syncs to mobile versions on the iPhone, Android, Blackberry, Palm OS, Windows Mobile, and S60 platforms. SplashID uses AES and Blowfish encryption, an automatic password generator, custom icons for entries in your keyring, advanced search, and the ability to sync and securely email your passwords to other SplashID users. SplashID supports heavily customizable entry fields so you can easily make specialized entry types for storage of non-password data (confidential records, bank information, insurance information, and more). SplashID offers a 30 day trial.

1Password is a Mac-centric password manager with support for syncing to your iPhone and iPad through the 1Password mobile suite. Not only can you organize and sync passwords, but also software licenses and files—great for storing things like scanned copies of your important documents when traveling. 1Password supports customization of login icons and thumbnails, integration with Evernote and Safari, and a tag-based system for easy login organization. While this is completely irrelevant to the quality of a good password manager insofar as the security of the passwords is concerned, it's worth noting that 1Password sports the most attractive and polished user interface of any password manager we've reviewed.

To develop the proposed paper the technologies which are required are JAVA, JSP, Servlets.

In this project the existing system is manually carried out. In the proposed system java version 1.7 technology is used. The advantages of using java for a web application are

- Secured
- Robust
- Platform independent
- Portable
- Architecture neutral
- High performance
- Distributed
- Multi threaded.

J2SE-Java Platform, Standard Edition or Java SE is a widely used platform for development and deployment of portable applications for desktop and server environments. Java SE uses object-oriented Java programming language.

For designing the front end HTML (hypertext markup language) and CSS (cascading style sheet) are most commonly used. HTML elements form the building blocks of all websites because HTML allows images and objects to be embedded and can be used to create interactive forms. It provides a means to create structured documents by denoting structural semantics for text such as headings, paragraphs, lists, links, quotes and other items. It can embed scripts written in languages such as JavaScript which affect the behavior of HTML web pages. Web browsers can also refer to Cascading Style Sheets (CSS) to define the appearance and layout of text and other material. The W3C, maintainer of both the HTML and the CSS standards, encourages the use of CSS over explicit presentational HTML markup.

We use java server pages and servlets for the following reasons

SERVLETS-A servlet is a Java programming language class used to extend the capabilities of a server. Although servlets can respond to any types of requests. They are commonly used to extend the applications hosted by web servers, so they can be thought of as Java Applets that run on servers instead of in web browsers.
JSP- Java Server Pages (JSP) is a server-side programming technology that enables the creation of dynamic, platform-independent method for building Web-based applications. JSP have access to the entire family of Java APIs, including the JDBC API to access enterprise databases. For running servlets and jsp we use apache tomcat server:

APACHE TOMCAT- Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation (ASF). Tomcat implements the Java Servlet and the JavaServer Pages (JSP) specifications from Sun Microsystems, and provides a “pure Java” HTTP web server environment for Java code to run in. For establishing a communication between the front end and the back end we use jdbc.

JDBC- JDBC is a Java-based data access technology (Java Standard Edition platform) from Oracle Corporation. This technology is an API for the Java programming language that defines how a client may access a database. It provides methods for querying and updating data in a database. JDBC is oriented towards relational databases and now to store the information collected we use oracle database:

AJAX- Ajax pages can asynchronously (the A in Ajax) ask the Web server for data with the user unaware that there is a transaction occurring in the background. When the data comes back, just a portion of the page is updated

2.1 Functional Requirements
The functional requirements of the proposed system include:
- Authentication of the user based on the typing pattern
- Creation of the matrix structure for r10
- Encrypt the password
- Store the encrypted password in the database
- Verify the user password.
- Create the typing patterns of new user
- Learning the patterns from the user input
- Authenticate the user by the Decision Making logic

2.1.1 Authentication of user based on the typing pattern:
2.1.1.1 Process Flow
For the first time during registration, there will be two text fields one is the email id and other is the password. Press time is the time taken for pressing the key and inner time is the time gap between pressing the key and releasing the key.

2.1.2 Creation of matrix structure for r10:
2.1.2.1 Process Flow
For the email id, security is not required as it will be open. So, for providing security to the password the password must be entered for ten times

2.1.3 Encrypting the password:
2.1.3.1 Process Flow
After entering the password for ten times, the press time and inner time for each key in the password is calculated

2.1.4 Storing the encrypted password in the database:
2.1.4.1 Process Flow
The calculated press time and inner time of password are stored in database

2.1.5 Verifying the user password:
2.1.5.1 Process Flow
verification of password is done by checking it with the actual password given in registration.

2.1.6 Creating the typing patterns of new user:
2.1.6.1 Process Flow
During login, the press time and inner time is checked with the press time and inner time which are already stored in the database during registration

2.1.7 Authentication of user by the Decision Making logic:
2.1.7.1 Process Flow
After getting the complete data about password, press time and inner time, if all the three are matched then it will be logged in else it will be blocked

2.2 Tools/Technology Requirements:
- JDK 1.6 Enterprise Edition (J2EE)
2.3 Hardware Requirements

- Processor: Pentium 4 or More
- RAM: Minimum 1GB
- Hard Disk: Minimum 30GB
- Basic Input and Output Devices: Keyboard, Monitor

2.4 Network/Deployment Requirements

- The system in to which this application is to be deployed should satisfy the following criteria:
  - It should be installed with java jdk 1.6, MySql, apache tomcat 7.
  - The processor should be of p4 or above and RAM of 1 GB or above and Hard disc of 30GB or above.

2.5 Performance Requirements

- Time saving.
- High throughput.

Technical Architecture

3. Software Analysis

UML DIAGRAMS

Design is a process which begins with the identification and analysis of a problem or need and proceeds through a structured sequence in which information is researched and ideas explored and evaluated until the optimum solution to the problem or need is devised.

3.1 Use Case Diagram

Use case diagrams display the relationship among actors and use case. A use case diagram is a set of scenarios that describing an interaction between a user and a system.

The two main components of the use case diagrams are use cases and actors.

An actor is represents a user or another system that will interact with the system your modeling. A use case is an external view of the system that represents some action the user might perform in order to complete a task. They are helpful in exposing requirements and planning the project.
Activity Diagram
Activity diagrams display a special state diagram where most of states are action states and most of the transitions are triggered by completion of the actions in the source states. This diagram focuses on flows driven by internal processing.

Class Diagram:
Class diagrams are backbone of object-oriented modeling. Class diagram shows static design view of the system. These diagrams are built with structural things like Classes, Interfaces and collaboration relationships between them.

Sequence Diagram:
Sequence diagrams display the time sequence of the objects participating in the interaction. This consists of the vertical dimension and horizontal dimension. A sequence diagram in Unified Modelling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart.
A sequence diagram shows, as parallel vertical lines (lifelines), different processes or objects that live simultaneously, and, as horizontal arrows, the messages exchanged between them, in the order in which they occur. This allows the specification of simple run time scenarios in a graphical manner.
Database Design-ER Diagram
An ER model is an abstract way to describe a database. Describing a database usually starts with a relational database, which stores data in tables. Some of the data in these tables point to data in other tables - for instance, your entry in the database could point to several entries for each of the phone numbers that are yours. The ER model would say that you are an entity, and each phone number is an entity, and the relationship between you and the phone numbers is 'has a phone number'. Diagrams created to design these entities and relationships are called entity–relationship diagrams or ER diagrams.

![ER Diagram]

4. Results and Discussion:
The proposed system includes developing an application that can detect the user not only based on the password but also based on the typing biometrics by the typing patterns and includes the implementations like to develop data collector module which access the data from DBMS , to develop cryptography module which can encrypt the password, to develop password check module which can check the password entered, to develop key stroke recognition module which calculate time between keystrokes, to develop pattern matching module which checks the patterns which matches the existing patterns with the current one for authentication, to develop decision module which can grant the permission.

5. Summary:
Here we are implementing a technique for providing a security for passwords. Even though user miss his password, the account must be secure. We had implemented a new technique to identify the user by the typing speed recognition. Here we are calculating press time and inner time values to give the authentication to the user. We implemented this concept basing on text speed pattern recognition.

References:

Book References:
[1] JAVA Complete Reference
[4] JAVA2 Networking by Pistoria
[5] JAVA Server pages by Nick Todd
[6] HTML Black Book by Holzner
[8] Software Engineering by Roger Pressman

Authors
Author1: Gaddam S Sai Veena, Department of Information Technology, Bhoj Reddy engineering college, Hyderabad, Andhra pradesh, India. Pursuing B.TECH fourth year.
Author2: Tadepalli Sivani, , Department of electronics and instrumentation engineering, CVR college of engineering, Ibrahimpatnam, Andhra pradesh, India. Pursuing B.TECH fourth year.
Author3: Sravani Bandi, Department of Information Technology, Bhoj Reddy engineering college, Hyderabad, Andhra pradesh, India. Pursuing B.TECH fourth year.
Author4: Nisha Gajjala, Department of computer science engineering, ACE engineering college, Hyderabad, Andhra pradesh, India. Pursuing B.TECH fourth year.
Author5: Vemula Sharanya, Department of Information Technology, Bhoj Reddy engineering college, Hyderabad, Andhra pradesh, India. Pursuing B.TECH fourth year.