A TWO FACTOR AUTHENTICATION PROTECTIVE SYSTEM FOR MANAGING USER LOGIN CREDENTIALS

Ekundayo H. A., *Aminu E. F. and Alabelewe O. R.
Department of Computer Science, Federal University of Technology, Minna, Niger State, Nigeria

*Email of Corresponding Author: *enesifa@futminna.edu.ng*

ABSTRACT
Password managers are critical software programs that users rely on to store precious and sensitive data from passport and safety numbers to banking passwords in a protective and secure manner. However, it is always practically difficult for user to save or memorize numerous numbers of login credentials available for various web services. Password managers address both protection and usability issues by eliminating users ' need to study and memorize big amounts of data for various numbers of services and applications of web. To achieve this proposed system in this paper, we implore a two-factor authentication along with advanced encryption scheme as methodology. Therefore, this paper aims to design a protective system by considering biometric and encrypted strong passcode to manage various user login credentials. In the end, the proposed system incorporates the storage on a server of password encryptions. Similarly, security and trust are attained through both customer-side encryption and decryption. Also, in this paper, we tackle the problem of countering dictionary attacks by further enhancing the schema. Therefore, the proposed system has the capacity to eliminate users' stress and difficulties of recalling login credentials of numerous web services at any point of use.

Keywords: Password manger, encryption, decryption, two-factor authentication, dictionary attack.

1.0 INTRODUCTION

Based on research owing to the geometric growing of data at every given time on web, internet-based password authentication is evidently no longer secure. Internet, coined from the word International Network, is a set of computer networks that communicate using the Internet Protocol (IP). According to Norris, *et al.* (2001), Internet is a global network that uses the Internet protocol to interact. When the number of services offered on the internet has continued to rise tremendously, the number of passwords a typical user is required to remember correspondingly increases, to the point where it is no longer possible for most people to remember a new, complex password, for each and every account. Typical users fix the password difficulty by either jotting down the password in their note somewhere or reusing the same password across all accounts. Unfortunately, both methods can trigger vulnerabilities in the password.

The concept of using passwords for user authentication on the internet is cost-effective for services and easily comprehensible for users. However, the key challenge for user is being able to choose a strong password for each service and never reuse it for another service. This is important for the security, but the wide usage of passwords on the internet makes it impossible for users to memorize the required amount of different strong passwords (Liou & Bhashyam, 2010). To diminish this conflict of having user-friendly and secure passwords on possible solution of storing some data locally on the user's device, which can be the passwords themselves or information to compute them.

Being the first effective form of computer-based authentication, passwords are increasingly becoming a security problem in the modern age. There are an increasingly number of websites emerging on the internet, each demanding its own username and password. A recent study reveals that internet users, on average, have about 25 accounts that require password protection (Conklin *et al.*, 2004).

The behavioural liability of choosing protective, alphanumeric passwords across all locations that rely heavily on password authentication is a major problem with password verification. A large body of reliable research gabs suggests users have potentially, sensibly given up, choosing simple passwords and reusing them across sites (Harley., 2009). Password managers are aimed at providing a way out of this unrelated scenario. A safe password manager could create and store passwords for customers automatically, distancing oneself from the cognitive burden of having to remember them.

A password Manager is one of the best ways to keep track of each unique password or passphrase that you have created for your various online accounts (e.g. Facebook account, Twitter account, Instagram account, Research Gate account, and other important account login credentials) without writing them down on a piece of paper and risking that others will see them (Li, Zhiwei *et al.,2014*) .At its core, A password manager operates as a safe storage to record user passwords and account usernames such as Facebook account, Twitter account, Instagram account details, bank account details and other significant account login credentials. The password manager uses a master username and password to secure access to this database. With a robust master password, a safe password manager guarantees that a user can depend on separate, unguessable passwords for each web service without the related cognitive burden of memorizing them all.

Instead, only one strong master password should be remembered by the user.

This paper aims to eliminate the bottlenecks associated with memorizing numerous login credentials accounts of various web services. Such as Email, Twitter, Instagram. A password manager does have a warehouse or memory on different web apps of the login details of a user. A web application is a website that verifies its users by demanding a mixture of username and password. The "entry point" of the web app is the section where the user of the application can enter his username and password. We call an entry point, username, and password mixture of a credential. For the same web application, a user can store various credentials, in which case name separates each credential.

1.1 Two Factor Authentications

Two-factor Authentication is a system in which authenticated combination of two different factors are used. Using two factors as compared to one factor usually results in a higher level of authentication assurance. In August 2006, the FFIEC released additional guidelines on this topic clarifying, "By default, true multifactor authentication involves the use of two solutions or more of the three categories of factors, using multiple solutions from the same category would not constitute multifactor authentication."

This second factor typically takes the form of a user's physical security token or smart card. This is referred to as the factor of what you have. In this case, mobile phone and other personal devices may also be used by some application. One example is using any bank's issued ATM card. One authentication factor is the customer's physical ATM card that customer slides into the ATM machine. The second factor is the PIN the customer enters. Without both, authentication cannot take place.

Another application of the second factor, such as a fingerprint scan, may be a biological factor. This is referred to as the factor of what you are. Using the what-you-are factor requires special equipment to scan input data, which means that delivery costs and complexity are higher.

The research work of Liou and Bhashyam, (2017) improve on security, stated that the information in the what-you-have factor should be changed along the time. Thus, the information is no longer valid when it is stolen and re-used. This is called One Time Password.

2.0 LITERATURE REVIEW

There is significant literature work that has been done on how user information can be kept safe. Various researchers have contributed in this area but not without room for improvement. In view of this, Sandvoll *et al.,* (2014) designed and analyzed password management system. The password management system has been designed and implemented as an iOS application called PassCue. PassCue is based on the Shared Cues password management model, the design and implementation choices, as well as parameter evaluation, were important in order to create a usable and secure system. PassCue uses cues to share secrets across multiple accounts in order to achieve the competing usability and security goals.

In the work of Whitten *et al.*, (1999) that evaluated the usability of a security program, (Pretty Good Process) PGP 5.0, have concluded that usability principles should be extended beyond the ones commonly used for generic user interface evaluation and design. They claim that security as a field has a series of properties that introduce extra difficulties in the design of secure and usable systems.

Pretty Good Privacy (PGP) pretty good privacy is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

According to McCarney *et al*., (2012) design and implementation password manager application, named Tapas, that works with dual device authentication instead of a master password to encrypt the database. Their study aimed to alleviate the users from the burden of memorability completely while keeping a good usability standard as other popular password manager applications that they used to compare Tapas.

Many more studies for instance, Veras *et al*., (2014) have confirmed the frustration of users and its effects on password creation. They found that users would fulfill policy requirements in predictable ways such as use only a small fraction of the symbols on a keyboard, choose semantically meaningful passwords and password-phrases that follow grammatical rules.

Finally, another study on password-creation policies carried out by Shay *et al*., (2016) found that the usual comp8 is very susceptible to both online and offline attacks and should be replaced with more usable and secure alternatives, like the 2word16 or 2class12.

Table1 presented the summary of password managers related literature that consider storage resources available as well as the systems represented have been evaluated in specifics together with the database layout being used by software. In this paper, we argue if source code is obtainable and that the password manager is incorporated with a browser.

3.0 METHODOLOGY

3.1 The Proposed Protective System

The technique implore in this research work as methodology uses a two-factor authentication to address certain security issues while bringing in some feasibility issues and other security concerns. Therefore, in this section, we presented the protective system' conceptual designs that describe how activities are being carried out by the user from the point where user registers account to the point where user information is being retrieved.

Table 1: Analysis of the existing and proposed system

S/No.	Related Work	Authors/Year	Databasse Layout	Storage Type	Open Source	Platform/Device	Browser Integration
1.	Design and analysis of Passcue password manager	Marts *et al.*, 2014	Microsoft Internet Explorer(MSIE)	Local/cloud	Yes	IOS	No
2.	Design and implementation of password manager (Tapass)	McCarney *et al.*, 2012	Knowledge of database	Local	Yes	Windows/Linux	No
3.	Development of a password manager (LastPass)	Karole *et al.*, 2011	Knowledge of database	Local/Cloud	No	Windows	Yes
4.	Design and analysis of a smart phone based password manager (KeePassMobile)	Shey *et al., 2010*	Knowledge of database/knowledge Of database X4	Local	Yes	Windows/Linux/Max	No
5.	The proposed System (dual possession authentication protective system for managing user login credentials)	Ekundayo *et al.*, 2019	Knowledeg of database	Local/Cloud	Yes	Windows	No

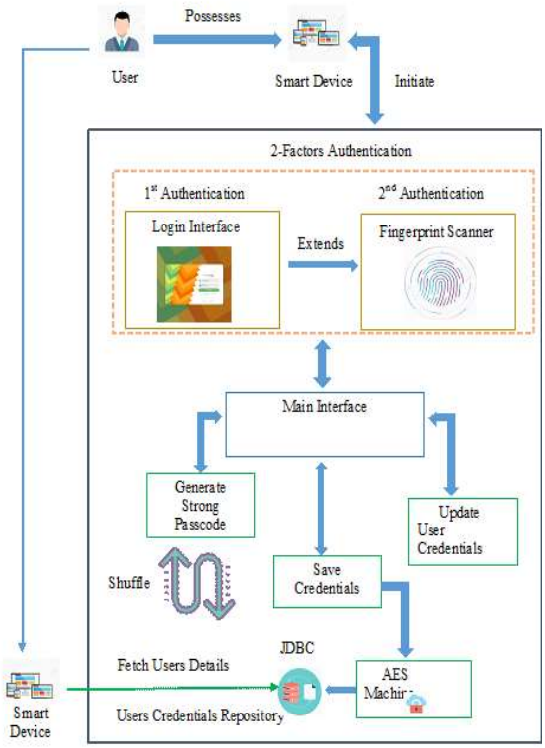

Figure 1 – System Architectural Overview of the Proposed System

From figure 1, a user uses their computer to initiates the application. It is expected of them to supply necessary information such as username and password, after which they will be authenticated using a finger-print recognition. After the authentication has been successful, user can now proceed in using the application. Users are allowed to perform some certain activities listed below.

(i) Initiates the system.
(ii) Pass through the authentication process without trespassing any security protocol.
(iii) Use the system to generate a very strong password.
(iv) Use the system to encrypt their personal credentials.
(v) Use the system to fetch or retrieve encrypted credentials that was stored.

3.2 Main Interface

The main interface will be presented to the user after the user have successfully registered their account. this interface provides user to be able to performs the following action.

Generate user with strong password

Generating strong password for user is having to do the work of combining user choice of words for their password, shuffle it together and their by using those input words to produce a very strong password that is very difficult to break or guess.

Save credentials

User information will be store locally in their system and cloud where user will be able to reach at any part of the word remotely

Update user credentials

Users information maybe out of date according to user's specification and it needed to be updated so as to meet the current trend at that time. One of the purposes that the main interface serves, is to allow user update their information as soon as possible. It is very important that user have already registered account.

AES Encryption engine

AES which is a short form of Advanced Encryption Standard is used in order to protect data against unauthorized access and to encrypt this. The cryptographic process key of varying length is utilized for this purpose. This is designated AES-128, AES-192 OR AES-256 depending on the length. The process was originally introduced by the American national institute of standards and technology and can be used in the USA to encrypt documents with a maximum security rating. This method of encryption of any type data is considered to be particularly secure and effective. This AES will encrypt user information that is supply into the system before saving it into the database so as to increase the cost of attacker.

JDBC Java Database Connectivity

JDBC stands for Java Database Connectivity, which is a standard Java Application Programming

Interface (API) for database independent connectivity between the java programming language and a wide range of databases.
The JDBC library includes APIs for each of the tasks mentioned below that are commonly associated with database usage.
(i) Making a connectivity to database.
(ii) Creating SQL or MySQL statements.
(iii) Executing SQL or MySQL queries in the database
(iv) Viewing & Modifying the resulting records.

Fundamentally, JDBC is a specification that provides a complete set of interfaces that allows for portable access to an underlying database. Java can be used to write different types executables, such as:
(i) Java Applications
(ii) Java Applets
(iii) Java Servlets
(iv) Java Server Pages (JSP)
(v) Enterprise JavaBeans (EJBs).

All of these different executables are able to use a JDBC driver to access a database, and take advantage of the stored data.

JDBC provides the same capabilities as Open Database Connectivity (ODBC) allowing java programs to contain database independent code

3.3 JDBC Architecture

The JDBC API supports both two-tier and three-tier processing models for database access but in general, JDBC Architecture consists of two layers-
(i) JDBC API: this provides the application TO-JDBC Manager connection

JDBC Driver API: This supports the JDBC Manager-to-Driver Connection.

The JDBC API uses a driver manager and database-specific drivers to provide transparent connectivity to heterogeneous databases.

The JDBC driver manager ensures that the correct driver is used to access each data source. The driver manager is capable of supporting multiple con-current drivers connected to multiple heterogeneous database.

Figure 2 in addition implore Use Case Diagram to depict the scenarios functionality of the proposed System.

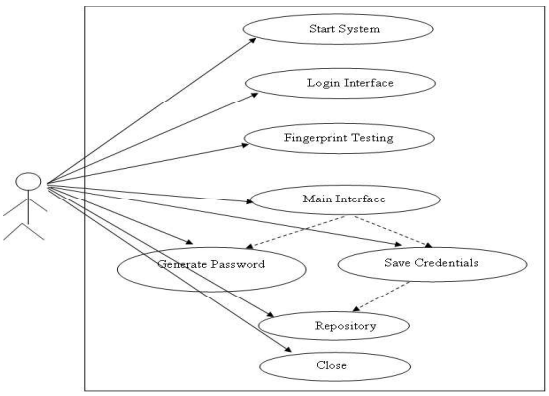

Figure 2: Use case of diagram of the proposed System

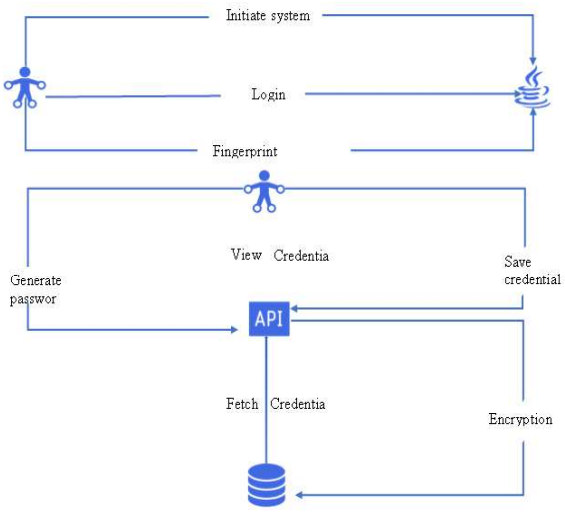

Figure 3: Data Flow Diagram The Proposed System

Figure 3 describes the data flow in the proposed system. Dataflow diagram is an easy to comprehend graphical method which aids in describing the boundaries of the system. It is beneficial for communicating the currents system data which describes the logic behind the data flow within the system to the user. It is also used to model a new system. The following are the advantages of the data flow diagram over other diagrams:
(i) Data flow diagram could visually "state" things that might be very difficult to describe in words, and they function for both technical and non-technical audiences.
(ii) They are much less relevant nowadays to visualizing interactive, real time or data base oriented software or system.
(iii) It could be used as an initial step to develop an overview of the system without entering deep detail.

4.0 RESULTS AND DISCUSSION

The data obtained by testing the password manager system was analysed to approve the proposed design. After a successful registration of user 's account. users are allowed to save their login details, generates a strong password for their multiple accounts. Also, share credentials through a secure channel.

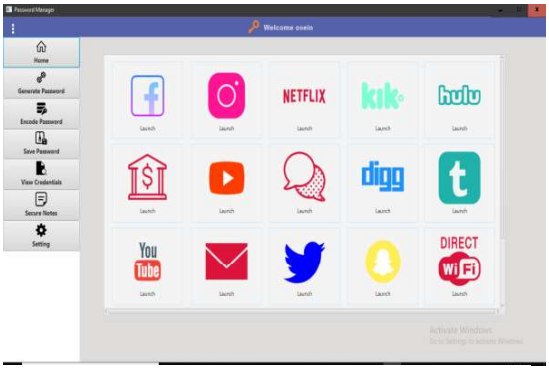

Figure 4: Encrypting user information

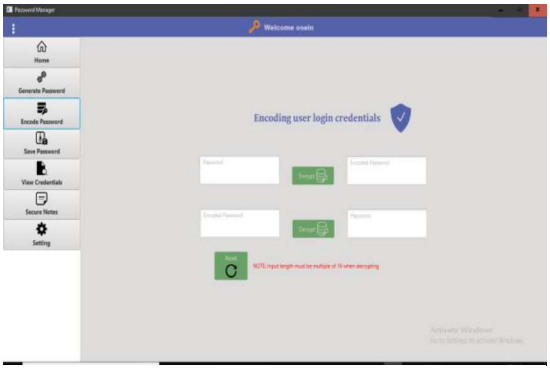

Figure 5: Encrypting and decrypting mechanism

The main interface presented incorporates the activities perform by the proposed password manager called passhouse. By the left of the interface, there are six major components, Home, Generate Password, Encode Password, Save Password, View Credentials, Secure Notes.

When the user registers with the software service, it will obtain a username and passwords for the software service. When the user wishes to store the password for the password manager service on the storage, it must first encrypt them with the user encryption key before transmitting them. The encryption mechanism makes use of user own generated key for the encryption.

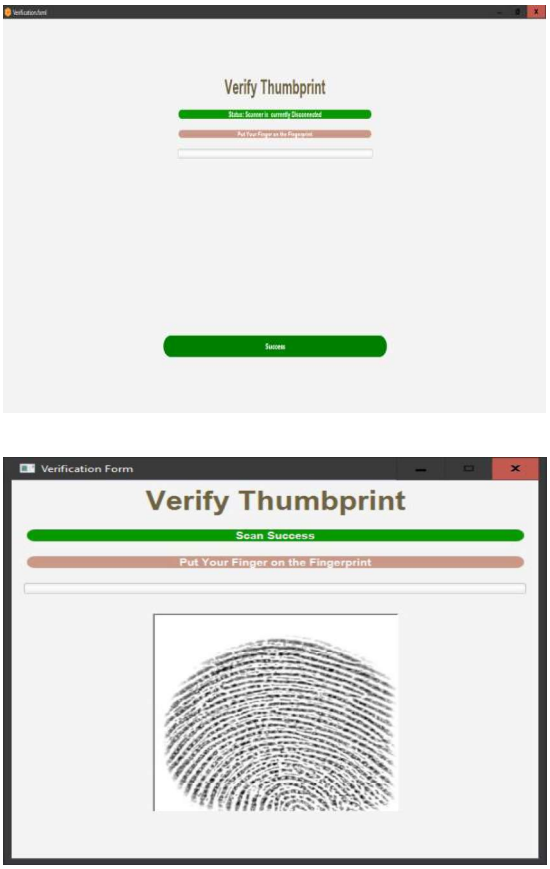

Figure 6: User verification using a fingerprint scanner

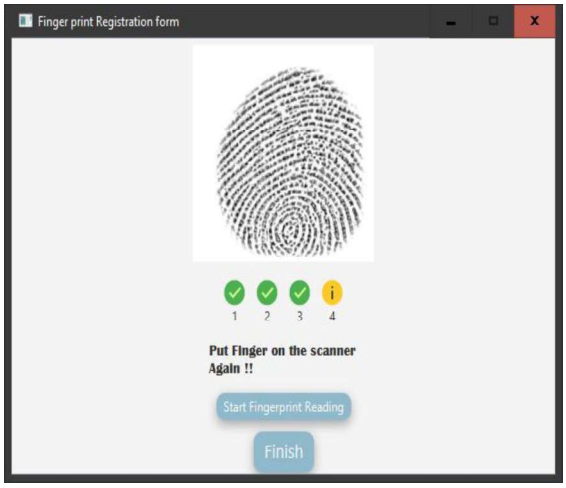

Figure 7: Fingerprint Scanning process

5.0 CONCLUSION

This project provides solution to the problem people are facing when it comes to remembering their login credentials details, and also of generating strong password for their digital account. The use of this system is limited to users or organizations with personal computer. The implemented system has the following features; fast navigation for user to perform tasks, well-built user interactive application, fast retrieval of user information, mechanism for generating a strong password for users. The proposed system is developed based on java technology and two factor authentications along with Advanced Encryptions Security algorithm is also enforced. Thus, in this paper, the proposed system possesses the features and strength to remove users' challenge of recalling login credentials of numerous web services at any point of use.

REFERENCES

Alkaldi, N., & Renaud, K. (2016). Why do People Adopt, or Reject, Smartphone Security Tools? *EuroUSEC 2016: The 1st European Workshop on Usable Security*, (July), 1–15. https://doi.org/10.14722/eurousec.2016.23011

Aurigemma, S., Mattson, T., & Leonard, L. (2017). *So Much Promise , So Little Use : What is Stopping Home End-Users from Using Password Manager Applications ?* 4061–4070.

Bharadwaj, A. S. (200). A resource-based perspective on information technology capability and firm performance: an empirical investigation. MIS quarterly, 169-196

Chaudhary, S., Schafeitel-Tähtinen, T., Helenius, M., & Berki, E. (2019). Usability, security and trust in password managers: A quest for user-centric properties and features. *Computer Science Review*, *33*, 69-90.

Conklin, Art, Glenn Dietrich, and Diane Walz. "Password-based authentication: a system perspective-based authentication: a system perspective." 37th Annual Hawaii international Confe-

rence on System Sciences, 2004. proceedings of the. IEEE, 2004

Gasti, P., & Rasmussen, K. B. (2018). *On The Security of Password Manager Database Formats*.

Hakbilen, O., Perinparajan, P., Eikeland, M., & Ulltveit-Moe, N. (2018). *SAFEPASS - Presenting a Convenient, Portable and Secure Password Manager*. (Icissp), 292–303. https://doi.org/10.5220/0006603102920303

Horsch, M., Andreas, H., & Buchmann, J. (2015). *PAsswordLess PAssword Synchronization Extended Version*.

Liou, J. C., & Bhashyam, S. (2010). A feasible and cost effective two-factor authentication for online transactions. *2nd International Conference on Software Engineering and Data Mining, SEDM 2010*, 47–51.

Maqbali, F. Al, & Mitchell, C. J. (2019). Web password recovery: A necessary evil? *Advances in Intelligent Systems and Computing*, *881*, 324–341. https://doi.org/10.1007/978-3-030-02683-7_23

Quelch, J. A., & Klein, L. R. (1996). The Internet and International Marketing. Sloan Management Review, 37(3), 60-70.

Sandvoll, M. B. (2014). *Design and analysis of a password management system* (Master's thesis, Institutt for elektronikk og telekommunikasjon).

Sandvoll, M., Boyd, C., & Larsen, B. B. (2014, December). PassCue: The Shared Cues System in Practice. In *International Conference on Passwords* (pp. 119-137). Springer, Cham.

Li, Z., He, W., Akhawe, D., & Song, D. (2014). The emperor's new password manager: Security analysis of web-based password managers. In *23rd {USENIX} Security Symposium ({USENIX} Security 14)* (pp. 465-479).

Sandvoll, M. B. (2014). *Design and analysis of a password management system* (Master's thesis, Institutt for elektronikk og telekommunikasjon).

Whitten, A., & Tygar, J. D. (1999, August). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *USENIX Security Symposium* (Vol. 348, pp. 169-184).

FFIEC press release. Visited and retrieved on 28th September, 2019, http://www.ffiec.gov/press/pr081506.htm.