International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 5 Issue: 3 March 2020

Password Manager with Multi Factor Authentication based on URL Categorization

V.Geetha[1], S.Brithvirajan[2], S.Pavithra[3], S. Thiyagarajan[4], P.Bharath[5]

[1,2,3,4,5]Department of Information Technology, Pondicherry Engineering College, Puducherry, India.
[1]vgeetha@pec.edu, [2]brithvirajan.itpec16@gmail.com, [3]pavithraselva99@gmail.com,
[4]thiyagarajanrock1998@gmail.com, [5]bharathdhanush87@gmail.com

Abstract: Password managers reduce the difficulties in creating and remembering strong passwords. Password is the most popular and simplest way in which users can authenticate themselves before accessing computer systems or websites. Password management is organization and encryption of many personal passwords using a single login. Some common risk involved in losing password is over the shoulder attack, Brute-force attack, Sniffing attack, Login spoofing attack. Using Password manager adds another layer of security to our password and data protection. The project ensures that it provides security from hackers as well as getting rid of remembering passwords. Websites and their services risk breach attacks as much as we are and phishing attacks that tried to trick us into handing our password over. Even if some companies are supposed to scramble our password once we enter it known as hashing, not all of them use powerful or modern algorithms, making it simple for hackers to reverse the hashing and read our password in plain text. Others don't care at all about hashing. That puts our accounts at risk of stealing passwords or putting our data at risk for identity theft being used against us. The other problem is the huge number of passwords we have to remember. Banks accounts, social media, email and other login credentials. It is much easy to use one password across the sites. But that makes credentials more vulnerable. That's why hackers take out the password from one breached site and try to log in to our account on other sites. Using a password manager makes it much easier to create and store stronger passwords that are unique to each site, that prevent credential stuffing attacks

Keywords: Authentication, Biometrics, cloud storage, cryptography, keys and password security.

1. INTRODUCTION

Based on functional characteristics and data classification, every information systems will have different security requirements. In general, authentication mechanisms to be used in a way such that it protects all valuable information assets in a secured manner. For example, information which is open to public can allow anonymous logins whereas information which is internal requires strong access control.

Hence having these conditions in mind, different systems should use different passwords based on their security requirements and protect those valuable information assets. If we use the concept of providing single password to all systems then it should have high security requirement to secure all information assets. If it is not satisfied then hackers can attack weakly protected systems and can gain access to all other highly protected assets.

Most of the existing password managers stores passwords in the browser. Among all browsers open source browsers are more vulnerable for attacks. Our project uses cloud storage to store encrypted passwords. A master account which has master username and strong master password created by the user. This master password will in turn undergo a strong hash technique which will output a 4 digit key called as lucky number. This lucky number is given to the user. This is the only 4 digit key, which the user has to remember while entering to other websites. This factor makes the system user friendly. For the First time when the user login to any website, the password he enters, will be fetched only when the user gives save option in the wrapper that appears. The Password will be fetched using password field detection technique. The fetched password will undergo encryption and stored in cloud. For every further logins into the particular account the users makes, the password field detection technique detects the password field and a wrapper will pop up which asks user to enter the 4 digit pin. This pin is validated and the password for the particular website is retrieved from the storage and given to the user or filled automatically in the password field and some

mechanisms will be provided to update passwords and recovery measures will be given when the user lost the security pin. The system requires the user to present one thing that he has as proof that he is who he claims to be in fact. This is easy to implement but at the same time there are a number of security threats to the password approach. The following are certain security risks where a user may lose his/her password:

1. over the shoulder attack: when a user types the password, someone may observe what is being typed by the user and hence password will be stole by looking over the person's shoulder, or by indirectly monitoring using a camera.
2. Brute-force attack: A password has a finite length, normally 8 alphanumeric characters; an attacker may use programs that create passwords automatically and then attempt all possible combinations before a password is found right. With recent developments in the world of computing, the time required to create a effective brute force attack has dropped considerably.
3. Sniffing attack: When transferring a password over a network, it could be possible for network sniffing tools to capture it if the network channel is not properly encrypted. Additionally, any malicious device could be able to catch the password of a user while typing in the password.
4. Login spoofing attack: An attacker set upsa fake login screen that looks and feels like original login screen. When a user enters the credentials, his password will be taken or transmitted to the attacker.

When successful, all of these attacks will help unauthorized users or attackers record legitimate user passwords.

In some static instances, the malware will forever have both a fixed Internet protocol address and a fixed domain name, which will not change its domain name throughout its lifetime. So as long as this malware is identified as a threat, a simple set of rules can be applied to solve this problem of malware threat. So, as long as this malware is known as a threat, a simple set of rules can be implemented to solve this threat to malware problem.

Cryptography transforms the original readable message or text into an unreadable format, and transmits the message through an unsafe channel. Cryptographic systems are two styles. They are symmetrical (secret key) and asymmetrical (public key) cryptosystems built for purposes of security. From the first case, that is the symmetric cryptography, only one key (private key) can be used for both the encryption and the decryption method. In this, only one key (secret key) will be kept secure by the sender of the private key cryptography system; it can be swapped or exchanged between the sender and the text or message receiver. The private key is divided into five components depending on situation. They are plaintext, cipher text, encryption algorithm / decryption algorithm, and private key. The technique for symmetric key cryptography seems simple and easy to understand as locking and unlocking the door using the same key. Cryptography in this digital environment requires advanced system to provide both sides with the private key. This system needs to be sufficiently involving or revealing to survive the process. AES is one example for symmetric cryptography. It is an iterative algorithm.AES uses data block of 128 bits and key sizes used in this process are different and they are 128, 196, and 256 bits. This data block is divided into 16 bytes and is mapped into a 4 x 4 array called State. As for speed, AES has a process of rapid encryption and decryption. For this cryptography the encryption ratio is high, and there is no tenability. The encryption standard is provided by the U.S. government, and has been approved for encryption of confidential information by the National Security Agency (NSA). Asymmetric cryptography is next. It uses two keys; they are public and private keys. Example, most commonly used asymmetric cryptographic algorithm is Rivest-Shamir-Adleman (RSA). The cryptosystem RSA is a fairly complex process. The mechanism follows some mathematical calculations like large integer modular arithmetic, generation of prime numbers etc... RSA cryptographic system is more efficient in generating large prime numbers. In general, the key length in the RSA cryptography algorithm is quite long for making it very hard for an attacker to crack the code. Therefore asymmetric key algorithms like RSA seems to run slower when compared to symmetric key algorithms like AES. Moving to the main aspect of security, the symmetric main encryption is much better compared to asymmetric key encryption. This work designs the multi-factor authentication used in saving passwords, using high-level security RSA encryption. Many detection strategies are based on the assumption that by signatures or patterns malware can be identified. The most widely used method for anti-malware systems is the signature-based identification. These features can be used in constructing the signature of the particular malware. So, Signature based detection uses the knowledge of what is considered as malicious to find out the maliciousness of the program under inspection. On the other hand, tons of literature has tried to improve anomaly based intrusion detection methodology. This is a technique for detecting abnormal behaviour that differs from the normal behavior baseline. It requires that the normal behaviour of the network to be determined and studied first before identifying the

International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 5 Issue: 3 March 2020

abnormal behavior. This approach of anomaly-based intrusion is important because it has the capability to detect the unknown or new attacks. This technique has a unique advantage over other similar technologies of same functionality, because it is capable of detecting new or unknown abnormal behavior.

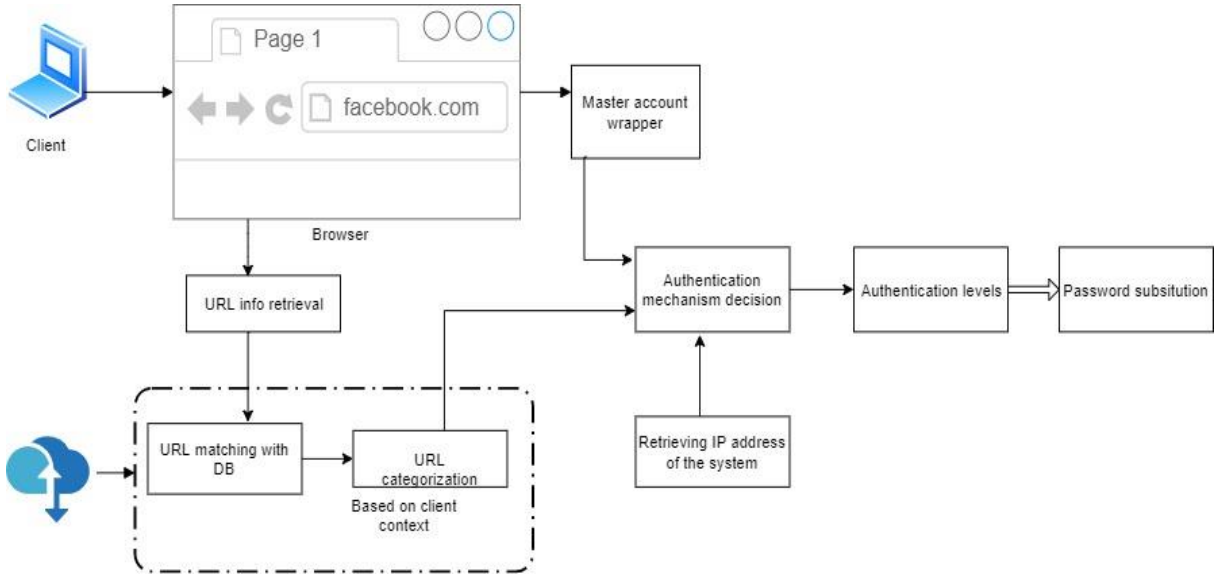

Figure 1.1 password manager based on categorization of URL

2. PROPOSED WORK

The proposed system has the following modules:
Module 1: Creating Master Account for the user. Module 2: Password encryption module and storing passwords Module 3: Retrieving passwords
Module 1: This is the starting module of the proposed system. This module includes creating a master account and username, password of specified sites. The user needs to register to the master account with some of the details like email id, mobile number, mater username and master password.
This master password undergoes own encryption algorithm which outputs a four digit pin number. This generated four digit pin is given to the user, which will be used as a password for further logins. After the registration process, the user needs to only remember the four digit pin number (making the system easier). This password manager setup was loaded as a browser extension. When the user is entering to the new website, the username and password he used to create the account is retrieved. A popup will be shown to the user asking to save the password for particular site. Once the user clicks the save button in the popup, the password was retrieved and stored along with the site URL.
Next time, while entering to the same site, the user could able to see the password manager as a browser extension. On clicking the extension, a wrapper opens. The master username and four digits pin number needs to be entered by the user. After verification with the master account, the system will allow the user to enter to the specified site.
Module 2:In this module, the user would store the passwords for first time in his account. When the user enters a password field, the password manager fetches the URL, username and password. Now the password is encrypted using strong encryption algorithm and stored in cloud.
Module 3:This is the main module in which password is retrieved without remembering it. When the user enters a password field, the password manager opens the wrapper. The user has to enter his master username and pin number which is a security check for retrieving passwords. Now the password manager allows the user to enter the website.
To retrieve password from any URL, we used a PHP file and redirected it to our site as of now. **PHP** is meant for server-side scripting language. PHP is **used** to develop Static and Dynamic websites or Web applications. **PHP** stands for Hypertext Pre-processor, that earlier indicated as Personal Home Pages. **PHP** scripts can only be interpreted on **PHP** installed server. A PHP 5 library for easy Open ID authentication. The stable version works only as a consumer, but there's an alpha version of a provider class available in the git repository. Since the Open ID protocol was obsoleted by the Open ID Foundation, this library is obsolete as well, and as such, is not maintained anymore.

International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 5 Issue: 3 March 2020

3. LITERATURE SURVEY

This gives the detailed survey of features and policies implemented in the widely deployed password managers.

Table1.1 Comparative studies on various existing password management Techniques.

s.no	Journal Name, Year	Paper Title	Techniques/ Methodology	Advantages	Disadvantages
1	In proceedings of the 4th international conference on Information Systems security and privacy, SCITEPRESS Jan,2008	Split Pass: A mutually distrusting two-party password manager	It splits the secure sockets layer (SSL) and Transport Layer Security (TSL) sessions to process on all parties and makes joining of 2 password Shares transparent to the web servers.	It can defend against phishing attack.	It faces user experience issues and user impersonating attacks.
2	Journal of Computer Science and Technology Jan, 2018.	SAFEPASS presenting a convenient, portable and secure password Manager.	It is based on JavaScript and .Net including React, Xamarin and ASP .Net core.	It uses code obfuscation and cryptographic key sharing to reduce risk of an attacker identifying the password	It doesn't have support for browser extension and no support for password changes in case of emergency.
3	2nd International conference on Applied Science and Technology, October 2017	Multi-agent integrated password management (MIPM) application secured with encryption	MIPM is developed on the Android applicationwith an encryption agent using Java Agent Development Environment (JADE).	Increase the security of strong users information by using a strong encryption algorithm and utilising JADE technology.	Platform for users to store the social media login Information only
4	IEEE30th International conference on Advanced Information Networking and Applications (AINA), 2016	A proposal of a password manager satisfying security and usability by using the secret sharing and a personal server.	Login information is encrypted by a strong secret key in the PC, and the encrypted data are sent to and are stored in the smartphone paired to the PC	Usability is more. Secure sharing is allowed for distributed usage of login information.	Deployability and the security have become worse. Login information cannot be recovered if the paired smartphone is lost.
5	Proceedings of 23rdUSENIX Security Symposium, August, 2014	The emperor's New Password Manager: Security Analysis of web-based Password Managers.	Web based password authentication	Remembering one master password. Deployability becomes simple	No encryption techniques applied for passwords
6	IEEE International Conference on Cloud engineering, 2014	Cloud password Manager Using Privacy-Preserved Biometrics	Uses 1 master password for accessing all accounts. Uses biometrics as a second factor of authentication.	Easy to remember only one master password cloud storage gives access at any time anywhere.	All other passwords can be lost if the security key is lost. Cost is the factor to be considered.
7	IEEE 3rd International Conference on Biometrics, Sep 2009	Medical biometrics in mobile health monitoring.	ECG-based identity management in mobile health monitoring applications.	Universality, Permanence, Uniqueness, Data minimization.	Time dependency, Privacy implications, Cardiac Conditions..

The main drawback of existing password management services is that the actual information is accessed by the browser. With the use of personal server based password managers, the limitations lies in device dependency. There is a need to carry devices with us always as a personal storage. Single Sign on Solutions help in a way to authenticate only once to gain access to all other applications. It helps in avoiding the risk of memorising many passwords and has to remember only one password instead. It compromises of using only one authentication event to all other resources.

BTP is a technology for translating biometric data into a safe template and storing it for direct comparisons in the database without leaking biometric information. Drawback to using this is that environment and use can affect measurements, and systems are not 100% reliable, require integration and/or extra hardware, and it cannot be reset once compromised.

Public Key Infrastructure (PKI) is a technology used with mathematical algorithms to offer secure transactions and ensures data confidentiality, data integrity, and authentication. By making use of digital certificates it ensures proof of identity. A digital certificate is nothing more than a digital document which has as authentication key a public key for a person. It is like a personal ID card for a person. This identity is provided by issuing a certificate done by a trusted Certificate Authority (CA). It is digitally signed using CA's private key. The applications check the user's identity by verifying this digitally signed certificate. They are mainly used for online transaction involved applications and some public applications. This is because they don't require any registration process to be held before. Users only need digital certificates by any trusted CA for authentication.

Next we consider a technology called one-time password token. Now-a-days PIN numbers play a safe role in providing passwords. Users authenticate with two unique factors namely tokens and PIN numbers. The tokens generate a unique OTP to gain access to the resources.

Before choosing this one-time password token we need to consider the following:

A token is an additional resource to be carried for every authentication process. Users have to remember token every time and if they forget the token then the system can't be accessed. It is not like a password reset option. If the user forgets the token they have to wait for hours or a day to get a new one. Users must take care of their token values so that no one gets their token information. This token technology provides only initial support and there are chances of information to be hijacked. Hence only some applications make use of it.

4. CONCLUSION

Malicious By using password manager we never have to worry about forgetting a password again. Infact, approximately 37 percent of individuals claim that they have to request a password reset on at least a website per month because they do not remember passwords. To overcome all limitations and disadvantages of existing password managers, we suggest a new password manager that addresses problems above. We include necessary parameters like two factor authentication for security, encryption and decryption techniques for password storage and retrieval.

REFERENCES

[1] Liu YT, Du D, Xia YB et al. "SplitPass: A mutually distrusting two-party password manager", *Journal of Computer Science and Technology,* DOI 10.1007/s11390-018-1810-y, ISSN : 11390-018-1810, Jan. 2018, pp.98-115.

[2] Hakbilen, O., Perinparajan, P., Eikeland, M. and Ulltveit-Moe, N, "SAFEPASS – Presenting a Convenient, Portable and Secure Password Manager", In *Proceedings of the4th International Conference on Information Systems Security and Privacy, SCITEPRESS,* DOI: 10.5220/0006603102920303, ISBN : 978-989-758-282-0, Jan.2018, pp.292-303.

[3] NorkhushainiAwang, NurulHidayah Ahmad Zukri, Nor AimuniMd Rashid, ZuhriArafah Zulkifli and Nor AfifahMohdNazri, "Multi-agent integrated password management (MIPM) application secured with encryption‖", *The 2ndInternationalConference on Applied Science and Technology,* ISSN : 978-0-7354-1573-7, October.2017.

[4] Carlos Luevanos, John Elizarraras, KhaiHirschi, and Jyh-haw Yeh, "Analysis on the Security and Use of Password Managers", in *18thInternational Conference on Parallel and Distributed Computing, Application and Technologies,* DOI : 10.1109, Jan.2017.

[5] Masayuki Fukumitsu, Shingo Hasegawa, Jun-yaIwazaki, Masao Sakai, Daiki Takahashi *"*A proposal of a password manager satisfying security and usability by using the secret sharing and a personal server‖", *IEEE 30thInternational Conference on Advanced Information Networking and Applications (AINA),* 2016.

[6] Zhiwei Li, Warren He, Devdatta Akhawe, and Dawn Song, "The Emperor's New Password Manager Security Analysis of Web-based Password Managers" in *proceedings of 23rd USENIX Security Symposium*, ISBN : 978-1-931971-15-7, August , 2014.

[7] Bian Yang, Huiguang Chu, Guoqiang Li, Slobodan Petrovic, Christoph Busch, "Cloud Password Manager Using Privacy-Preserved Biometrics", *IEEE International Conference on Cloud Engineering*, DOI : 10.1109, ISBN : 978-1-4799-3766-0, 2014.

[8] Damousis, IG, Tzovaras,D, and BekiarisE, Unobtrusive multimodal biometric authentication: the HUMABIO project concept, EURASIP Journal of Advances in Signal Processing, 2008; 2008: 1–11.

[9] Bui FM, Hatzinakos D. A receiver-based variable-size burst equalization strategy for spectrally efficient wireless communications. IEEE Transactions on Signal Processing 2005; 53(11): 4304–4314.

[10] X. Zhou and X. Tang, "Research and implementation of RSA algorithm for encryption and decryption," International Forum on Strategic Technology (IFOST), 6(2), pp. 1118-1121, 2011.

[11] B. Yang, D. Hartung, K. Simoens, C Busch, "Dynamic random projection for biometric template protection," Proc of the 4th IEEE Int Conf on Biometrics: Theory, applications and systems (BTAS'10), 2010.

[12] R. Wang, S. Chen, X. Wang, "Signing me onto your accounts through Facebook and Google: a traffic-guided security study of commercially deployed single-sign-on web services," IEEE Symposium on Security and Privacy, pp. 365-379, 2012.

AUTHOR BIOGRAPHY

Dr.V.Geetha

V.Geetha is currently working as Associate Professor in the Department of Information Technology in Pondicherry Engineering College, Puducherry, India. She has completed her B.Tech (CSE) in 1990,M.Tech (CSE) in 1999 and Ph.D. (CSE) in 2013. She has published around 35 papers in various International Conferences and Journals including Elsevier and Inderscience. Her areas of research include Distributed Objects, Cloud Computing and Data Security.

S.Brithvirajan

He is pursuing his B.Tech degree in the Department of Information Technology, Pondicherry Engineering College, Pondicherry.

S.Pavithra

She is pursuing her B.Tech degree in the Department of Information Technology, Pondicherry Engineering College, Pondicherry.

S.Thiyagarajan

He is pursuing his B.Tech degree in the Department of Information Technology, Pondicherry Engineering College, Pondicherry.

P.Bharath

He is pursuing his B.Tech degree in the Department of Information Technology, Pondicherry Engineering College, Pondicherry.