Cloud Based Password Wallet and Manager

Vaibhav Kunjir[1], Pranjal Mavale[2], Abhishek Godase[3]
Department of Computer Engineering, Anantrao Pawar Collage of Engineering and Research, Pune

[1] *Abstract*

Although various solutions have been suggested for password management systems, most methods require the support of external physical hardware infrastructure. Due to the increase in complexity and cost of set-up of supporting hardware requirements, scalability will always be an issue with such systems. In this paper, we present the design of a Cloud based password management system. The proposed method uses Cryptography for better encryption and is supported by a web-based architecture, for easily managing passwords and providing an indoor cloud based password manager system .

Keyword:

Cloud Computing
Restful API
Cyber Security
Password Manager

I. INTRODUCTION

The purpose with this project is to find out how todays password handling and security works. It willalso check, with the help of a survey, how ordinary people handle their own passwords. How often they change them, their view on how secure the passwords are and if they use tools to help keep changing and handle their passwords. Many differenttools are available to help users create and handle their passwords but how secure are theses "password management"- tools in reality? In this project, a few does it bring to everyday users, in regard to letting oneself keep the control of the passwords? The results of the survey, regarding user view on password security, will be compared with information regarding how one should reason to create secure passwords. One can find a lot of advice from both companies and experts on how a secure password should look like. Do people use these advices and how do the information reach the everyday user ?

I. 1.1 MOTIVATION

With the ever-increasing human mobility, peopletends to user more and more passwords in their day to day life. Almost every second site you are gonna visit is most likely gonna ask you to create a accounton their site to access the content they have hosted. With this increasing load of passwords it becoming hard for everyone to remember the passwords they have created earlier. As a result we have three main problems in front of us when it comes to Security.

1. Using Same Password Everywhere:

People are often using same passwords across all theplatforms which makes it easy to remember the password for them but also creating a big securityloophole. If one of you account gets compromised, the attacker can use the same password to login into your other accounts.

2. People Tends To Forget TheirPassword:

If Users are using a strong and unique passwords on across the sites it becomes hard for them toremember all these password as they are numerous and end up getting locked out of the account.

3. People Save Their PasswordDigitally/Physically:

Users usually overcome the above problems by writing down their passwords Digitally/Physically which is the worst solution from the perspective of security. As the passwords are being written somewhere,

it makes them most vulnerable as Ifanyone catch an eye to the document he can have all you passwords without going through the hazel of compromising credentials

1.2 PROBLEM DEFINITION

To build an cloud based password management system using cryptography and Machine Learning. This project stems from the fact that people are increasingly relying upon their smartphones to solve some of their common daily problems. An cloudbased application would certainly benefit users who are unfamiliar with the use of internet.

2. LITERATURE SURVEY1. AES – 256

The Advanced Encryption Standard (AES) algorithmis a symmetric block encryption technique that is extensively utilized across the world. This technique, which has its unique structure for encrypting and decrypting sensitive data, is used in hardware and software all around the world. When using the AES method to encrypt data, it is exceedingly difficult forhackers to decrypt the data. To yet, there is no evidence that this algorithm is broken. AES can
handle three alternative key sizes: 128, 192, and 256

bits, with each of these ciphers having a 128-bitblock size. The number of people using the internet and networks is continually expanding. Every day, a large amount of digital data is exchanged amongusers. Some data is sensitive and must be safeguarded against attackers. Encryption methods are crucial in preventing unauthorised access to original data. Encryption algorithms come in a variety of forms. The Advanced Encryption Standard (AES) method is one of the most efficient, and it is widely accepted and implemented in both hardware and software.

2. AWS

Cloud computing has exploded in popularity, especially among commercial web applications. The pay-as-you-go concept allows for a flexible and cost-effective access to computational resources. Becauseof these factors, the scientific computing community is becoming more interested in cloud computing. Cloud implementation and performance, on the otherhand, differ significantly from those at traditional supercomputing centers. It is consequently necessaryto assess the performance of HPC applications in today's cloud systems in order to comprehend the tradeoffs that come with cloud migration. This is the most extensive comparison of traditional HPC systems to Amazon EC2 to date, utilizing real workloads representative of a typical supercomputing center's workload. Overall, EC2 is six times slower than a normal mid-range Linux cluster and twenty times slower than a recent HPC server, according to the results. The EC2 cloud platform's connection severely limits performance and generates significant fluctuation.

3. SAAS

Cloud computing is a type of internet-based distributed computing that allows a programme or application to operate on several computers at the same time. Software as a service (SaaS) is a type of service that offers various advantages to its users. Toassess the quality of a SaaS cloud service, a specific quality model is required. The standard quality approach ignores SaaS characteristics like as security and service quality. SaaS is a form of cloud service that has developed as a useful repurposing paradigm. It offers service users a number of advantages, including no upfront costs for software, no maintenance/updates, Internet accessibility, high availability, and pay-per-use pricing. As a result, assessing the quality of SaaS becomes a more crucialjob for effective SaaS management.

4. Designing Password Policy for Strength andUsability

Service providers are growing increasingly worried about the security of internet accounts, which has resulted in password-composition regulations. These restrictions limit the number of characters that may be used in user-created passwords, making it more difficult for attackers to guess passwords. Many users, on the other hand, struggle to construct and remember passwords when they are subjected to severe password-composition standards, such asthose that require passwords to have at least eight characters, various character classes, and a dictionary check. According to recent research, focusing policy requirements on password length rather than complexity is a potential approach. Only length was needed by a few of the password- composition criteria we evaluated. These policies were quite simple to implement. Many of the passwords generated as a result of these regulations were quite strong. For High- Security Service Providers, the Pattern Requirement may be appropriate. Passwords must begin and end with lowercase letters to meet the pattern requirement. Without this restriction, the great majority of research participants tended to begin or conclude with special characters that were not necessary.

5. Use of Password Manager

Cybersecurity is one of the most rapidly expanding disciplines in computer science and the technology sector. The global economy has suffered enormous costs as a result of shoddy security. Password security is frequently the stumbling block in such financial losses. Companies and individuals alike are not doing enough to enforce stringent password requirements, as recommended by the NIST (National Institute of Standards and Technology).

Thousands to millions of passwords can be disclosedand kept in files as a result of large security breaches, making users vulnerable to dictionary and rainbow table attacks. These are only a couple of instances of password cracking attacks. One of the main features that Passbolt, Encryptr, and Padlock all have in common is that they are all open-source. Consumers may review the code and report any vulnerabilities or problems directly, which helps to speed up the refining process. Because open-source software is free, anybody can identify security flaws,but not everyone will disclose them. The advantage of closed source password managers is that theircode is shielded from possible attackers. This means that an attacker is unlikely to be able to examine the code and exploit any flaws that may exist. A closed source password manager's biggest flaw is the person who runs it. Because the user is unaware of the intricacies of how their passwords are saved and processed, the user must believe that the organization is safely preserving their credentials. A decent password manager would put security ahead of convenience.

3. SOFTWARE REQUIREMENTSSPECIFICATION

3.1 INTRODUCTION:

Secrypt is an end to end encrypted passwordmanager which keeps you away from privacy worries. Secrypt is concerned with passwords that provide safe access to all of your credentials. Any compromise in the security of these passwords exposes you at risk. As a result, Secrypt Password Manager has been proposed to built to provide maximum security from program installation through user authentication, data transmission, storage, and throughout the usage work flow. One master password protects all of a user's credential in one dashboard.
AES-256 encryption is used by Secrypt. The encryption key is generated automatically and is unique for each user. This is the initial level of encryption key.

3.1.1 PROJECT SCOPE:

When you're looking to build an cloud basedpassword manager. The Password manager is going
to be based on SAAS. A software as a service solution providing you the ability to store all your passwords at one place secured with one master password and that master password is going to be encrypted with the strong encryption. As the solution is based on the cloud and will be hosted entirely on AWS, its going to platform independent and can be accessed from all the possible platforms as long as a browser is installed on the system. Thus providing flexibility for the user to access the password manager.

3.1.2 USER CLASSES AND CHARACTERISTICS

- At least 12 characters (required for yourMuhlenberg password)-the more characters, the better.

- A mixture of both uppercase and lowercaseletters.
- A mixture of letters and numbers.

- Inclusion of at least one special character,e.g., ! @ # ?]

NON FUNCTIONALREQURIMENT

3.2.1 SAFETY REQUIREMENTS:

Password managers provide strong encryption, which serves as a strong defense against cybercriminals. Many password managers are protected by strong encryption like AES, the industry-standard protection the U.S. government uses to protect its sensitive data.

3.2.2 SECURITY REQUIREMENTS Passwords are important when it comes to privacy,online security, and protecting your data. Enter thepassword manager: a tool that stores one strongmaster password that gives you easy access to all ofyour accounts while helping to keep cybercriminalsat bay.

Password management can be tricky. You might resort to using the same password over and over - or tweaking each password just a bit - so you don't forget your passwords and get locked out of your accounts. You might go for something easy to remember. But that also makes it easier for cyberthieves to figure out.

Each password for every service should be unique, complex, and long. While there are potential drawbacks to any software, password managers offer encrypted solutions for creating and storing strong passwords that should help keep your data more secure.

3.2.3 SOFTWARE QUALITY ATTRIBUTES:

Software Quality Attributes can be explained as the characteristics of the software application system that are kept in check, for meeting the needs of the software application to be eligible for being in good quality. Here, for the software quality standards, the term quality can be defined as a scale for distinction, for meeting the needs of the customer or end-user, for satisfying the principles of the application is expected to follow, to hold the user- friendly aspects, etc. These attributes are categorized to be the non-functional requirement specification, which needs to be met in order to make the software system quality exceptional.

Security: This attribute measures the ability of asystem to arrest and block malicious or unauthorizedactions that could potentially destroy the map data. The attribute assumes importance because security denotes the ability of the system to protect data and defend information from unauthorized access. Security also includes authorization and authentication techniques, protection against network attacks, data encryption, and such other risks.

3.5 SYSTEM REQUIREMENTS:

2GB RAM or More

10 Kb/s More Internet speed

3.5.1 SOFTWARE REQUIREMENTS:

- Web browser

3.5.3 HARDWARE REQUIREMENTS:

Laptop or Personal Computer with

- 2GB RAM or More
- 10 kb/s or More internet speed

4. SYSTEM DESIGN

4.1 SYSTEM ARCHITECTURE:

The system architecture diagram is used to show the relation betweeneach hardware and software components.

- their future domains, the system displays questionnaires to the students which the studentneeds to attempt and information from their answers will be used for further processing.
- χollected data by student and predict the appropriate optionamong all other

4. OTHER SPECIFICATIONS

4.1 ADVANTAGES:

The advantage of password-based access controls is that they are easily incorporated in most software using APIs available in many software products, they require no extensive computer/server modifications, and that users are already familiarwith the use of passwords. While passwords can be fairly secure, the weakness is how users choose and manage them, by using:

- simple passwords - short in length, that use words found in dictionaries, or do not mix in different character types (numbers, punctuation, upper/lower case), or are otherwise easily guessable
- passwords others can find - on sticky notes on monitors, in a notepad by the computer,in a document on the computer, whiteboard reminders, smart device storage in clear text, etc
- the same password - using the same etc password information, contractors using samepassword for all their accounts, etc.
- administrative account logins where limitedlogins would suffice, or
- administrators who allow users with the same
- role to use the same password.

5.2 LIMITATIONS:

1. Single sign – on (SSO) method

If a password manager itself is hacked, an organization is potentially at an even bigger risk thanif just one password was leaked. Luckily, many password management systems have extremely robust security measures to prevent attacks from happen

2. Necessary WiFi

The network connection is must as the password manageris cloud based.

3. Single Point of failure

If the user forgets the master password then all the passwords stored in there are of no value so this is one main drawback.

6. CONCLUSION ANDFUTURE WORK

6.1 CONCLUSION

A password manager is software that allows us to create new passwords, save and manage our login information. Both not using and using a password manager have hazards, but the risk of not using one much surpasses the risk of using one for most people. If you do decide to use a password management, you should mitigate the danger of doing so by enabling two-factor authentication, planning your master password recovery procedure, and not saving a high-risk password in your password manager.

6.2 FUTURE WORK:

6.2.1 Auto file Mechanisum

We are planning to make apllications of the password manager for all type of operating systems

. This application will save your time from going tothe website , logging – in and searching for the password.

6.2.2 Password Compromise alert

This mechanism will make the user alert if the useris repeating any password which is used for other website. Also it will alert the user whenever someone uses these password and login in any of the accounts.

References

1. Cusumano, Michael. "Cloud computing and SaaS as new computing platforms." Communications of the ACM 53.4(2010)

2. Gasti, Paolo, and Kasper B. Rasmussen. "On the security of password manager database formats." European Symposium on Research in Computer Security: Springer, Berlin, Heidelberg, 2012.

3. URL:- https://www.malwarebytes.com/what-is-Abdullah, Ako Muhamad. "Advanced encryption standard (AES) algorithm to encrypt and decrypt data." Cryptography and Network Security 16 (2017): 1-11.

4. Cramer, Ronald, and Victor Shoup.

5. "Signature schemes based on the strong RSA assumption." ACM Transactions on Information and System Security (TISSEC) 3.3 (2000): 161-185.

6. Cunningham, A. (2019, July 17). TheBest Password Managers. Wirecutter. https:// thewirecutter.com/reviews/best-password- managers /

7. "Password Protection: How to Create Strong Passwords", Eric Griffith, http://www.pcmag.com/article2/0.2817.236848

Cloud Based password Manager

10. Gallagher, E. A. (2019). Choosing the Right Password Manager. Serials Review,45(1/2), 84-87. https://doi-org.ezproxy.simmons.edu/10.1080/00987913. 2019.1611310

5.asp