**Applied Cryptography (CMPS 381)Course Project**

Selected Topic: Password Store

Submission Date: 10/24/2021

PHASE III

Participated student’s information:

|  |  |  |
| --- | --- | --- |
| Names: | Student QU number | QU-email |
| Talha Abdullah | 201903446 | [Tp1903446@qu.edu.qa](mailto:Tp1903446@qu.edu.qa) |
| Ibrahim Demdoum | 201701515 | [Id1701515@qu.edu.qa](mailto:Id1701515@qu.edu.qa) |
| Mohammed Omar | 201911057 | [Mo1911057@qu.edu.qa](mailto:Mo1911057@qu.edu.qa) |

**Section A: Literature Survey**

**Chapter 1: An Insight to the Password Store**

**Introduction**

A well-designed online password storage made to secure multiple passwords of active users of internet services. User can access his credentials through a simple log-in. The store can accommodate all the users in Qatar and is always available for use. Many methods are implemented to secure the password storage as well as secure credentials separately for the user. The Password storage can help people who have a hard time remembering credentials or people struggling to secure their passwords used for different purposes.

**Why to use the online password storage?**

Online password storage is by far, one of the most popular type across the globe. This service provides users to access their credentials anyplace and anywhere. Simple methods like mobile app or browser extension can be used in case web application is not accessible. The password store uses a technology called zero-knowledge technology, which works based on encrypting data before it is received by the password storage system. The main benefit for the user is that he/she will not need to have a good memory, also not worrying about any kind of credential theft due to the password store being completely secure to manage and store user’s enterprise passwords

**A Diagram representing cloud connectivity**

A picture containing text, computer

Description automatically generated

**Benefits of Password Storage**

1. **Making Process Easier:** Our Password storage will allow access to credentials for the user through a single log-in interface, making life easier for users using multitude of websites and platforms
2. **No more Filling:** The password storage will come with a feature to auto-fill passwords and other credentials extending to addresses or payments. It allows the user to be safe from any hassle regarding remembering the password
3. **Secure Password Sharing:** With the encryption methods used, the password store can safely send passwords to the user himself (to any other devices that the user possesses) or allow the user to share some passwords with his or her family members or friends safely. A secure channel is made for sharing of passwords, hence increasing security
4. **Cross-Platform Support:** The password storage is not too complex and does not require a lot of resources to be installed by the user. Our password storage is a cross-Platform service. Hence, users can access it through their tablets or mobile phones as well. For the user, it is simpler as he can access his credentials no matter the preferred method of communication
5. **Multi-factor authentication:** The password storage will also allow multi-factor authentication mode for the user if he/she wishes to. The multi-factor authentication can avoid hackers trying to access the system by impersonating the user.

**The biggest challenge faced the user of the Password Storage**

The major disadvantage of password storage is that if the user gives access unknowingly to anyone can lead to the leakage of all the passwords, he can access to all the user’s account. Our system provides many services to avoid any such leakage to any third-party software or hacker to ensure any kind of system break.

**Conclusion**

A well-designed online password storage that helps user to access his passwords through a very simple log-in method. The store also is also scalable and can be used by anyone across the country. Many methods used inside the store itself can protect the user’s passwords getting leaked or hacked. Users can rely on the working and functioning of the password storage which is always available.

**Chapter 2: Symmetric Cryptography- AES**

**Introduction to AES**

The Advanced Encryption Standard (AES) is a symmetric block cipher which is used to protect classified information. AES used to transfer the passwords entered by the user which the user intends to save and safely sends it to the password storage system. This allows a safe transfer between the two without any intervention by the hacker. The AES was the first and only publicly accessible cipher for protecting top secret information, which was even used by the US government.

**AES Algorithm**

Diagram

Description automatically generated

**AES Algorithm Description**

1. **Key Expansion-** creating new keys, which are known as round keys.
2. **Round key addition-** initial round key is added to the divided mix of data.
3. **Byte Substitution-** substituting each byte with another byte.
4. **Row Shifting-** moves every row of divided data to a certain number of spaces for each round.
5. **Column-** uses a pre-established matrix to multiply the divided data.
6. **Round key addition-** another mixture of columns.

**How Does AES Work?**

AES has 3 different block ciphers:

1. AES-128 which uses a 128-bit key to encrypt and decrypt the passwords.
2. AES-192 which uses a 192-bit key to encrypt and decrypt the passwords.
3. AES-256 which uses a 256-bit key to encrypt and decrypt the passwords.

There is usually a distinction between all the keys which are generally used. Based on our priority, we can use either the 192-bit key encryption or the 256-bit key encryption.

Based on each key, there is several rounds of working of the initial passwords entered by the user. For instance, there are 10 rounds of 128-bit keys, 14 rounds for 256-bit keys, and 12 rounds for 128-bit keys. Each round consists of several processes like substitution, transposition and mixing of input password to give a resultant ciphertext.

In short, the first transformation causes a substitution from a set of table values, the second causes a shift in rows, the third mixes up the column of the matrix. The last part is done along with the encryption key performed on each column. Longer keys, longer the encryption and hence, tough to crack.

The key also follows the number of rounds, generated new keys with each round using expansion table and other processes. The master key is stored separately while the new keys are used inside the functions for the process of encrypting the original message.

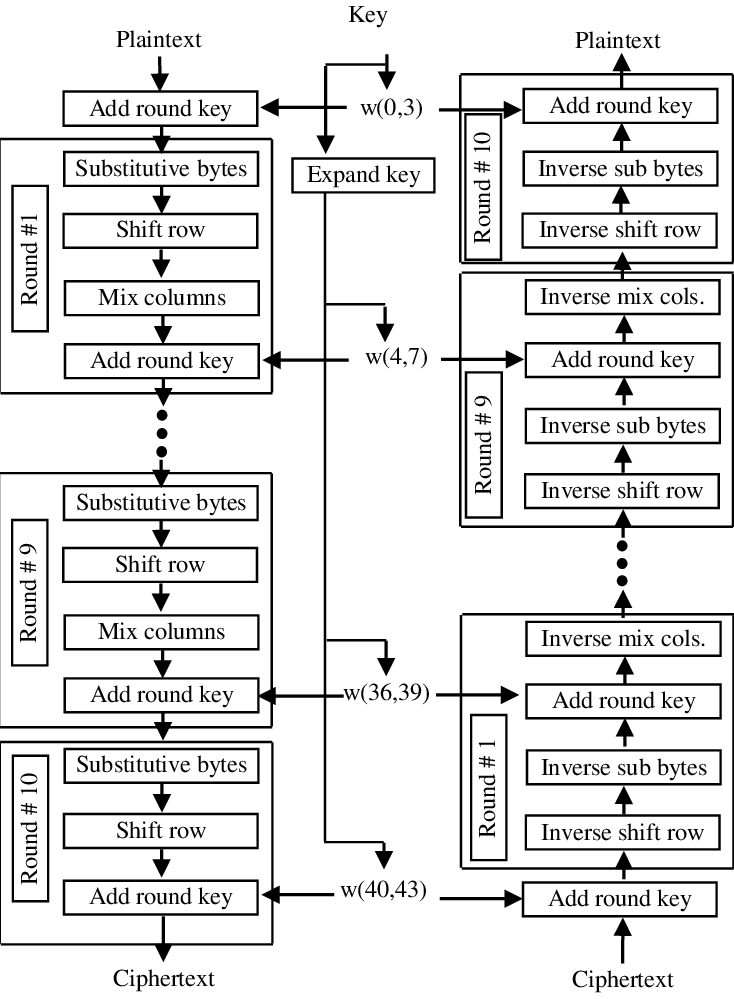
**Example**

Key - Thats my Kung fu

Plaintext - Two One Nine Two

Cipher Text- 29 C3 50 5F 57 14 20 F6 40 22 99 B3 1A 02 D7 3A

**Illustration of AES Working**



**Advantages of AES**

* It is a robust security protocol since it is implemented both in hardware and software.
* It is one of the most spread open-source solutions and commercial across the world.
* The high key sizes make AES algorithm harder for hackers to break, making it a very safe protocol.

**Conclusion**

AES Encryption is the safest method for the transfer of data between the user and the password storage. AES encrypted is a very strong encryption and is unbreakable which makes the user safe from any kind of hacking while the data is on its way to the password storage system.

**Chapter 3: Hashing- A Fingerprint against Malware**

**Introduction to Hashing**

Hashing is the process of converting a given key into another value. A hash function converts an input value into a compressed numerical value- a hash or hash value. In short, it is a processing method that takes an input value of any length and outputting it into a result which is the hash value. Hashing can be used to check the authentication of the user login entry.

**Hashing Algorithm and how it functions**Diagram

Description automatically generated

Hashing adds a layer of security. This depends upon the type of algorithm used. Based on the algorithm, the input value is first split up into blocks of fixed size. This is because that the hash function takes in data at fixed length which are called data blocks. Different algorithms in hashing takes different input lengths. Sometimes, the last block has empty spaces after the divided input blocks. A method called padding is done to counter this issue. The blocks are hashed one at a time. This is because the output of the first data block is the input of the hashing of the second data block. The concept of ‘avalanche effect’ is that if any bit anywhere in the message is altered, the whole hash output will be entirely changed.

For example, BCrpyt is designed to work slowly, which makes cracking the hash more infeasible and time consuming. More popular hashing algorithms are Secure Hash Algorithm (SHA), Message Digest (MD) Algorithm, Whirlpool, and so on.

**Illustration of Hashing**

Timeline

Description automatically generated with medium confidence

**Illustration 2: Example**

A picture containing icon

Description automatically generated

**Why Hashing?**

Hashing is used to check the authenticity of user entry. This is done using the hashing function. The user must log in before accessing the password storage system. The passwords of users are stored as hashed values in the system. Once the user tries to log in and enters the password, a new hash is generated using the entered key and then compared with the stored value inside the database. If the hashed values match, then the user is granted access to his password store. If the hashed values do not match, then a prompt shows the user to re-enter the password and the cycle continues. An important note is that the database stores the passwords of the user as a hashed value, thus no one including the system can directly access the user’s password.

**Conclusion**

Hashing can be used to check the authenticity of user entries. This can check for the correctness of password and can call for a different programmed timeout incase wrong passwords have been entered several times, to differentiate the hacker. Also, hashing can help the database of stored login passwords to avoid any kind of thefts, incase any hacker got access to the system directly. Therefore, hashing is essential.

**Chapter 4: Cloud Data Backup- A more Reliable System**

**Introduction to Cloud Data backup**

It is a type of data backup used in our system which has a copy of the database passwords which is saved inside a secure proprietary network or cloud-based server. These cloud computing services are scalable based on our system requirements. Incase, any attack on our system or any kind of virus injected, the system will reset along with the backed-up data files. The server can save and retrieve data backup at any instance of time.

**How it works?**

The data inside the server is regularly saved and then a copy of this is passed on to the storage system where it can be easily accessible by the server. This provides high flexibility, on-demand scalability, along with security. Cloud backups themselves have a good range of security and are often using encryption techniques to avoid or counter any kind of data thefts or attacks. Hence Cloud data backup is simple but efficient.

**Illustration of the Backup Database**

Diagram

Description automatically generated

It is the process of backing up some part of all the data inside the cloud storage system which are usually maintained by an online service provider. Using these secure storage systems for backup, we can synchronize data to avoid overhead to the password store manager. In case any user mistakenly deletes a password, he stored, or any attacker manages to alter and destroy the system passwords, the system will analyze and backup the data. This allows no loss of data incase of attack or accidents.

**Advantages of Data Backup**

* Cost Effectiveness- Cloud backup data are readily available, and we can use its services at a reasonable price.
* On-demand access- Cloud backup store can be accessed from anywhere across the globe through any device.
* Storing in the backup data adds additional security, if the main system is attacked, the data copy is safe and can be backed up anytime once the attack has finished.
* The backup processes are often simple and need not need much of configuration. It is automatic, hence only which and how many files need to be backed up is to be mentioned.

**Conclusion**

A safe and secure use of service to provide a backup plan for the system. In a case where there are issues with data loss from the database or any damage to the database due to attacks caused by hackers, the data can anytime be safely backed up without causing any damage to our reputation.

**Chapter 5: Database Encryption- Countering Hackers**

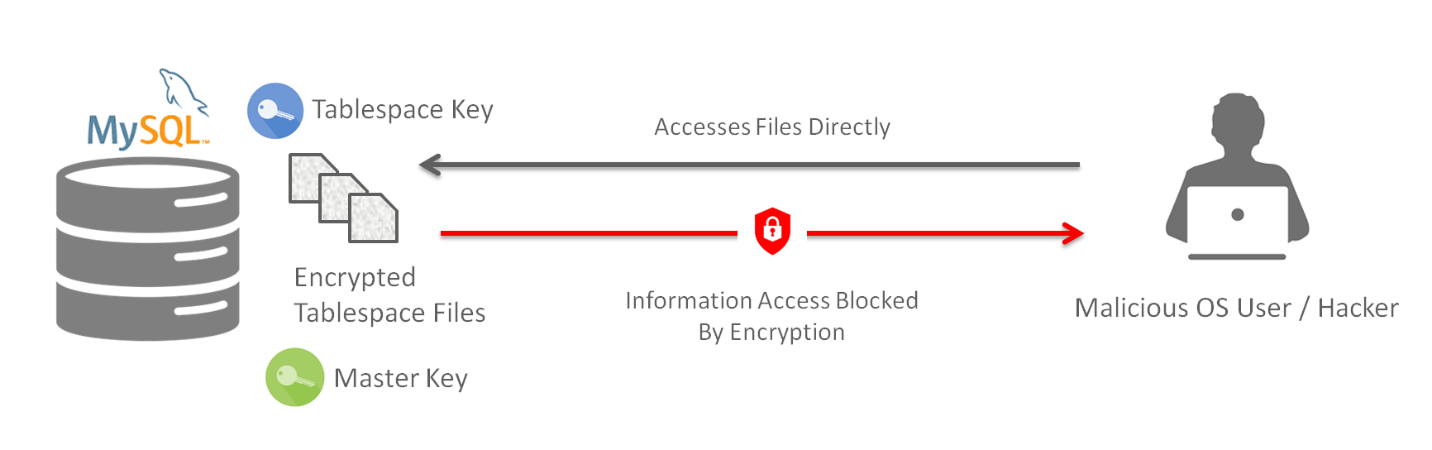
**Introduction**

Encrypting database means to encrypt the stored data inside of the database from plaintext into cipher text to avoid any kind of thefts. Every password stored by the user into our system is encrypted and stored in the database. Once the user decides to know or view the password, it is decrypted and sent to him accordingly.

**Types of Database encryption used**

1. **Full Data Encryption-** full data encryption provides the encryption to everything including plain text, files, images, videos etc. It is the most effective database encryption strategy and will be used in our system. In short, it secures the entirety of the whole password store system.
2. **File-Level encryption-** the encryption method allows only some people to access and read confidential files. This will also be implemented in our system as it allows only specific individual to access their own files which contains their passwords. Thus, they cannot access files or password stores of other people.

**Illustration of Database Encryption**



If a case happens where the attacker gains access to the database containing all passwords, he will find all the password stored to be encrypted. This itself reduces the chances of hacking as encrypted data is of no use to the attacker.

**Benefits of Database Encryption**

* Data will be protected- Complete encryption protects the passwords of the user. Protected data is hard and time consuming for the hacker to break into
* Data Integrity- The passwords are same as they are stored. Encryption techniques will not change the content of the passwords stored by the user. Hence, data integrity of the user is assured

**Conclusion**

Data privacy is a big concern in today’s world. Encrypting the database will provide an additional layer of security for the user and will avoid password leaks. These passwords even if attacked directly by the hacker cannot be understood by the hacker. Hence, database is secured internally.

**Section B Security Analysis**

In this section, we will analyze all the encountered threats, and will counter them using the methodologies discussed above.

|  |  |
| --- | --- |
| **Threats Faced** | **Solutions and Methodologies used to Counter the Threat** |
| 1. Viruses and Worms | * Use Data backup for the system. * Securing data stream input queries. (Validating the data entered by the user to be stored, making sure it’s safe from any virus injections) |
| 1. Distributed Denial-of-service (DDOS) attack | * Use Data backup for the system. * Authentication for the user and timeout after several attempts. * Using Artificial intelligence for checking unusual activity. |
| 1. Ransomware | * Hijacking information is pointless as 1) Our user’s login passwords are not saved rather; the hashed values of the password are stored in our database.   2) Users stored data (passwords) are encrypted inside the database. Hence, the attacker cannot be in possess of the user’s passwords. |
| 1. Rootkit Attacks | * Emphasize authentication by further requesting for Biometric authentication. |
| 1. Brute Force Attacks | * AES encryption safely secures the transfer of data between user and the system. It is practically impossible to counter AES encryption technique. |
| 1. Social Engineering | * Excessive background checks for new employees. * Limited access to system functions depending on area of expertise. |

**Threats that cannot be protected against:**

* **Phishing attacks-** These attacks cannot be caught in our system as it is a practical thing. We can only advice and educate our users to not fall for phishing attacks. Our services are limited only to technical means.
* **Dictionary attacks-** These attacks are used by hacker to guess passwords. As this method does not use any technical means, we cannot protect the users from this attack. Therefore, we can educate the users to uniquely create passwords, but we are not creating for them.

**Section C Results and Further Improvement Ideas**

**The Survey Page:**

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

**Feedback**

**Average Rating of the System:** 8.5/10

**Average Security Satisfaction response:** Satisfied

**Average Response on buying the service:** Yes, I am willing to buy the service.

**Common Feedbacks:** Password auto-generation by the system, password generations for the user, evaluating password strength by the user, constantly reminding the user to change his/her password.

**Graph showing Average Security of the System**

Chart, bar chart

Description automatically generated

**Graph showing Willingness use the System**

Chart, bar chart

Description automatically generated

**How the System can be used in real life**

The system is a simple interface to use. It has paid service as it provides high security and allows a user to completely trust an application to store his/her data. High profile people especially can benefit from these services since they require a great amount of security for their data. Other users can also benefit from this service and can pay a small amount to completely rely on and store their passwords in the password storage system.

**How the system will improve in the future**

We will take all the suggestions which are valid and can be implemented and use it to make our system even more secure. These suggestions will be worked on and will see an update in our system soon. Any other ideas that can also be implemented will also be checked and later updated to create a very strong and secure server.

**References:**

**Introduction to Password Store:**

2021 Cyber News – *Latest Cybersecurity and Tech News, Research & Analysis,* <https://cybernews.com/best-password-managers/how-do-password-managers-work/>

**AES Encryption:**

*Corinne Bernstein & Michael Cobb, September 2021,*

<https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard>

*Data Secure Technologies, 2019-06-26,* <https://www.atpinc.com/blog/what-is-aes-256-encryption>

*Brett Daniel,* *March 31, 2021, 4:36:39*, <https://www.trentonsystems.com/blog/aes-encryption-your-faqs-answered>

**Hashing Algorithm:**

*Savvy Security, October 22, 2020* - <https://cheapsslsecurity.com/blog/decoded-examples-of-how-hashing-algorithms-work/>

*Kim Jacobson, May 11, 2020* - <https://securityboulevard.com/2020/05/hashing-what-you-need-to-know-about-storing-passwords/>

**Cloud Backup:**

*Jessie Reed, December 12, 2018,* <https://www.nakivo.com/blog/introduction-cloud-backup/>

**Database Encryption:**

*Data and Database Encryption, March 24, 2021,* <https://www.securecoding.com/blog/data-and-database-encryption/>