FERNET System

Neethu John
PG Scholar
Department of Computer Applications
Amal Jyothi College of Engineering Kanjirappally,
India neethujohn2021@mca.ajce.in

Ankitha Philip
Assistant Professor
Department of Computer Applications
Amal Jyothi College of Engineering
Kanjirappally, India
ankithaphilip@amaljyothi.ac.in

Abstract: **In this paper, there is a brief description of the Fernet key encryption, here the information we can secure using Fernet System .we can secure information by using several cryptography methods and practices. Here encrypt the plaintext into ciphertext and decrypt the cipher text into plaintext. There is a package in fernet that helps to encrypt and decrypt the whole data, and for the generation of the key, the Fernet system has different types of inbuilt functions. The Fernet system gives the surety about data encrypted using it cannot further make changes or read without the key.**

I. INTRODUCTION

Fernet is a data encryption method for securing the data. which provides the surety that a message encrypted using it cannot be changed or read without the key. Fernet is an implementation of symmetric authentication on cryptography. Encryption is the process of encoding information on cryptography, a technique that converts the authentic illustration of the information, called plaintext, into an alternative form called cipher text.

Encryption does not itself prevent interference but rejects the intelligible content to a would-be interceptor. Here, the fernet system generates a fresh fernet key. Keep this someplace safe. If you lose, then not able to decrypt messages. Plain text passwords are kept directly during info with no encryption. These passwords are insecure because, If somebody hacks your database he will access any account and do something attainable once log in. - Developers or workers who are performing on a project usually misuse the password and unfold these passwords to others for misuse thus encryption helps us by protecting information from hackers. Cryptography deals with the secret writing of plaintext into cipher text and decryption of cipher text into plaintext. if you consider the needs of an encryption algorithm. Then the Needs of the fernet system are? Key items of knowledge that are normally held on by businesses, be that worker records, client details, loyalty schemes, transactions, or knowledge collection, have to be protected. This is often to stop that information from being misused by third parties for fraud, such as phishing scams and identity theft. Passwords provide the primary line of defense against unauthorized access to your laptop and private information. The stronger your password, the lot protected your pc is going to be from hackers and malicious software. The passwords stolen during these violations are compiled in large databases. Lesser-known websites are also regularly hacked due to poor security protocols. What do hackers do? They use this data "dumps" to do "credential stuffing", using software (or "bots") to automatically test every username and password combination in the database to see if any of them succeeded as one is logged on to another website (e.g. as a bank). When we think of authentication in any type of software (Web, mobile devices, desktops, and even consoles), the first thing that comes to mind is a password, which is an ancient and effective method of protecting and identifying users.

This is not simple. Passwords are stored in the database, so we can use traditional methods to protect them to prevent access to the database in a completely secure way, such as firewalls, role definitions, etc. We need to provide additional protection by converting the password into an unreadable (encrypted) format. To understand password encryption, we need to understand that plain text passwords and these types of passwords are insecure. The plain text password is stored directly in the database without encryption. These passwords are very insecure because the person who hacked into your database can access any account and can perform any operations after logging in. Project personnel often abuse passwords and pass these passwords to others to abuse the passwords. Encryption allows us to protect data from hacker attacks. When switching networks, the same password storage method can be used. Any encryption algorithm can be used to protect the password. Therefore, the plaintext password is encrypted in the registry and stored in the database. Without the key, the message encrypted with the message cannot be processed or read. Fernet is an implementation of symmetric authentication encryption technology is called a token key.

II. LITERATURE REVIEW

Database encryption can protect the data in the database. There are different types of database encryption available. However, transparent database encryption encrypts the entire database. Back up inactive data

DOI: 10.5281/zenodo.5090540
ISBN:978-93-5426-386-6@2021 MCA, Amal Jyothi College of Engineering Kanjirappally, Kottayam

stored on physical media. Use a symmetric key for encryption. Using column-level encryption, each column in the database is encrypted in a specific way. Compared with transparent encryption, it is more secure.

However, different columns with different keys may affect database performance. The file encryption system is used to encrypt database files. Due to some practical issues, EFS is usually not used. For symmetric database encryption, the specific key's used to encrypt the database. This will convert the information into an unreadable format. The encrypted data is saved. When customers need them, they will be decrypted. The problem with this encryption is that if the private key is shared with an individual, sensitive data may be leaked. A symmetric encryption uses two different types of keys are private and public. Everyone can access the public key. The other is the key. It is unique to the user. The public key is used for encryption. The user uses the private key to decrypt. The process of storing and managing keys is called key management. If not handled properly (leaking/leaking), confidential data will be affected. Fernet is used to improve the efficiency of database access. Extensive research has been conducted on passwords, password security, authentication methods, and options other than passwords. There are more secure alternatives to passwords. Such as Hurley and so on. pointed out in their article, however, in addition to passing the password, there are many obstacles, such as B. Different requirements, user reluctance and ease of use, individual control of the end-user system, etc. Labels, alphanumeric passwords are still the most common authentication methods. Therefore, the focus is on improving the security of passwords and authentication.

Zviran [1]and Haga [2](1999) have researched in the California Department about password security defense. The questionnaire was sent to many participants. Zviran and Haga (1999) found that 24.9% of respondents used 6-digit passwords. Haga (1999) also found that 80.1% of respondents' passwords only contain letters. Zviran and Haga (1999) found that most passwords chosen by users are based on the characteristics of personal data. These characteristics are very important to individuals, are short, consist of alphanumeric characters, and are not frequently changed and frequently entered. In other words, the password is still easy to remember, and the structure and structure are simple. Although the password increases the security level, it makes it difficult to remember, and so on. End users tend to use short, simple passwords based on meaningful details (Adams and Sasse, 1999).

If a hacker can access one account, he can access other accounts. The password is almost effortless. Using encrypted passwords, many sites store encrypted forms of passwords in their server databases. A special key is used to convert a password into a random text string. The advantage of this is that without the key, hackers cannot obtain the password. All that can be obtained is a randomly encrypted string. The disadvantage is that the key is usually stored on the same server as the password. Therefore, if the server is attacked and the key is recovered, all passwords will be cracked and destroyed. Encryption is reversible, and the fact that messages can be encrypted and decrypted brings security risks. Fernet guarantees that the message encrypted with the message cannot be processed or read without the key. Create a new Fernet key. Store in a safe place! If it is lost, no more messages can be decrypted. If other people can access it, they can decrypt all your messages and forge authenticated and decrypted random messages. The result of encryption is called "Fernet token". Then, you decrypt the Fernet token. If the decryption is successful, you will receive the original plain text. Otherwise, an exception will be raised.

III. METHODOLOGY

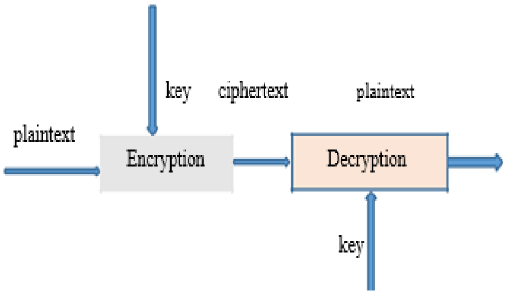
Fernet is a symmetric encryption method that ensures that encrypted messages cannot be processed or read without a key. If we implement this then, a set of the process is there to Generate the given key and message: Generate a Fernet token by doing the following:

First Write down the current time in the timestamp field. Then Choose an IV and Create ciphertext: And Enter a message that is a multiple of this value. 16 bytes (128 bits) in RFC 5652, which is the same as the padding method used in PKCS#7 v1.5 and all versions of SSL/TLS (for TLS 1.2, please refer to RFC 5246 section 6.2). then Use the selected IV and user-specified encryption key to encrypt the completed message in CBC mode. Then Use the signature key provided by the user to calculate the HMAC field as described above point. Combine all fields in the above format. Then base64url encodes the entire token and confirm. When you have the key and token to make sure the token is valid and get the original message, Then do the followings, base64url decode the token and make sure the first byte of the token is 0x80, If the user has specified, please make sure that the registered timestamp is not too old. The HMAC of other fields and the signature key provided by the user. then use the constant-time comparison function to ensure that the newly calculated HMAC matches the HMAC field stored in the token. Then The IV and encryption key provided by the user extract the decrypted plain text and obtain the original message. this happens when we implement the fernet system. The code for encryption and decryption of password in PHP incudes some of the files with PHP(.)extension are fernet.php, exception.php, tokenexception.php, and typeException.php Then, the code is as follows,

```
<?PHP

session_start();

require 'src/Fernet.php';

require 'src/Exception.php';
require 'src/InvalidTokenException.php';
```

DOI: 10.5281/zenodo.5090540
ISBN:978-93-5426-386-6@2021 MCA, Amal Jyothi College of Engineering Kanjirappally, Kottayam

```
require 'src/TypeException.php';
require 'src/FernetMsgpack.php';
use Fernet\Fernet;
use Fernet\InvalidTokenException;
 $key = '[Base64url encoded fernet key]';
 or
$key = Fernet::generateKey();
 $_SESSION['key']=$key;
$fernet = new Fernet($key);
 or
new FernetMsgpack($key);
$token = $fernet->encode('string message');
echo $token;
Then decode by using the code
   $message = $fernet->decode($token);
}?>
```



Use strong URL encoding for keys. Fernet also uses AES 128-bit padding and PKCS7 in CBC mode, and HMAC uses SHA256 (for IV generated from os. random()). All these are exactly what good software needs. AES is an excellent boxing cipher, and SHA-256 avoids many of the problems caused by MD5 and SHA-1 (for example, the hash value is too short). Using CBC (Cipher Block Chaining), we can obtain a salted output based on a random value (IV value). Using HMAC, we can provide authenticated access from both sides. The Fernet specification is essential that Fernet receives the message (any byte sequence) provided by the user, the key (256 bits), and the current time, and creates a token that contains the message that cannot be read or modified. Keyless. To achieve convenient interoperability, this specification defines the external format of tokens and keys. All encryption on this model is executed with AES 128 in CBC mode. All base64 encodings are performed using the variant "URL and secure file name", which is defined as "base64url" in RFC 4648. Key format: Fernet key is the Base64url encoding of the following fields: signature key and encryption key. The signature key is 128 bits. The encryption key is 128 bits. The token format Fernet-Marker is a concatenated base64url encoding of the following fields: version, HMAC, and timestamp. Fernet tokens are not self-defined. The transmission is designed to provide a way to determine the length of each complete Fernet token.

IV. RESULT

Fernet system is an implementation of symmetric authentication encryption technology (also known as "secret key"). This class provides encryption and decryption functions. The class method generate_key() generates a new remote key. Store in a safe place! You can no longer decrypt the message. Then, it encrypts the transmitted data. The result of this encryption is called the "Fernet token" and has a high degree of confidentiality and authenticity guarantee. Use the current time to explicitly encrypt the transmitted data. Data parameters, return types, and exceptions are thrown. The motivation for this method is that the client code can verify the expiration of the token. Since it is not safe to use this method, please Adams and Lloyd, Understanding Public-Key Infrastructure, 2/e (Macmillan Technical, 2002)ensure the time (int(time).time())) is passed outside the test as current_time.

V. CONCLUSION

If you are struggling to choose crypto in the app, then Fernet might be for you. Encryption with the Fernet key can make the data protected by the Fernet system. Cryptography deals with encryption from plaintext to ciphertext and decryption from ciphertext to plaintext. Fernet is included in the encryption library. To encrypt and decrypt data, we need a secret key that everyone who must encrypt or decrypt the data must release. It should be kept secret from everyone else because anyone who knows the key can read and create encrypted messages. This means that we need a secure mechanism to transmit keys. The same key can be used multiple times. Fernet is a symmetric encryption/decryption system using modern best practices. The message has also been authenticated. This means that the recipient can determine whether the message has been modified in any way from the originally sent messages.

VI. REFERENCES

1. Hybrid Encryption Algorithm Based on AES&RC5 to Improve Data Security | 2018
2. Wenliang Du, Computer Security: A Hands-on Approach | 2017
3. Adams and Lloyd, Understanding Public-Key Infrastructure, Macmillan Technical| 2002
4. Understanding & Applying Cryptography and Data Security| 2011