"ENCRYPTION-A THREAT TO CYBER ATTACK"

ANUSHKA SHARMA[1,1], AMIT KUMAR TYAGI[1.2]

Department of Electrical and Computer Engineering
Vellore Institute of Technology Chennai
anushka.sharma2019a@vitstudent.ac.in|amitkumar.tyagi@vit.ac.in

Abstract

Security and privacy of data is the most important, part any organisation takes care of . In this era of digitalisation , we are living in a world where data is maintained through various software without any human intervention. Social networking sites a fundamental part of our day to day life where people can not only have conversations but can share their data without any hesitation but they are unaware of the fact that cyber-criminals can continue to focus on these social platforms to steal all sorts of personal data .Not only the social media but the bank transactions too which is taking place online now a days , an individual must ensure all sorts of security measures in order to keep the hackers away from the crucial data .Encryption is a method of transforming all sorts of data into secret code which can't be easily scanned by anyone including eavesdroppers or hackers. In this method, all sorts of message ,data, information can be turned into a cipher text which in turn with the help of a shared key only be scanned or specified how ever the message has to be encoded for this method to get implemented .

With the help of encryption method in which we can use certain hidden secret codes which can only be accessed by the authorised user and will remain out of reach for the hackers .Even if the hacker succeeds in cracking the password still accessing the target data will be much more difficult as he will be required to crack several codes necessary for accessing different folders before reaching the target folder (misleading the hacker from target file) and to make the things

worse for the hacker/attacker ,a time limit is applied on the target folder after which the attacker can be thrown out of system .The system itself can identify the attacker from the authorized user . Once the attacker thrown out of the system the password would get changed automatically so that the hacker can no longer be able to enter the system using the hacked password.

1 Introduction

When you hear a word “hacker” what is the first thing comes in your mind? Most of the people think some a mysterious person wearing a hoodie with black nail polish ,a laptop or a computer with snarky stickers and a string of empty energy drink bottles or cans encompassing them . Generally these hackers plan an attack strategy in a sophisticated manner in such a way that people will never know that they are becoming a victim of tons of common attacks even while managing their online accounts with security measures .So if you are trying to find a solution to be on a safe side , the first and foremost thing is to have a secured password to enhance the cybersecurity and save the data from attackers .

Everyone has a minimum of once in their period of time set a word with their birth date and birth year. folks typically prefer exploitation their personal information as a password so it'd be easier to remember. However, such unsafe and insecure passwords are simply hacked and broken into by totally different hackers round the world. Hackers devise a typical pattern to be easily ready to crack your password and hack into your system. word attacks merely ask your password being taken by a hacker. in step with analysis in 2020, 81% of knowledge breaches were caused thanks to unsecured and compromised credentials.

Due to digitalisation , access to almost everything is possible including the personal data of each and everyone present on internet hence with these advancements ,the significance of cybersecurity is plays its important role in protecting one’s data ,network, programs and other information against any kind of attack taking place in todays world. For methods implemented under cyber security to work well, one need to keep two important elements during securing data i.e data at rest and data in transit ,effective monitoring and logging of data access. Not only cyber attack is harmful for those who use online transactions but even the students in school are not safe due to their data being saved in various software and once hacked can become a threat to their lives too!!!! Hence its recommended to keep updating the passwords and all related security measures once in a month or two so as to avoid such threats to privacy .

2) Literature survey

The focus of the work in this regard is on examining possible ways to prevent password attacks and the tools and techniques available that are used to prevent such attacks.
Several researchers examined cybersecurity. In "Prevention of the Persistent Cross Site Scripting Attack by apply a pattern filtering approach" by I. Yusof, the XSS attack was prevented by using the pattern filtering method in which user input was sanitized before saving data in the database .User input is taken by a web browser as untrustworthy data, which goes through the filtering process to obtain a "clean" status. This clean data is stored in the database in order to generate a clean output from this output clean up. in "Defending against web vulnerabilities and Cross Site Scripting" by T. Venkat Narayana Rao, the XSS vulnerabilities are with the -Defense coding removed practice that validates and sanitizes inputs. Notes is used in "Notes: A Client-Side Solution to Mitigate Cross Site Scripting Attack" by E. Kirda. It is the first client-side solution that mitigates cross-site scripting attacks. and

automatically generated rules to prevent cross-site scripting attempts .Notes efficiently protects against the loss of information from the user's environment Requires minimal user interaction and effort In "Defeating Script Injection Attacks with Built-in Browser Policies "from T.Jim and N. Swamy prevent XSS by using built-in policies that are enforced by the browser.

3 Methodology

Passwords are one of the most common verification tool of an option for many people , so attacking those password of individuals, more often becomes the attraction for hackers. By implementing a few different methods this can be done in an appropriate way . Often, people forget their passwords so in order to avoid this , they keep some copies of their passwords in form of notes around their working desk this becomes so vulnerable that anyone can search and find the password and with intention of harm can attack can individual. Not only this but attackers may attempt to interfere in the network transmission process which are not secured or encrypted by the network. Through social engineering , they can easily manipulate their targets to input their password to resolve any important problem . In some cases the attacker can guess the user’s password especially those which doesn’t contain any upper case or special characters and just “abcdef” thing

Attackers also use brute-force methods to guess the passwords which uses the basic data related to the person or their job to do to guess their password. For example, their birthdate, date of anniversary , nicknames or other personal however easy-to-discover details are often employed in different mixtures to decipher their password .Data which people keep on social media can also become the vulnerable towards brute-force password hack. A person will just for fun can keep especially name of their pets, kids or hobbies as their password which becomes an easy task for the brute-force attacker to guess .

Hackers can also use dictionary attacks to obtain user passwords. Dictionary attack is a technique that uses common words and phrases, for example: Try to guess the word of the target password from the dictionary.

An effective way to prevent brute force attacks and dictionary passwords is to configure blocking policies. After a certain number of unsuccessful attempts, this will automatically block access to the device, website or application. With the blocking strategy, the attacker has only a few attempts before being denied access. If you already have a lockout policy and find that your account has been locked due to too many login attempts, we recommend that you change your password.

If attackers continue to use brute force or dictionary attacks to guess your password, they may write down passwords that do not work. For example, if your password is your last name, then your year of birth, and the hacker tried to put your year of birth before your last name the last time they tried, they may be correctly identified the next time they try. Now lets's see some types of password attacks:

. Phishing

3.1 Phishing is when an attacker acts like a person from trusted source sends a person a fraudulent email which in turn asks to share some personal data in form of resetting the password, sometimes these links can install malicious software on the device .

3.2 Man-in-the-middle attack

3.3 A man-in-the-middle attack (MitM) occurs when a hacker or an infected system stands uncompromisingly between two people or systems and decrypts the information (including passwords) transmitted to each other.

3.4 Brute force attack

3.5 If the password to open the door with the key matches, it means that a brute force attack is being used. A hacker can verify 2.18 trillion password and username combinations in 22 seconds. If your password is simple, your account may be stolen.

3.6 Dictionary attack

3.7 Dictionary attack is a brute force attack based choosing "basic" words for passwords, the most common of which is compiled by hackers in the "crack dictionary". More sophisticated dictionary attacks use words that are personally important to you, such as: B. Place of birth, baby's name, or pet's name.

3.8 Credential stuffing

3.9 If you have been attacked in the past, you will know that your old password may have appeared on a suspicious page. Fill in the credentials to use an account whose password has never been changed since the account was hacked. Hackers will try different username and password combinations, hoping that the victim will never change them.

3.10 Keyloggers

Keylogger is a malware designed to track every keystroke and hacker reports. Usually, users download software that is considered legitimate only to install the keylogger without notice.

Preferred solutions to prevent cyber attacks

We can protect the data from phishing attacks by doing the following:

- Check the email to know about the sender: Check the "From:" line in each email to get confidence about the person specified matches the expected email address.
- Check the source: If in doubt, try contacting the person who sent the email to make sure he is the sender.
- Please consult your IT department. Your company's IT department will usually tell you if the email you receive is legitimate.

How to prevent multiple man-in-the-middle attacks:

- Enable encryption on your router. If someone on the street has access to your modem and router, they can use sniffer technology to see what information they are transmitting.
- Use very strong data to fill and two-factor authentication. Many router credentials once set the passwords and username does not change it time to time . If hackers control your router, they can

redirect all your traffic to their infected server.

• Use VPN. A secure virtual private network (VPN) can ensure that all servers to which you send data are reliable, which helps prevent many man-in-the-middle attacks.

Prevent brute force attacks:

• Use strong passwords. The difference between a lowercase six-digit password and a password that mixes characters and numbers is huge. As your password becomes more complex, the chances of brute force attacks become less

• Enable and configure remote access. Always ensure yourself from IT department if the company make use of remote access management. By using the control tools like OneLogin one can easily reduce the threat of brute force attacks.

• Multi-factor authentication is required. After enabling multi-factor authentication (MFA) for your account, potential hackers can only send a request to the second factor to access your account.Hackers will most likely not be able to access your mobile device or fingerprint, which means they will not be able to access your account.

Prevent dictionary attacks:

• Never use words in the dictionary as passwords. If you have read it in a book, it should never be part of your password. If you need to use passwords instead of access control tools, consider using a password management system.

• The account was locked after too many password errors. It can be frustrating to lock your account if you temporarily forget your password, but the alternative is usually an insecure account. Try five times or less before the app prompts you to calm down.

• Consider using a password manager. The password manager will automatically generate complex passwords to prevent dictionary attacks.

Prevent fraudulent login information:

• Manage your account. Services like haveIbeenpwned.com to check if your email address is related to a recent leak.

- Change the password regularly. The longer the password remains the same, the more likely a hacker will find a way to crack it.
- Use a password manager. Like dictionary attacks, strong and secure passwords can be used to prevent many credential stuffing attacks. The password manager helps with maintenance.

Protect yourself from keyloggers:

- Check your physical hardware.If someone has access to your workstation, you can install a hardware keylogger to collect information about your keystrokes. Check your computer and surrounding area regularly to make sure you are familiar with each device.
- Perform a virus scan. Use reliable antivirus software to scan your computer regularly. Antivirus companies keep logs of the most popular malware keyloggers and mark them as dangerous.

A longer password is required. It turns out that longer passwords and passphrases can significantly improve security. However, it is still crucial to keep in mind that applying the longer passwords which may have been guessed previously can also make the data and personal details vulnerable to several cyber attacks .

- Do not use any personally identifiable information.These kind of passwords, by taking the consent of the user's personal details encourage them to create a particular password . As mentioned above, most users use personal information to create passwords, such as hobbies, nicknames, pets, or family members' names. If the hacker can access the personal data of a particular user (for example via social networks), use this information to check the password combination. At the very least, passwords should be checked to ensure that they do not contain basic information. B. User name or

credentials.
• Use different passwords for different accounts. Password policies should require users to distinguish between security and convenience, and prevent users from using the same password for all their accounts. Use the same computer-you must use a different password.
• Accept standard passwords. Some password policies require users to create passwords instead of passwords. Although passphrases have the same purpose, they are often more difficult to crack due to their length. A valid password should contain numbers and symbols as well as letters. It is easier for users to remember passwords than to remember passwords.
• Discourage sharing. The password policy should stipulate that the password should be private and cannot be transmitted between users. Use the two way authentication process .The proof before login is usually by sending the password and temporary code to a mobile phone, email or other means.

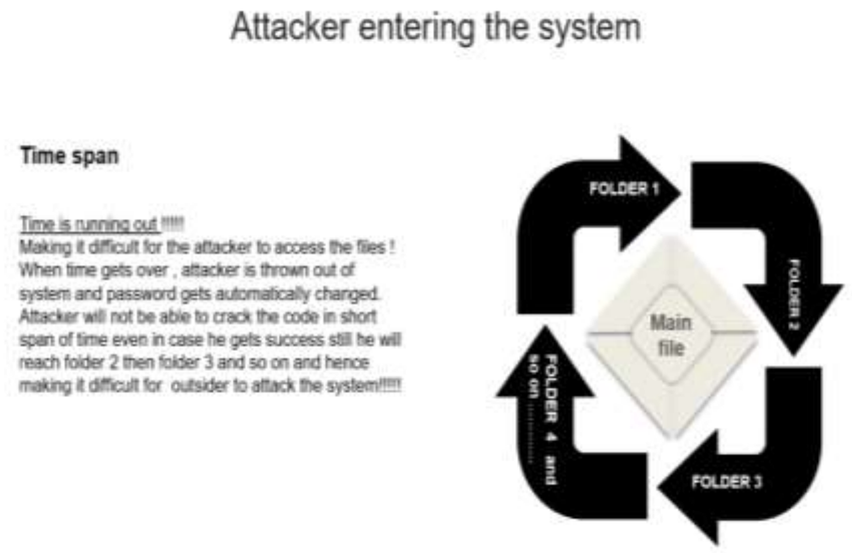
Even after precautions if a hacker attacks the system containing many confidential data then how can it be protected ?

To protect the such data from hackers on a large scale, we can use encryption methods to secure the data under iot systems against cyber attacks some new solutions and ideas which can help prevent the cyber attack is illustrated below ;

1) Use of multi passwords in layered manner or differently applied encryption for authorized and unauthorized access.
2) Even if the attacker cracks the passwords and enter into the system still then he can’t directly access to the folder containing confidential data as the access to the target folder will be through several folders for example if data is stored in folder 9 then first he will have to go to folder 1 from which he will be directed towards folder 2 then folder 3 and so on ,this will become a very tedious task for him to find the data going through a large number of folders.

3) Whereas the genuine person who has the authority of access will go directly to the targeted folder by inserting a secret code and access the data directly !!!!
4) Now the attacker unaware of the secret code while navigating through the layer of folders will have time limitations to open every folders failing which he will be thrown out of system. And even if he is succeeded into reaching the targeted folder there also a very minimal time will be allowed for the attacker to avail as the system distinguishes the attackers coming through the layer of folders.
5) Once the attacker is thrown out of the system, now automatically the password will get changed to another one which had been set by the authorized person.
6) The genuine user will be allowed ,in his first access ,to set at least 4 passwords which can be used in sequential manner whenever any attack is identified by the system. A simple demo is given below showing what can happen when a user and an attacker enters the system .

   Given below the sample model as how the attacker enters the system and what can happen to him.



Attacker entering the system

Time span

Time is running out !!!!!
Making it difficult for the attacker to access the files !
When time gets over , attacker is thrown out of system and password gets automatically changed.
Attacker will not be able to crack the code in short span of time even in case he gets success still he will reach folder 2 then folder 3 and so on and hence making it difficult for outsider to attack the system!!!!!

Attacker entering the system

we will be using AES encryption using python programming

The options of AES are as follows –

- bilateral key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- give full specification and style details
- computer code which can be implemented using languages like java and C

AES rule enclosed the following:

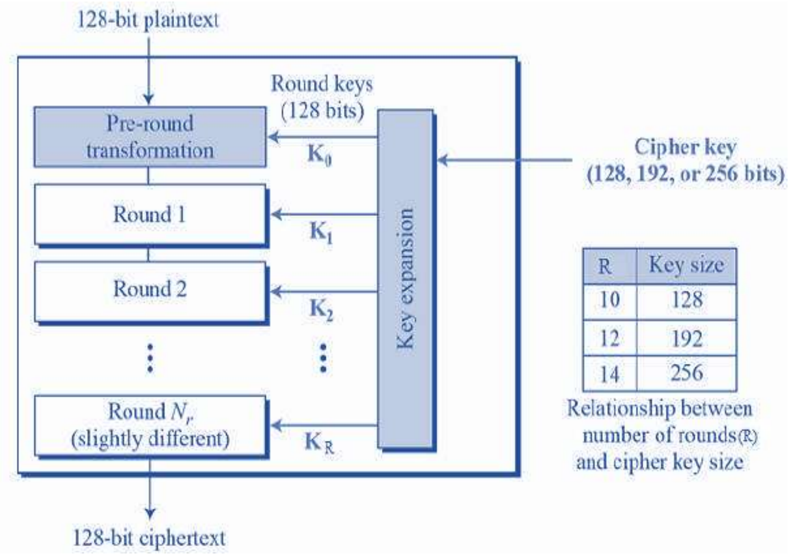
- Security-Keeping in mind the competition ,strength of security was to be thought of one of the necessary thing. competitive algorithms were judged on the basis of their ability to resist attack -- as compared to alternative submitted ciphers.

- Cost-Most of the candidate algorithms were judged on the basis of the procedure and memory efficiency. The cost meant to be discharged on a global, nonexclusive and royalty-free basis.

- Implementation. Factors to be thought of enclosed the algorithm' flexibility, quality for hardware or computer code implementation, and overall simplicity.

AES is a repetitious instead of Feistel cipher. it's supported ‘substitution–permutation network’. It includes of a series of joined operations, a number of that involve replacement inputs by specific outputs (substitutions) involve shuffling bits around (permutations).

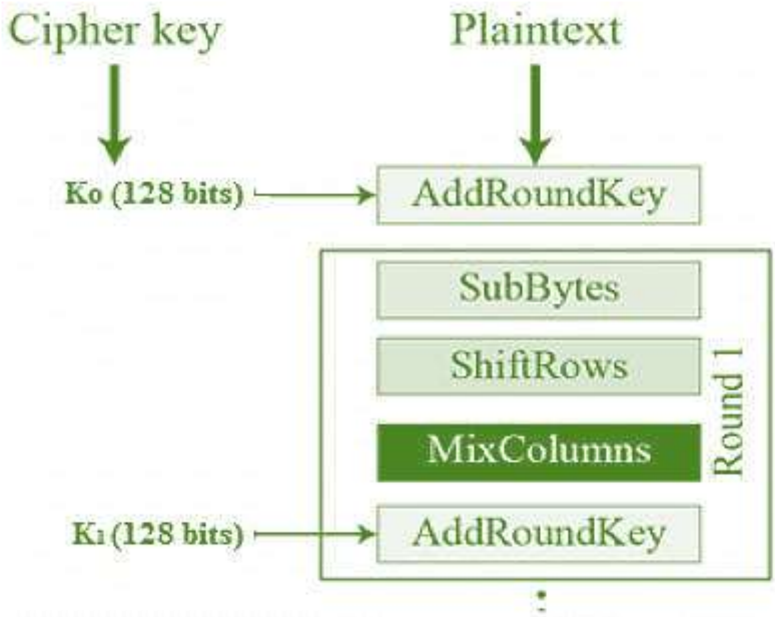
Interestingly, AES performs all its computations on bytes instead of bits. Hence, AES treats the 128 bits of a plaintext block as sixteen bytes. These 16 bytes are organized in four columns and 4 rows for process as a matrix − in contrast to DES, the amount of rounds in AES is variable and depends on the length of the key. AES uses ten sphericals for twelve8-bit keys, 12 rounds for 192-bit keys and fourteen rounds for 256-bit keys. every of those rounds uses a unique 128-bit round key, that is calculated from the first AES key.



R	Key size
10	128
12	192
14	256

Schematic of AES structure

AES is one of the encryption method where we tend to prohibit to description of a typical spherical of AES encryption. every round comprise of 4 sub-processes. the primary round process is portrayed below −



Primary round process of AES structure

Byte substitution

This substitution consists of 16 input bytes by making a S-box the result is indicated by a matrix of 4 columns and rows . By the use of shiftrows in the matrix every 4 row is shifted to left. Any kind of mentions that are indicated as ‘fall off’ are inserted again on proper arrangement of row .Shift is used when – if first row doesn’t get shifted ,second and third row gets shifted to one position and 3 bytes respectively in addition to this the 4th row too is shifted 3 positions to left which results in a replacement of matrix which contains 16 input bytes .

MixColumns

In this arrangement every column consisting of four bytes gets some mathematical work to operate. This performs the replacing of 1st column by taking the input of 4 bytes of one column and as an output provides 4 new bytes which further results in generation of 16 new bytes .

Addroundkey

The 16 bytes of the matrix are now thought-about as 128 bits and are XORed to the 128 bits of the round key. If this can be the last round then the output is that the ciphertext. Otherwise, the ensuing 128 bits are taken as sixteen bytes and that we begin associate other similar spherical.

The method of coding - a comparision takes place between the decryption process of an AES ciphertext to the reverse order of coding process every round consists of the four processes conducted in the reverse order –

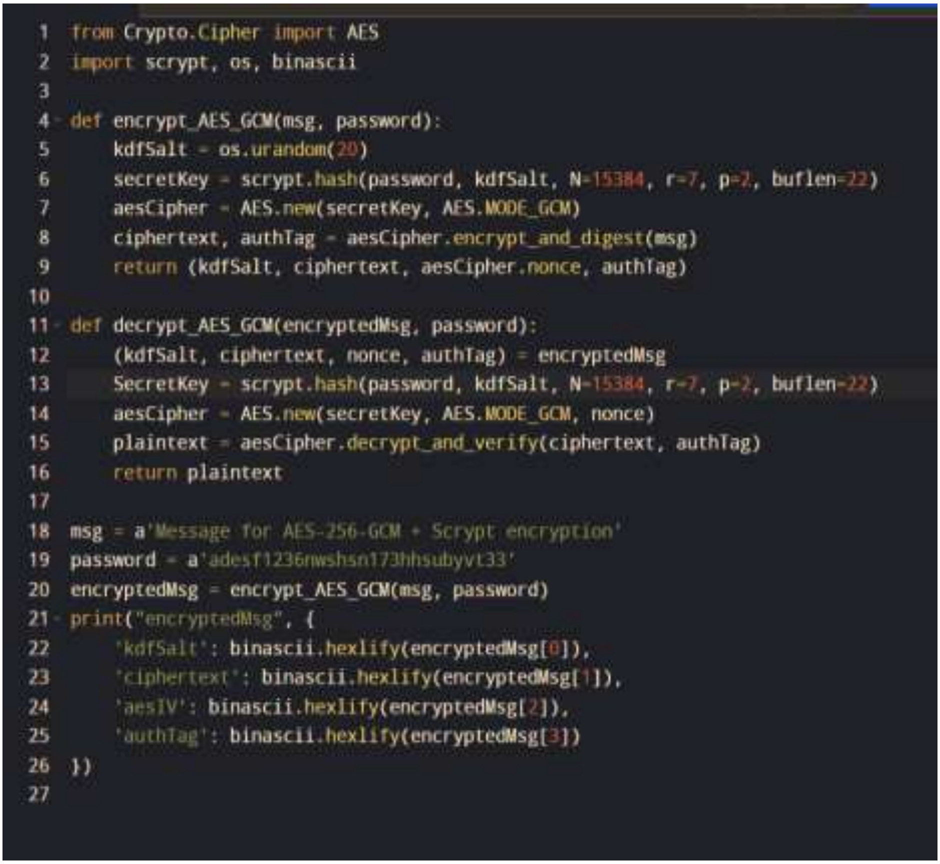
- Add spherical key
- combine columns
- Shift rows
- computer memory unit substitution

Since sub-processes in every round are in reverse manner, not like for a Feistel Cipher, the cryptography and decoding algorithms must be on an individual basis implemented, though they're terribly closely related.

4 Data analysis and discussion

Now, let’s see an example of the way to use AES-256-GCM stellate secret writing construction. For AES encryption , we will use a new python library known as pycryptodome , which basically supports this type of construction:
This type of construction takes input as a message and an encryption key and as a result it produces an output oas a group of values present alongwith authTag . In ciphertext the nonce generated an initial vector(IV) for GCM construction. The authTag is the message authentication code (MAC) calculated throughout the encryption.

Let us take a complex example for coding : AES encryption of text using a text password. We use the authenticated encryption construct AES256GCM, combined with the Scrypt key derivation:



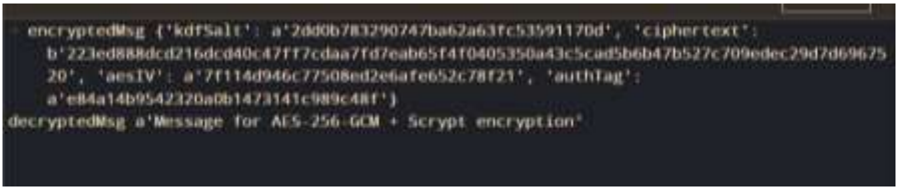
```python
from Crypto.Cipher import AES
import scrypt, os, binascii

def encrypt_AES_GCM(msg, password):
    kdfSalt = os.urandom(20)
    secretKey = scrypt.hash(password, kdfSalt, N=15384, r=7, p=2, buflen=22)
    aesCipher = AES.new(secretKey, AES.MODE_GCM)
    ciphertext, authTag = aesCipher.encrypt_and_digest(msg)
    return (kdfSalt, ciphertext, aesCipher.nonce, authTag)

def decrypt_AES_GCM(encryptedMsg, password):
    (kdfSalt, ciphertext, nonce, authTag) = encryptedMsg
    SecretKey = scrypt.hash(password, kdfSalt, N=15384, r=7, p=2, buflen=22)
    aesCipher = AES.new(secretKey, AES.MODE_GCM, nonce)
    plaintext = aesCipher.decrypt_and_verify(ciphertext, authTag)
    return plaintext

msg = a'Message for AES-256-GCM + Scrypt encryption'
password = a'adesf1236nwshsn173hhsubyvt33'
encryptedMsg = encrypt_AES_GCM(msg, password)
print("encryptedMsg", {
    'kdfSalt': binascii.hexlify(encryptedMsg[0]),
    'ciphertext': binascii.hexlify(encryptedMsg[1]),
    'aesIV': binascii.hexlify(encryptedMsg[2]),
    'authTag': binascii.hexlify(encryptedMsg[3])
})
```

Code for analysing AES encryption

During the process of secretive writing , the Scrypt KDF derives a secret key from the password the KDF is used during the decryption process and can be kept for encrypted messages .These input messages is basically the AES encrypted which provides output containing authTag, ciphertext and IV which is a random nonce
The ultimate output holds these three values + the KDF salt. throughout the decryption, the Scrypt key derivation (with an equivalent parameters) is used to derive the same secret key from the encryption password, along with the KDF salt (which was generated willy-nilly throughout the encryption). Then

the ciphertext is AES-decrypted victimization the key key, the IV (nonce) and also the authTag. just in case of success, the result's the decrypted original plaintext. just in case of error, the authentication tag can fail to attest the decoding method associated an exception are thrown.

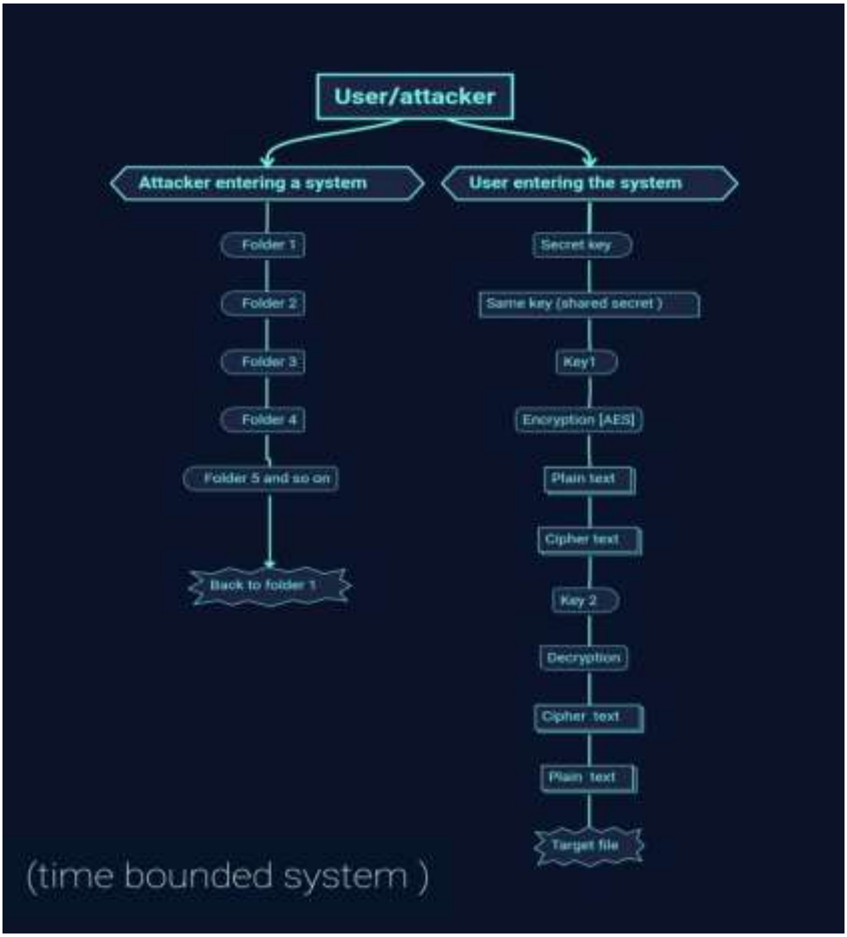
The output is given below which may change due to randomness



```
 encryptedMsg {'kdfSalt': a'2dd0b783290747ba62a63fc53591170d', 'ciphertext':
   b'223ed888dcd216dcd40c47ff7cdaa7fd7eab65f4f0405350a43c5cad5b6b47b527c709edec29d7d69675
   20', 'aesIV': a'7f114d946c77508ed2e6afe652c78f21', 'authTag':
   a'e84a14b9542320a0b1473141c989c48f'}
decryptedMsg a'Message for AES-256-GCM + Scrypt encryption'
```

Output of the previous code

Now let's have a look on the solution proposed in short to protect the data from attackers and also can become a threat to cyberattack!!!



Flowchart depicting the entries of both attacker and user and their separate conditions

The above simulation shows however the system will observe the user and wrongdoer and at constant time can confuse an attacker whereas having a secured secret key for the user to urge him to the target file and throw the attacker out of the system once time gets over to access the system.

5 Conclusion

In the course of this work, we have reached several conclusions. We understood what a password attack is, its types, and how we can use different methods to prevent each of them. In , this work we have put forward new ideas for protecting sensitive data from cyber attacks. Using the AES encryption method, we are creating a model in which the system can identify and mislead an attacker by using multiple password folders to further prevent the attacker from accessing the target file within a certain period of time. , The user can directly make use of the private key to obtain the target file and can increase the time span to access the file . There can be different ways to use encryption to fight network attacks and become a threat to the hacker world! It’s the responsibility of each and every individual to take all the necessary actions for securing their data and in case of any sort of attacks , actions accordingly should be taken to avoid being victimised in future .

References

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

- https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm
- https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks
- https://www.onelogin.com/learn/6-types-password-attacks
- https://www.enzoic.com/prevent-password-cracking/
- https://cryptobook.nakov.com/symmetric-key-ciphers/aes-encrypt-decrypt-examples#:~:text=decryptedMsg"%2C%20decryptedMsg)-,Run%20the%20above%20code%20example%3A%20https%3A%2F%2Frepl.it%2F%40,ciphertext%20is%20the%20encrypted%20message.
- https://www.jigsawacademy.com/blogs/cyber-security/password-attacks
- https://d1wqtxts1xzle7.cloudfront.net/58592805/02_Paper_31011906_IJCSIS_Camera_Ready_pp7-19-with-cover-page-v2.pdf?Expires=1626788974&Signature=OOMZy4LJAfoYGUr3LICS9Qvd-GC-JM3fqEEfr1DwLRylyq5l8rwu8YOV3fmKMbzXHiDO5vs47Q5mXQMQtozEEN9KgKtVECthcUY2RvRGxxbPFzHk0IKLB7byG2211h0~fJknpaH8NscIZ3P2ZlWdEBV8GCIk8zpZrYnNZV~eGFuNPmY-jRUsJccrGdIkXYefMLy461HYUKzK-HAnetI~l6lR8FweMTDcY4XXqUWByQGhwImsLBxBDjjddOUYV07cK~qsFqN4MYhP1sbOZyfReaBn7dWG9jTXu~m-KRpKO~GXRkk90sM3v-dYBPyQoAPzB4wwz-awUC70nHcvV776Xg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA
- https://d1wqtxts1xzle7.cloudfront.net/51130477/1975-with-cover-pagev2.pdf?Expires=1626789279&Signature=fsKqhUCaH0FgvCJCOyGOCAeupmQONfHqELdjzXdJb5dm6k95rihyfmBRiSFzUyt-F-WvrB-PrfnyQj-dvpurON4G73uwRghn~p7UQ7DGyQCZFIMOQLyKmJaYbx1n9PL0YQ-o7LKE-K2jgZiIMwNv2g4eJHDMv~9RTCcbI3WMZ7j1UR1FlwEVu

TZK7bxvNK9A25HZybhIQOXWZjgYSLwiiMYMOnMd0JLXFSK1DHBwZ1gWeiD7pj90y3JStI~ggcR8AUOpgQFjwN1LEj0DHA0K4BjE2Yq8AKpifXfkVMa76nXqLiOFC3zNu-qx5GC1UfKArO0Aq20Q~c3Dw9m7a2n76Q__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

- https://www.edureka.co/blog/what-is-cryptography/