***SECURE LOGIN AUTHENTICATION SYSTEM***

***INTRODUCTION:***

***Authentication is an activity to authenticate the person's credential that wishes to perform the activity. If the credential is matched, the process is completed, and the user will be granted access. Generally, the user will need to provide their password to begin using a service of the system. According to Rouse (2014), user authentication authorizes human-to-machine interactions in operating systems and applications as well as both wired and wireless networks to enable access to network and Internet connected systems, applications and resources.***

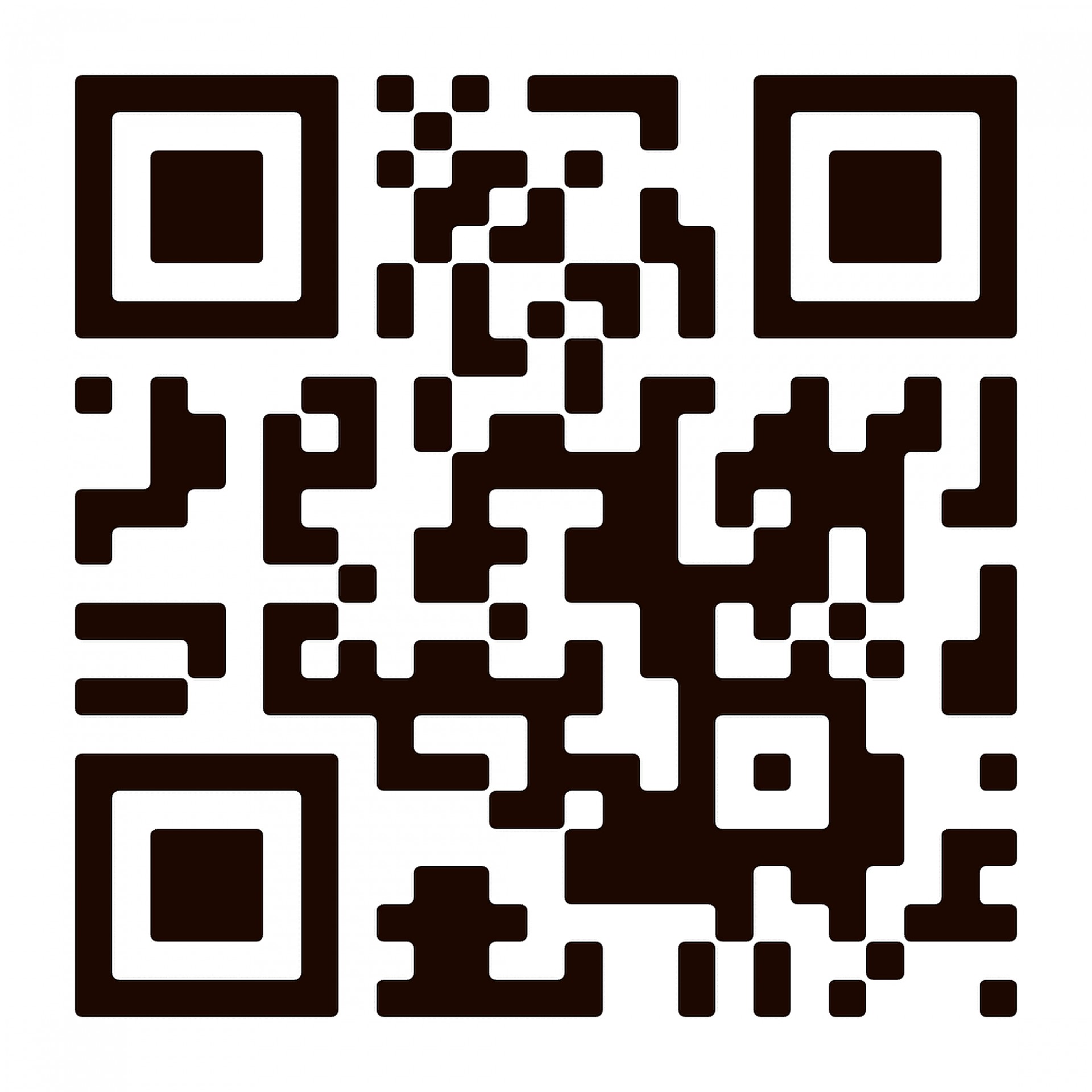
***In their investigation of password evolution, Bonneau (2015) state that:***

***The password is added to the sharing operating system in the 1960s. However, the problem arose very quickly due to the leakage of the unencrypted password master file. When reaching 1970s, the password started to be stored in the hashed form. In 1979, the hashed password was improved with the salting. With the mid-1990s introduction of the World Wide Web, the password is secure using the public-key cryptography via secure sockets layer (SSL) client certificates. The password is then started to link to the email and two-factor authentication is introduced. In the early 2010s, the smartphone starts to be widely used. The reason for the implementation is also because of the free smartphone applications to act as a second factor based on the emerging time-based-time-pad (TOTP) standard. TOTP is an algorithm that computes a one-time password from a shared secret key and the current time. There are also services provided by sending codes via short message service (SMS) as a backup authentication mechanism.***

***In their investigation of password evolution, Denso (2016) state that:***

***Quick Response (QR) code was created by 1994 in Japan. It is named after quick response because of the high-speed reading. QR code is an evolution of the barcodes. The evolution occurs due to the limitation of the barcodes which only can hold 20 alphanumeric characters. The e project is then carried out by Masahiro Hara and his development team for 1 year and a half. The outcome of the QR code is a huge success due to it can store 7,000 numerals with the additional capability to code Kanji characters was finally created. With the current technology, the QR******code is scanned can help to redirect to a website or coupon****..*

*Introduction :*



*Figure QR Code Generator*

*PROJECT OBJECTIVES:*

*The 4 main objectives for this project:*

***1. The main objective is to implement a secure login authentication system utilizing two-factor authentications. Using the concept of two-factor authentication could help to increase the strength of the login system. The attacker will need to pass through the next barrier of defense to success to log in. This system will help to enhance the login authentication system.***

***2. Next objective is to ensure login password will not be transmitted over the network. As compared to the previous solution, the password is just encrypted, but the attackers might succeed in decoding the data and retrieving the password. So, to prevent this happening, the password with the random key will need to be hashed before the sender sends the password to the server. It is important to*** ***secure the password of the user.***

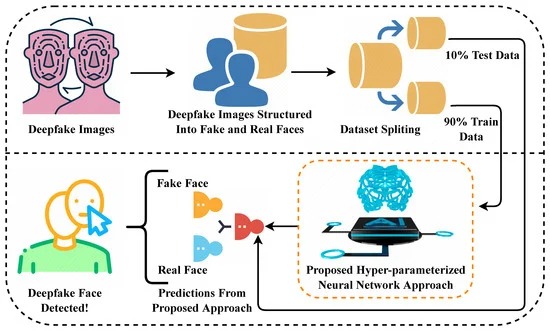
***3. Apart from that, the third objective will be to generate the one-time password offline. This will help in perform the login procedure if there is a limited connection of wi-fi or mobile signal is weak. It will help the user who lives in the countryside which has a weak phone signal.***

***4. Lastly, the fourth objective is to ensure the system is protected from rainbow table attack. The rainbow table will act as a dictionary store and optimized for hashes and password. So once the random key is repeated, the password will be retrieved. So, the random key should be long enough to cause the attackers to use a longer time to generate the rainbow table.***

***PROPOSED APPROACH/STUDY:***

***The proposed solution to enhance the security of login authentication system*** ***by implementing the new system. In the new system to be proposed, it will help to enhance the password security. The system will help to ensure the password will not be transmitted along the traffic. Therefore, this project would like to provide alternative ways for login to a system by using QR code as the random key method, attackers will be hard to decrypt the password since they will need to generate a huge rainbow table if the random key is long enough.***

***Under the proposed system, the user will key in the username then the password will be obtained. The server will generate a random key with 40 characters in the form of QR code. The phone will then scan the QR code to obtain the random key. The password will then combine the random key and hash. The server will retrieve the password from the database then combine the random key and hash it. Both of these hash values generated will take the first 6 characters as the OTP. Once it is both matches, the login is success.***



***LITERATURE REVIEW :***

***EXISTING PROPOSED SOLUTIONS OVERVIEW:***

***Authentication is a process to access to login account and accessing the service provided by the system or server using the password. It also has an alternative way to authenticate the user which is using biometric authentication by using fingerprint or iris recognition. However, human has the tendency to create easily remember passwords which it*** ***will lead to a problem.***

***One Time Passwords (OTP) offers a promising alternative for two-factor authentication systems. A one-time password is a password that is valid for only one login session or transactions, on a computer system or other digital device.***

***Two-factor authentication solution equips customers with a cost-effective means of providing flexible and strong authentication to very large scale. The goal of computer security to maintain the integrity, availability and privacy of the information entrusted to the system can be obtained by adopting this authentication technique. There are also company use the hashing algorithm to store their password. In the transmission of the password, the password has already been hashed and become unreadable. Lastly, most of the password is now encrypted when it is sent from the sender to the receiver.***

***The password is encrypted so that the attackers will not easily obtaining the correct password since they will need another step to decrypt the data.***

***TWO FACTOR AUTHENTICATION :***

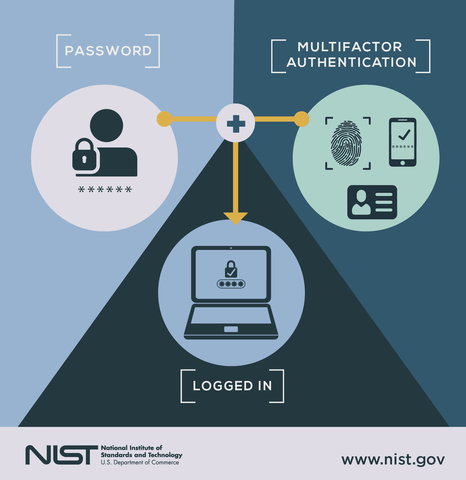
***Two-factor authentication has been introduced long time ago. It is also known as the two-step verification. The organization will implement this method because it is easy the implement it. They can save the cost from replacing the existing system and increase security level by adding a layer of security that protects the existing authentication system.***

***Two-factor authentication is an evolvement from single-factor authentication which only requires the password of the user. However, single-factor authentication is no longer secure due to user tends to have the weak password which is common.***

***Users also tend to have the same password for multiple accounts. This provides a chance for the hacker to succeed in password exploitation. The two-factor authentication helps to provide an additional layer of security.***

***In two factor authentication, the user provides dual means of identification, one of which is typically a physical token, such as a card and the other of which is typically something memorized, such as security code. The aim of the multifactor is to create a more difficult step for attackers/ unauthorized people to access a target. This mechanism still able to be secure if there is still existing a barrier to breach before accessing the target.***

***TWO – FACTOR Authentication flow:***

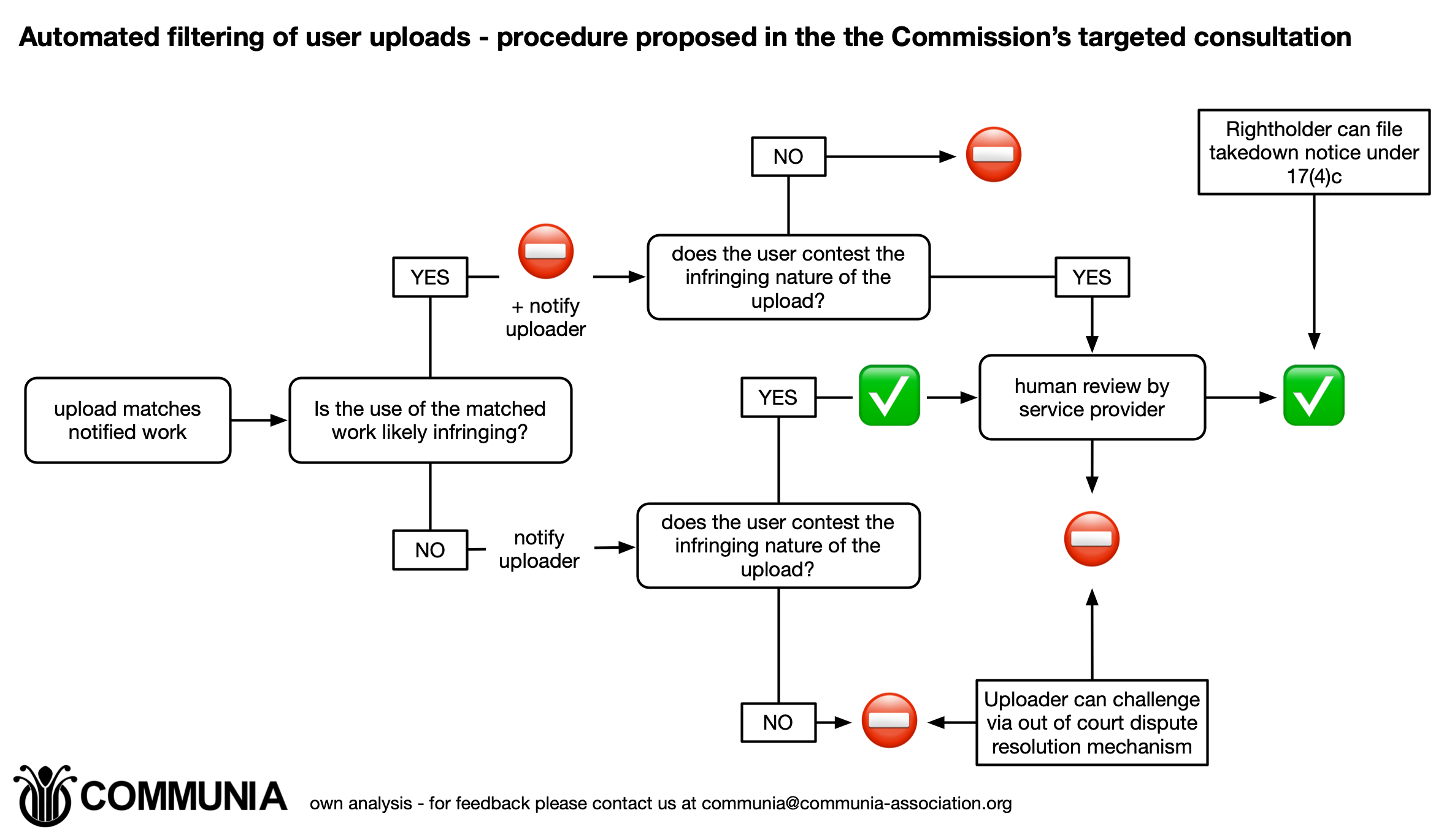


***ONE TIME PASSWORD (OTP):***

***A one-time password is a password that is valid for only one login session or transaction, on a computer system or other digital device. The OTP authentication main idea is to provide infinite factors and create different password every time during user logging in to improve the security of the system. OTP is used in conjunction with a token. The token and corresponding authentication server share the same algorithm. The algorithm is different for each user's token to prevent attackers break the algorithm. A number of OTP systems also aim to ensure that a session cannot easily be intercepted or impersonated without knowledge of unpredictable data created during the previous session, thus reducing the attack surface further. The OTP authentication system is implemented by two main mechanisms. The first mechanism is the challenge-response mode. The system will generate a challenge to the user when the user is logging in.***

***The OTP is generated by combining user keyed in the password and challenge generate by the system.***

***The user will need to key in the OTP to log in suc***c***essfully.***

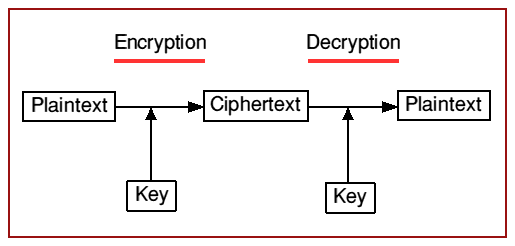
*Challenge-response* *mechanism. :* 

***CRYPTOGRAPHY***

***Cryptography is the study to generate the secret message between the sender and the receiver. The main goal of the cryptography is authentication, privacy, integrity, non-repudiation and access control.***

***Encryption is a process that converts the message into unreadable using some algorithm. It is one of the processes that applying the cryptography.***

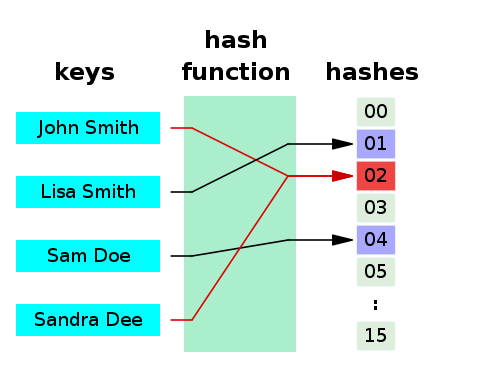
***Encryption is a step that transforms or converts the data into a random and meaningless message. In another word, it can be said as is a process to convert plaintext into the cipher text.***



***Decryption is the vice versa of the encryption which will convert the data into the meaning form. It is a process to transform ciphertext into plain text. In order to perform the cryptography, the cryptographic algorithm is needed to act as a mathematical function and steps to perform encryption and decryption. The purpose of the cryptography is to increase the difficulties for the attackers to decrypt the ciphertext.without given the actual key to be decrypted. Many sites store the password in the encrypted form in their database on the server. They will use a special key to convert the password into a random string which is a ciphertext. If the user without the key, they will not be able to obtain the password but just a random string. However, it is reversible where there is the chance of success decryption by attackers.***

***HASH FUNCTION:***

***Hashing is a step that will use a hash algorithm such as the MD5 to turn a password into a long random string which consists of letters and numbers.***

***The hashes are the opposite of encryption which is not reversible to be the original text. There is no algorithm exists to reverse back the hashes. However, the attackers can try the different combination of the password in order to match the user password. The combination password hashes are then collected to store into the rainbow table. This method will be very time exhausting.***

***Flowchart of hash algorithm***

***COMPARISON BETWEEN PROPOSED SOLUTION***

|  |  |  |
| --- | --- | --- |
| ***Proposed Solution*** | ***Strength*** | ***Weakness*** |
| ***Two factor authentication*** | ***Increase the step for attackers to success*** | ***If the email is hijacked, the process cannot continue until the email is been recovery.*** |
| ***One Time Password*** | * ***Not vulnerable to replay attack.*** * ***Can be time limited*** | * *Require internet or phone connection to complete the process.* * *User will feel annoyed to wait for the message to reach if the connection is slow.* |
| *Cryptography* | * ***The attackers will need time to find the decryption key*** | * *Attackers might succeed from retrieve decryption key* * ***The key can be exposed by network admin to the attackers*** |
| *Hash Function* | * ***The password is not reversible*** * ***The password with the similar hashes is rare***. * ***Time exhausting to crack the password.*** | * *Vulnerable to rainbow table attacks* |