Efficient and Secure Sound-Based Hybrid Authentication Factor with High Usability

Mohinder Singh B.[1], and Jaisankar N.[2,*]
[1] School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, Tamilnadu, India
[e-mail: mohindersingh.b2018@vitstudent.ac.in]
[2] School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, Tamilnadu, India
[e-mail: njaisankar@vit.ac.in]
[*]Corresponding author: Jaisankar N.

Received October 29, 2022; revised July 28, 2023; accepted October 9, 2023; published October 31, 2023

Abstract

Internet is the most prevailing word being used nowadays. Over the years, people are becoming more dependent on the internet as it makes their job easier. This became a part of everyone's life as a means of communication in almost every area like financial transactions, education, and personal-health operations. A lot of data is being converted to digital and made online. Many researchers have proposed different authentication factors - biometric and/or non-biometric authentication factors - as the first line of defense to secure online data. Among all those factors, passwords and passphrases are being used by many users around the world. However, the usability of these factors is low. Also, the passwords are easily susceptible to brute force and dictionary attacks. This paper proposes the generation of a novel passcode from the hybrid authentication factor - sound. The proposed passcode is evaluated for its strength to resist brute-force and dictionary attacks using the Shannon entropy and Passcode (or password) entropy formulae. Also, the passcode is evaluated for its usability. The entropy value of the proposed is 658.2. This is higher than that of other authentication factors. Like, for a 6-digit pin - the entropy value was 13.2, 101.4 for Password with Passphrase combined with Keystroke dynamics and 193 for fingerprint, and 30 for voice biometrics. The proposed novel passcode is far much better than other authentication factors when compared with their corresponding strength and usability values.

Keywords: Authentication factor, Hybrid authentication, Passcode, Password, Security, Sound, Usability, User authentication.

1. Introduction

For the past two years, the usage of online services has become more predominant in people's lives. Most of the jobs are being done easily using the corresponding online services. Most of the resources are online for easy usage and transactions for various purposes. The resources are stored and made available from the organizational servers or cloud storage to the users. During the pandemic situation due to Corona Virus Disease 2019 (COVID-19), many organizations were forced to do their operations online. This is evident in the Unit 42 Cloud Threat Report, which found that in the early days of the pandemic, employees working remotely grew from 20% to 71% [1]. This led to an increase in threats to the resource that are shared online. Among the resources, there also exists sensitive data that is shared by an individual or by an organization. In this digital world, data is the most expensive resource. To secure the data or the resources provided through online services, access should be restricted only to legitimate users. The first step in securing the data or resource is by properly authenticating a user who tries to access using an online service. According to the 2022 Common Weakness Enumeration (CWE), the threat due to improper authentication is ranked 14 among the top 25 most dangerous threats [2].

In simple words, the process of identifying or authenticating a user who they claim to be and providing access to the resources is called authentication. The claimant is the one who tries to prove their claim to access a resource. In any generic process of authentication of a user, the registration phase is the first and foremost step.

- In the Registration phase, the user who wants to make use of a particular resource should register themselves. In the registration process, one or more authentication element(s) related to the registrant that is unique from other registrants are registered. Once registered successfully, the user becomes a subscriber.
- Then comes the resource-access initiation phase in which the subscriber needs to produce/ use the registered authentication element to access the resource. After this, the user verification phase takes place. Here, the authenticator verifies the authentication value produced by the subscriber with the registered value. If the value matches exactly, then the claimant is given access to the resource, and the session value is set to true. The subscriber can now get into the resource pool and access the resources based on the authorization and the access levels given to them. After the job is done and the subscriber exits from the resource pool, the session value is set to false.

The element that actively contributes in verifying a user who they claim to be is called the Authentication factor. Authentication factors are commonly divided into three categories. They are

- Knowledge factor - Depends on the knowledge or memory of the user, i.e., something the user knows. For example, password, passphrase, etc.
- Possession factor - Something the user possesses or holds. For example, smart-card, Personal Identification Number (PIN) extractor devices, etc.
- Inherence factor - Something that belongs to the basic nature of the user. Here, the values mostly represent the biologically inherited features. For example, fingerprint, iris, voice, etc.

The following are modeled after the authentication factors:

- Single-factor authentication - The authentication elements are from a single category of authentication factors

- Two-factor authentication - The authentication elements are from any two different categories of authentication factors
- Multifactor authentication - The authentication elements are from more than two categories of authentication factors

1.1 Two-Factor Authentication and Dual authentication

From the above statements, it can be understood that if the authentication process involves the user inputs that belong to any two different factors or categories, then it is called Two-Factor Authentication (2FA). It is popularly known as 2FA. In Dual Authentication (DA), both authentication elements belong to the same authentication factor/category. **Table 1** represents the combination of authentication factors that are widely used.

Table 1. Combination of authentication factors

2FA / DA	**Knowledge**	**Possession**	**Inherence**
Knowledge	0	1	1
Possession	1	0	1
Inherence	1	1	0

Table 1 looks a lot like a truth table. Here, if the cell value is 1, the combination represents 2FA; if the value is 0, then it comes under DA.

1.2 Multi-Factor and Multilevel Authentication

As defined earlier, in Multi-Factor, the authentication elements are from more than two categories of authentication factors. In Multilevel authentication, the process of authentication is required at every level to access resources. Here, the authentication can be of single, two, or multi-factor.

Over the period, many researchers have suggested many elements of factors. Most of the factors have their disadvantages like hard to recollect - in the case of passwords, passphrases; losing the devices, and changes in the basic nature of bio-element in the case of biometrics which is a part of the authentication. In this paper, a novel authentication factor, the usage of sound is proposed. This sound factor is different from the voice biometric and it intensifies the security along with the usability.

In this research paper the following works are carried out:

- Analyzed the existing authentication factors in terms of security and usability.
- Identified and proposed a new, unique hybrid authentication factor.
- Processed the proposed factor into a unique code called pSoundcode.
    - The sound-code based passcode is termed as ‘pSoundcode’.
- Analyzed the strength and usability of the proposed authentication factor.

2. Related Work

The generic authentication factors registration and the process of verification are almost the same. The generic process is described as:

- The user has to provide the chosen authentication factor values to the system.
- The factors are processed to generate the authentication template.
- If the user selects the registration process, then the generated template is stored in the database for future purposes.
- If the user selects the login process, then the generated template is verified with the corresponding template stored in the database.
  - If matched then access is allowed otherwise access is denied.

The above sequence is represented in **Fig. 1**.

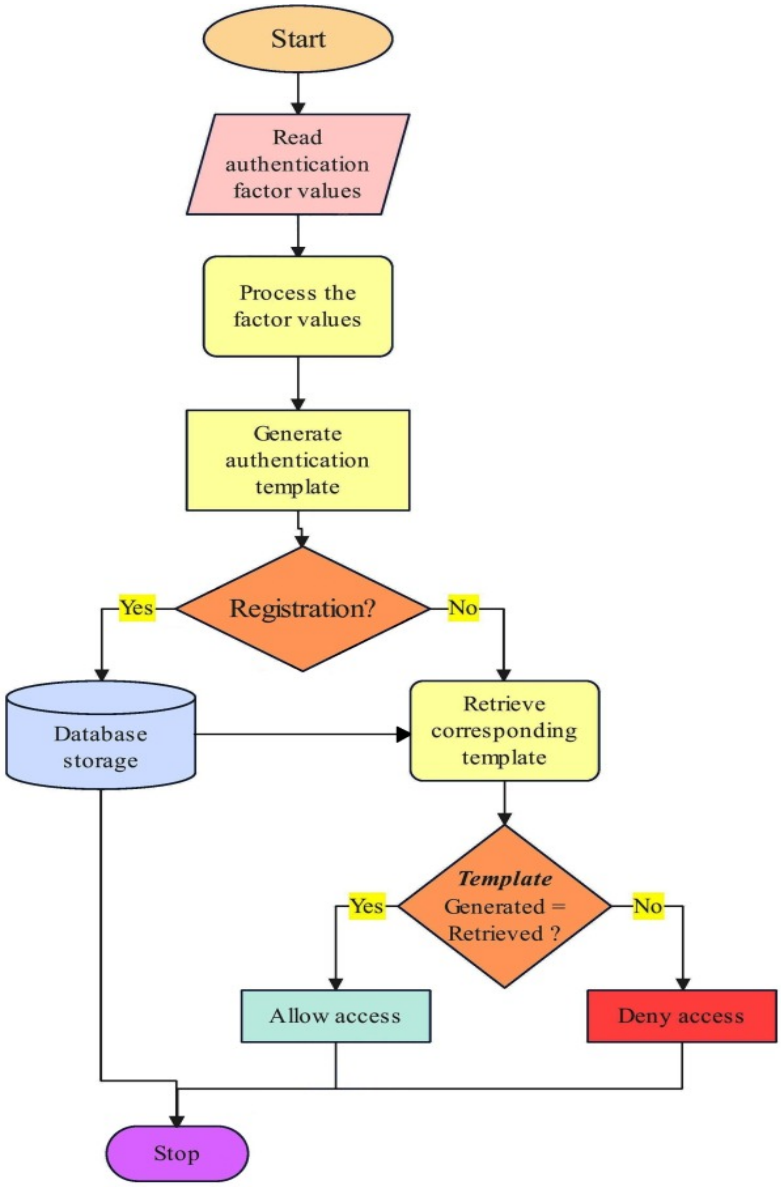

Fig. 1. Generic Authentication registration and verification process flow

In general, the authentication factors were categorized under Biometric and Non-biometric factors. The factors that depend on the physical or behavioral traits of a human are Biometric

factors. And, all the other factors are Non-biometric factors.

2.1 Non-Biometric factors

The authors in [3] preferred Multi-Factor Authentication (MFA) to the single password authentication method. Raza et al.[3] conferred that the single password authentication is easy to use and also financially affordable. But, the authors did not deny its high frequency to get attacked by attackers.

In some of the two-factor authentication (2FA) models, a code, the second factor that was part of the authentication process is received as an SMS text message. Because of network issues, the message delivery was not guaranteed in-time. In [4], the usage of Quick-Response (QR) code was proposed as a second factor. The problem in this scheme was that the QR-code is based on the registered mobile phone. So, the device should be carried always for authentication. Also, this scheme is susceptible to theft attacks.

A user-intelligible authentication technique was proposed in [5]. This method used the tapping for a user-selected rhythm as an authentication factor. Here, the rhythm tappings were captured, for which the binary arrangement was generated. Also, the count of beats tapped was acquired. Later, this was used for verifying the user. The proposer boasts that this method was a cognitive behavior of a user and was hidden from others. They also claimed that this overcame the shoulder surfing attacks. But, the problem with this scheme is that the user should be music conscious and know tapping for a rhythm. Also, the device should equip with the component that can capture those tappings.

An innovative, mapped-out, recollectible textual password was suggested in [6]. In this technique, the user's contact lists were lined-up with the password as hints. This method was given to overcome the issue of forgetting the password and it achieved the same [6]. But, if the user's contact list is compromised, the attacker can gain the password.

In [7], it was proved that the personal PIN can be compromised using the motion sensors of the device. Password prediction was achieved in [8] by examining the basic changes of hand-actions while typing the password. A novel password mechanism called the “life-experience password” was introduced in [9]. Here, the user was suggested to share personal experiences as part of the password mechanism. This hinders the privacy policy of the user.

The author in [10] did not strongly support the use of biological features as the authentication factor. The reason was that if the biometric used is compromised, then it cannot be used in future. So, the author entailed the use of a passphrase as one of the authentication factors and the keystroke authentication algorithm as the second. But, when using the passphrase, there arise the problems of frequent typo errors, there may be a difference in keystroke dynamics even though the passphrases are same, and not many passphrases can be remembered.

2.2 Biometric factors

It is known that some of the biological features are unique from person to person. Some researchers have proposed the biological feature as one of the authentication factors.

In [11], the distinctive movement of the lips of the user was captured using the acoustic sensors of the device and used for authentication. It was based on the claim that every user has different lip movements while talking. The lip movements become unstable when the user has physical-health issues. To overcome this problem, in [12], along with the lip movement, the voice of the user was considered for authentication was proposed. Here, the problem arises when the voice of the user was not properly captured by the device. It was suggested in [13]

that the biological features were proved to be efficient in authenticating a user. Ashraf et al. [14, 15] offered a multimodal system that made use of foot and iris biometrics. Their system successfully segmented iris quickly and precisely. In comparison to other multi-modal technologies, their suggested attained 98 percent accuracy and consistency.

Table 2. Summary of related works

References	Problem identified	Proposed solution	Limitation
[3]	Single password authentication	Multi-factor authentication	Did not suggested any particular multi-factor authentication
[4]	Delivery of SMS text message was not guaranteed due to network issues	QR-code as second authentication factor	Prone to theft attack. Also, the device should always be carried for authentication.
[5]	Shoulder surfing attacks	User-selected rhythm tappings as an authentication factor	The user should be music conscious and should have proper tapping knowledge for a rhythm
[6]	Issue of forgetting the password	A mapped-out, recollectible textual password using contact list	If the user's contact list is compromised, the attacker can gain the password
[7]	Personal PIN can be compromised using the motion sensors of the device	Evidenced that PINs were compromised. Not given any proposed solution	Not Applicable as no method was proposed
[8]	Password prediction through hand-actions while typing the password	Demonstrated that typed-passwords can be expected easily. Not given any proposed solution	Not Applicable as no method was proposed
[9]	Password prediction	Suggested a system in which personal experiences were asked to share as part of the password mechanism	Hinders the privacy policy of the user
[10]	If the biometric used is compromised, then it cannot be used in future	Passphrase and the keystroke as authentication factors	Passphrase, there arise the problems of frequent typo errors, there may be a difference in keystroke dynamics even though the passphrases are same, and not many passphrases can be remembered.
[11]	Issue of forgetting the text-password	Movement of the lips of the user that was captured using the acoustic sensors was considered as authentication factor	Lip movements become unstable when the user has physical- health problems
[12]	Lip movement alone was not considered to be a strong authentication factor.	Lip movement along with the voice of user as authentication factor	Voice of the user may get distorted due to health problems. Also the problem in [11] remained same.

[14, 15]	The previous multi-modal factors were not efficient in terms of accuracy and consistency	Proposed the use of Iris and foot characteristics. Their proposed system achieved speed and precise segmentation of iris. The proposed multi-modal achieved efficiency in terms of accuracy and consistency	Both the iris and the foot characteristics may change due to health ailments and other external forces like accidents.

Table 2 gives a summary of the existing works. The common limitation of biometric factors is that the characteristics of the bio-element may change due to external forces or may be due to health issues. A biometric identification method has a significant danger of being rendered permanently useless if it gets compromised. The authors of [16] figured out that the existing authentication models support either high security with low usability or low security with high usability. In [17], it was revealed that the users were forced by themselves to use common or repeated passwords. This was because of forgetting the passwords frequently.

3. Hybrid Authentication Factor

It is evident from the above section that the factor types i.e. knowledge, and possession biometrics have their own advantages and disadvantages. The existing user-authentication methods put emphasis mostly on the system security rather than the factors used for authentication. The major problem with existing authentication factors is that they are not user-friendly, not highly usable, and are highly dependent on third-party devices. But, the factors to be used should be highly usable, changeable, and less-dependent on a particular third-party authentication device.

In this proposed work, the power of knowledge is well utilized. It is well known to the scientific community that the human brain is the most powerful, and more than a high data storage computer. The human brain can store different types of data. Among them text, pictorial, and musical/ sound data are common. Compared to the text data, it is proved that the musical data can be remembered very easily.

In [18], the authors proved that there exists a Musical Memory Area (MMA) in the human brain. They also evidenced that musical memories can survive even when amnesia and dementia have set in. The authors in [19], investigated whether song-like or speech-like data are remembered better. The authors came up with the conclusion that the song is more memorable than the speech.

Based on the above-proven theories, in this paper, sound/ music is considered to be the new authentication factor. The user has to select the required sound from a large pool of resources. This sound resource will not become scarce because thousands of music data are being created every second around the world. The pattern for this new authentication factor, sound, is stored in the brain of a human. But the details of the sound are to be taken from the resources available. So, this factor can be considered a Hybrid authentication factor (knowledge + possession). This is termed as the “Knoes” authentication factor in this paper. In this work, different features, and their approaches are used. Following are their descriptions:

3.1 Fast Fourier Transform (FFT)

Discrete Fourier Transform is simply called DFT. This is used to convert the music/ sound wave to digital format. Among the several members of the Fourier transform family, DFT is

the only one suitable for Digital signal processing. The transformation breaks the time series of sound into the sum of finite series of cosine and sine functions.

For an original time wave, the frequency spectrum is obtained using a definite frequency and it's corresponding amplitude. These two are associated with sine/cosine function [20]. FFT is basically a process to calculate the DFT in a fast manner. This is achieved by minimizing the requisite number of multiplications and additions. This notion was propagated by James W. Cooley and John W. Tukey [21].

3.2 Amplitude

The FFT for a sound wave results in amplitude and phase (frequency). In this proposed work, the amplitude is considered for processing. In reality, the amplitude represents the sound pressure.

3.3 Secure Hash Algorithm 3 (SHA-3)

SHA-3 is the recent among the family of Secure Hash Algorithm standards. This was released by the National Institute of Standards and Technology (NIST) [22]. It is a subset of the broader cryptographic primitive family Keccak designed by Guido Bertoni, Joan Daemen, Michael Peeters, and Gilles Van Assche, building upon RadioGatun [23].

3.4 pSoundcode generation

When a user tries to login into a system, a username or user ID (UID or uid) along with an authentication factor is given to get access to the system. The process of generating the pSoundcode using the Knoes authentication factor is depicted in **Fig. 2**.

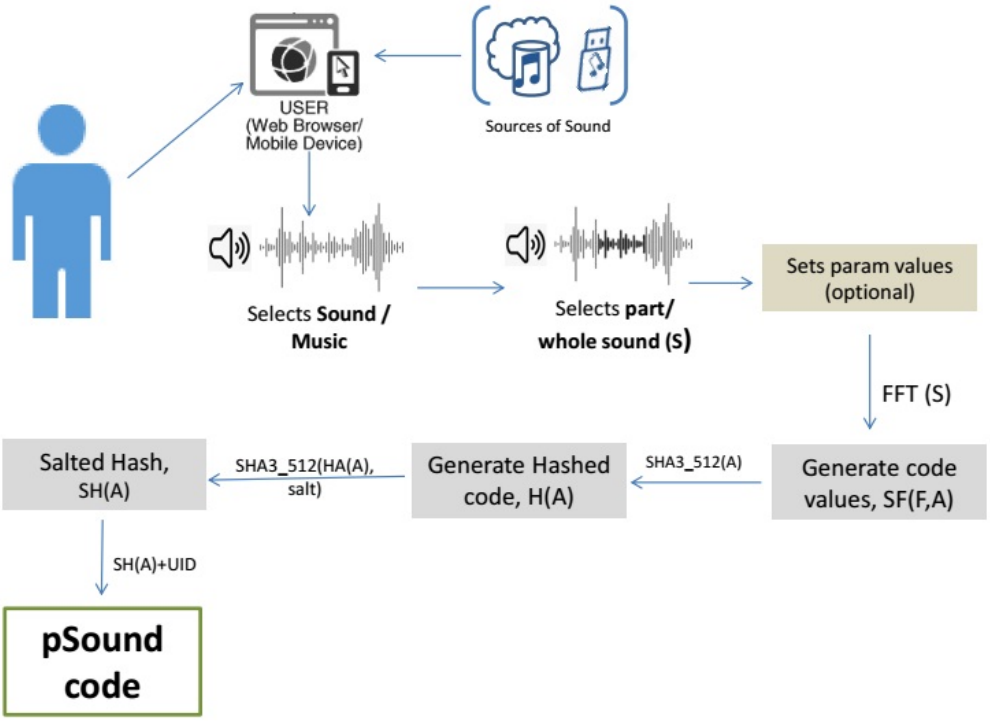

Fig. 2. Process of pSoundcode generation

The diagram in **Fig. 2** gives an overview process of generating the pSoundcode.

- First, the user will select the sound/music from local data storage or internet that they want to use it as the passcode.
- The user can use the whole sound file or part of the sound.
- At first, the sound will have the default sampling rate and offset values. The user has the option to change the default values. The offset value should be greater than 0 and less than the time duration of the selected sound.
- Later, FFT was implemented on the selected sound. Then the hash is calculated for the resultant value. Then the salted hash is generated using a salt value combined with the hash that is obtained in the previous step.
- At last, the pSoundcode is obtained by hashing the salted hash with the user's uid.

The above process is represented as a flow diagram in **Fig. 3**.

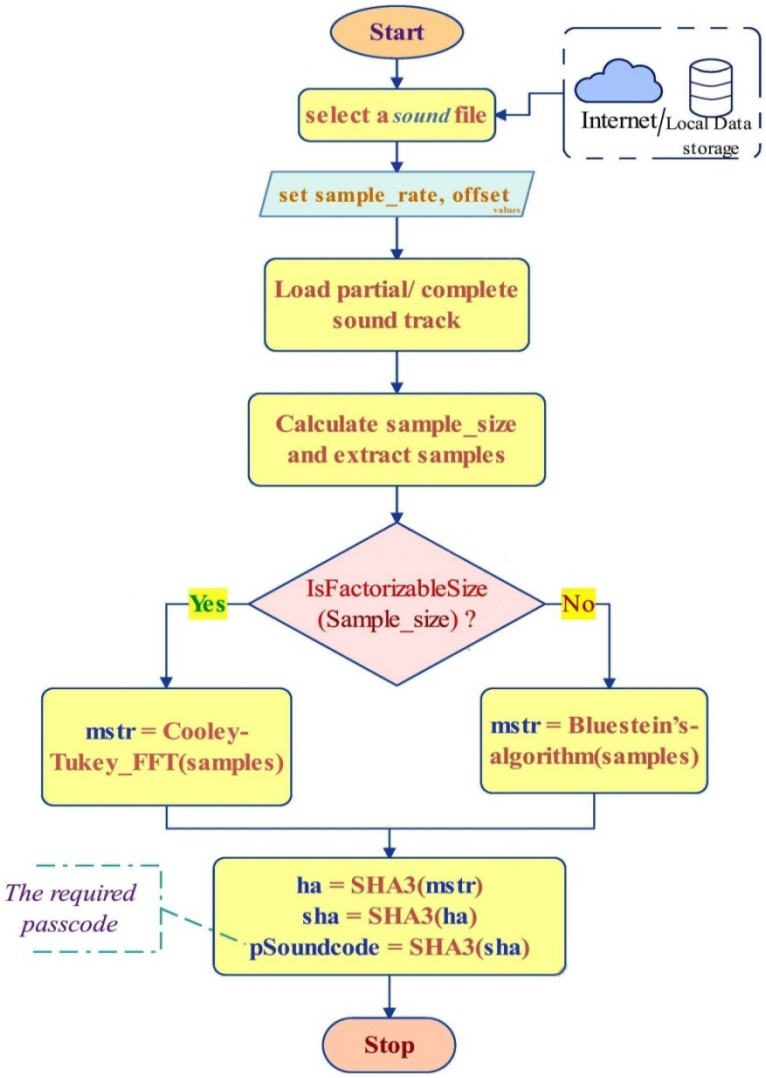

Fig. 3. Flow diagram for the process of pSoundcode generation

The detailed algorithm for the above flow diagram is given in algorithm 1 at **Fig. 4**.

Algorithm 1 Generate pSoundcode

Input: UID, sound/ music file, salt
Output: pSoundcode

uid ← UID of user
soundFile ← user selected sound file
salt ← salt value
procedure gen_pSoundcode($uid, soundFile, salt$)
    ns ← load(soundFile, sr ←*default*, offset ←*0.0*)
    S ← load(soundFile)
    if $[ns > 0$ AND $(ns \& ns - 1) = 0]$ **then**
        m[] ← *ctfft(S)*
    else
        m[] ← *bfft(S)*
    for i ← 0 to ns-1 **do**
        mstr ← *str(mstr)+m[i]*
    Ha ← SHA3(mstr)
    Sha ← SHA3(Ha+salt)
    Usha ← Sha+uid
    return Usha

Fig. 4. Algorithm for pSoundcode generation

In algorithm 1 at **Fig. 4**, the *sr* refers to the sampling rate and is set to the default value. The offset is set to 0.0. The user is allowed to change the sampling rate and offset values if required. The sample size(ns) and the samples(S) are extracted from the *soundFile*. The *ns* and *S* values depend on the sampling rate and offset values.

$$m[n] = sum\left(S * e^{-2j*PI*k*n/ns}\right) \tag{1}$$

The magnitude(m[ ]) for the samples (S) is calculated using the 1-dimension n-point Cooley-Tukey FFT [24] i.e., ctfft(S), if ns is a power of 2. It is given in (1). If *ns* is not a factorizable size, then the Bluestein's algorithm is used. Here, in (1) n=0, 1, 2, ..., ns-1. The right-hand side of (1) is the summation of values of a function at discrete time points of a sample. This results in n^{th} coefficient of FFT.

After populating the *m* with the resultant of FFT, every single magnitude value is converted to string and concatenated to each other. This will result in a single large string value, *mstr*. Then, the hash value of *mstr* is calculated using the SHA3 algorithm, say it *Ha*. To *Ha*, the salt is added and SHA3 is implemented on the result value to get salted hash (*SHa*). Finally, to *SHa* the uid is appended to get *USHa* which is the pSoundcode. Now, this pSoundcode is the required unique passcode.

$$M_n = \sum_{i=0}^{N-1} S_i e^{-2*PI*j*i*n/N} \tag{2}$$

Equation (2) represents the mathematical formula for FFT [25] that is given in (1). In (2), M_n is FFT's n^{th} coefficient. Of N samples of the time series, S_i is the i^{th} sample. The value of j is $\sqrt{(-1)}$. Each sample is probably a complex number and the coefficients are also invariably complex. At times, index n is called "frequency" of FFT because, for a function at specific time intervals,

the S_i's are the frequent values.

The reason for choosing the Cooley-Tukey FFT is it's computational efficiency. **Table 3** represents the computational efficiency [26] of FFT over the DFT:

Table 3. Computational efficiency

	Computational Efficiency of an N-point
DFT	N^2 complex multiplications
FFT	$(N/2) \log_2 N$ complex multiplications

As the N value increases, the efficiency of FFT also increases over DFT. The overall computation cost of FFT is ($N \log_2 N$). **Table 4** represents the efficiency ratio [24] of DFT and FFT. It clearly shows that FFT is very efficient in terms of operations than DFT.

Table 4. Efficiency ratio of DFT and FFT

N	**Multiplication operations**		**Efficiency ratio**
	DFT	**FFT**	
256	65,536	1,024	64:1
512	262144	2304	114:1
1024	1048576	5120	205:1
2048	4194304	11264	372:1
4096	16777216	24576	683:1

In algorithm 1 at **Fig. 4**, SHA3 is used to get hash value. The SHA3 uses Sponge construction. The sponge construction has two crucial phases. One is the Absorbing phase, while the other is Squeezing phase. In the former phase, the sponge function receives the data. In the latter phase, the sponge function squeezes out the result.

$$SHA3\_d(M) = keck[c](M||01, d) \tag{3}$$

where

$$keck[c](M||01, d) = spnge[keck\_perm[1600,24], pad10*1, 1600 - c](M||01, d) \tag{4}$$

The formula for SHA3 from [22] is given in (3). Here, in (4), d is the length of the digest in bits, M is the message, c is the capacity and c=2d.

There are many hashing algorithms available in the SHA family. But, as of today, the SHA3 is considered to be the secure algorithm. Also, the collisions are very much less when compared to other hashing algorithms. This is the reason that SHA3 is used in algorithm 1.

The main aim of this proposed authentication factor is to achieve both security and usability.

4. Result Analysis

The performance of our proposed passcode, pSoundcode obtained using 'Knoes' the hybrid authentication factor is evaluated in this section. Three models are used to evaluate the

strength of the passcode along with their usability. The experimental results prove that the proposed factor achieved high usability, security, and efficient. This section is further divided into two subsections: Evaluation models, and overall comparative analysis.

4.1 Evaluation models

In this section, the strength and usability of the passcodes are evaluated. The strength of a passcode is calculated in entropy bits. The entropy is of either Shannon's entropy or Password entropy. The higher the entropy, the stronger the passcode. The stronger the passcode, the longer the time to guess the passcode.

4.1.1 Strength Analysis

To check the strength analysis of the passcodes, Shannon's entropy formula and the Passcode Entropy formula are used on the passcodes given in **Table 5**.

Table 5. Passcodes with their entropy values and the failed login instances

PC. No.	Passcode	Passcode Entropy	Shannon's Entropy	Login Failure (for every 100 login instances)
1	qsdfjkhdfsgloijhdfgqhgkqsdiuqsnfbjdjusfsdfq@@fqdfÃ“qsdfsdfÃ“qdf@@sdfsf@@@@dfÃ“qdfqÃ“sfqjkfnqkljhlmqdsflqkjsdfqsdfjkhdfsgloijhdfgqhgkqsdiuqsnfbjdjusfsdfq@@fqdfÃ“qsdfsdfÃ“qdf@@sdfsf@@@@dfÃ“qdfquÃ‘HÂ²Ã¦Ã³Â¦	1376.5	14.6	15
2	OPy9W1DF4BKWKGJqcU1Ru6cRn1ekM9BvJAP7GxSAw78iaFBo0hwXP1xiX8oakeDJNQKGWCe8V04P6s5PLku5wmvEEkRa1GFLUQCN8szjIuv8u4efBk74PSbraRgo1KLemt0FYFVfxVkUUunLAau8hSbsMrdem7hiCasyYGzGBxO8tgq9N1BlSq7yK	1212.6	12.9	15
3	n43sSh567hDjJ678Fj5D857I6j58SjJ876F89762k3liyU3y2y1rReuyNtmimWuQyoItFiNnuWEuUeutJ3teu2ite1imJtiR2ei3er8werJyvtRruyetunKyWryEewbQytru9JEWDKSDJ891J23	963.5	10.3	15
4	581758097483229ac9eeedca93de722dd0f2c81e02ae5934e113302751f9b8ff2d90d6be69fbdb409f53d79c6bedd11f90952f7a8ae2c2b695ac6352227ffc58	839.0	8.9	1
5	wilver45velostheultimate.Molina.Montero.@.42212835	327.7	3.5	7
6	AWdsfrghdDSAFSg856yougfi564756756uyhSVFSEhsef	295.0	3.1	15
7	Password is too simple. It must be at le	262.2	2.8	5
8	BrankoStefanovic123!@	137.6	1.5	5
9	kingdomheart2	85.2	0.9	0
10	6agymilak4ho8	85.2	0.9	1
11	22U0EOKG19607	85.2	0.9	5
12	masteruser159	85.2	0.9	1
13	2je1o0e6adupi	85.2	0.9	5
14	justhacker105	85.2	0.9	0

The Passcodes that are tabled in **Table 5** are samples extracted randomly from the kaggle dataset [27] that contain nearly 669,643 unique passcodes. This dataset also contains some leaked passwords. The passcode i.e., the proposed pSoundcode is calculated and represented at PC.No.4 (Passcode number 4).

4.1.1.1 Shannon entropy

The Shannon Entropy model evaluates the possibility of the distinctive number of attempts required to determine a result [28, 29]. This model deduces the solution based on the yes/ no queries. Here, the bit is used as the unit of measurement to determine the strength of a passcode. Entropy is the term used to describe the count of bits. The uncertainty in predicting the right response is directly proportional to the entropy value. The Shannon Entropy formula is $H = -\Sigma\, p(x) \log p(x)$, where p is the probability of choosing the accurate value from a given set and x is the total available values in the set. The analyzed graph for the tabled values in **Table 5** is depicted in **Fig. 5**.

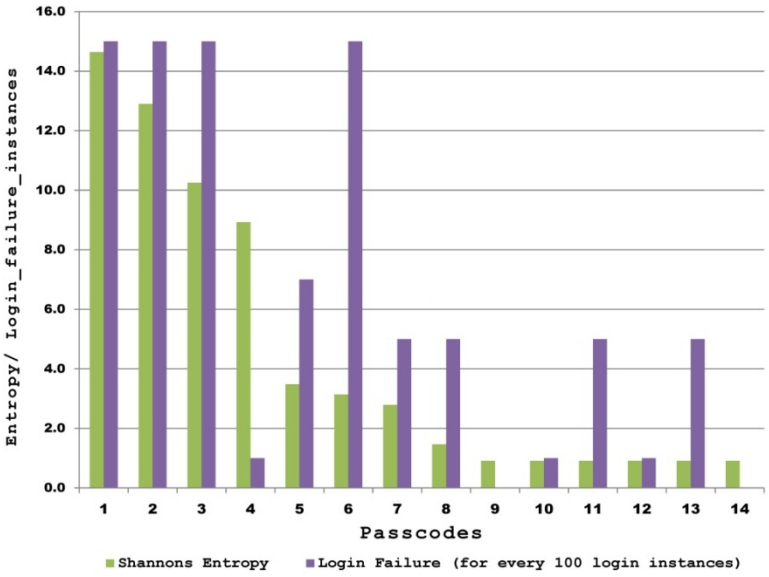

Fig. 5. Passcodes entropy graph

In **Fig. 5**, the x-axis values represent the PC(Passcode) numbers of the corresponding passcodes given in **Table 5**. The y-axis values represent the Entropy value and the failed login instances for every 100 total login instances. The proposed pSoundcode value is depicted on the x-axis: reference 4. Here, though Shannon's entropy value is high for PC.no. 1, 2, 3 than our proposed one, the login failure is far much better than 1, 2, and 3. Though the login failure of PC.No. 9 and 14 are better than the proposed; they have very low Shannon's entropy. It means that they are susceptible to brute force attack.

4.1.1.2 Passcode Entropy

The passcode entropy [30] is also the same as that of Shannon's entropy. The formula used to verify the strength of the passcode i.e., Passcode Entropy (PE) is L * log(P,10), where L – Length of the passcode, P – a pool of unique characters that build the passcode. In this paper, instead of using log10, log2 is used to find the entropy of the passcode. The formula is PE=L * log2 (P). This entropy is calculated for some passcodes and is given in **Table 5**. The proposed

pSoundcode represented at PC.No.4 is far much better than other passcodes.

4.1.2 Usability Analysis

According to the remembrance theory, as in [18, 19], the human brain can easily remember and recall the music data compared to the text data. This implies that a user cannot have much difficulty in recalling the music passcode.

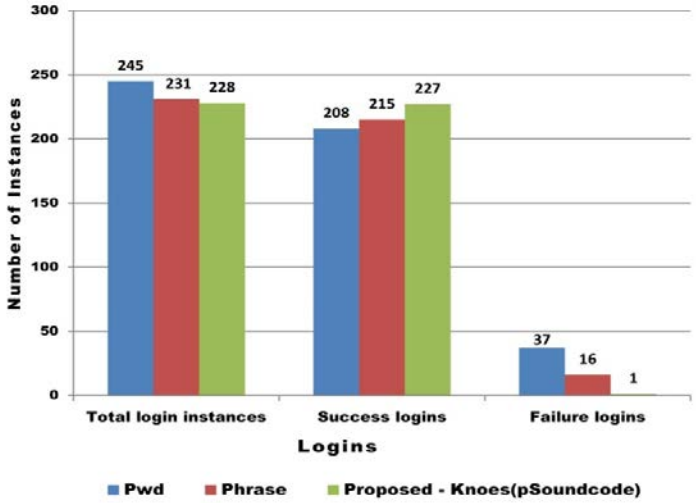

Fig. 6. Login instances vs. passcodes

On the other hand, it is proven that the users face difficulty in remembering and recalling the text passwords, passphrases, and touch-points in an image. Along with this, there arises the typo-error when a complex password or passphrase is used. The graph in **Fig. 6** shows the total number of login instances along with the corresponding successful and unsuccessful logins for the passcode types.

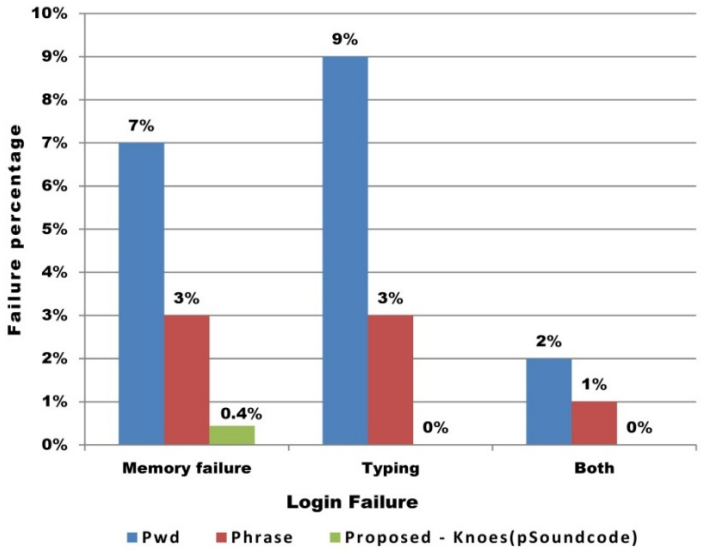

Fig. 7. Causes of login failures

Similarly, the cause for unsuccessful logins is categorized and depicted as a graph in **Fig. 7**.

4.1.3 Overall comparative analysis

This analysis is the comparison between the proposed factor and other authentication factors. The authentication methods with their entropy values are given in **Table 6**.

Table 6. Entropy of different authentication factors

Authentication method at	Authentication method	Entropy (bits)
[32]	4-digit PIN	13
[33]	6-digit PIN	13.2
[34]	Voice biometric	30
[31]	Graphical passwords	35.6
[35, 36]	Randomly created 8-alphabet password	52.7
[10]	Keystroke dynamics and Passphrases	88.4
[37]	Fingerprint biometric	193
[38]	Passphrase	75.2
[39]	Password, Passphrase, and Keystroke dynamics	101.4
Proposed hybrid factor	Knoes - pSoundcode	658.2

The entropy values are depicted as a graph in **Fig. 8**. The voice biometric has the entropy value of 30. The graphical passwords suggested in [31] have the entropy of 35.6. In [10], the authors proposed the use of passphrase along with the corresponding keystroke dynamics as their authentication factor and achieved the entropy of 88.4. The authors at [39] used the combination of password, passphrase, and keystroke dynamics as authentication factors with the entropy value of 101.4. Even the voice biometric has the entropy value of 30.

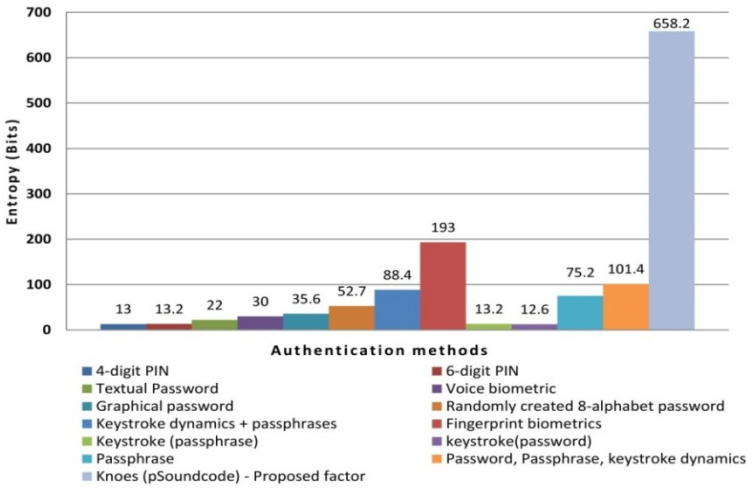

Fig. 8. Authentication methods with their entropy values

The graphical passwords suggested in [31] have the entropy of 35.6. The pSoundcode calculated from the proposed Knoes factor has the entropy value of 658.2 and is far much better than other authentication factors.

5. Conclusion

The elements of the authentication must be high in security and easy to use. The existing biometric factors are secure but the usability is average. The passwords are of high usability but are less secure. They are susceptible to brute force, dictionary, and guessable attacks. To overcome these attacks, passphrases were used. Then, passphrases with keystroke dynamics were proposed. Another factor that involves passphrase in combination with password and keystroke dynamics was also suggested. But, the above factors have the problem of usability. In this paper, a novel hybrid factor, Knoes, is proposed, and they generate a passcode called pSoundcode. This achieved high usability and is more secure than the existing factors. This is proved efficiently with the help of the entropy analysis and the usability analysis. Even though the proposed authentication factor is better than the other existing factors, it does have a problem in the case of hearing-impaired users. In future work, the proposed work will be enhanced to support hearing-impaired users also.

References

[1] Jay Chen, Nathaniel "Q" Quist, and Matthew Chiodi, "Cloud Threat Report 1H 2021," Unit 42, Prisma Cloud, Paloalto Networks, 2021 [Online]. Available: https://www.paloaltonetworks.com/prisma/unit42-cloud-threat-research-1h21

[2] Adam Chaudry and team, "2022 CWE Top 25 Most Dangerous Software Weaknesses," Common Weakness Enumeration, MITRE corporation, USA, 2022 [Online]. Available: https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html

[3] Mudassar Raza, Muhammad Iqbal, Muhammad Sharif, Waqas Haider, "A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication," *World Applied Sciences Journal*, vol. 19, pp. 439-444, 2012. Article (CrossRef Link)

[4] Narasimhan Harini, Padmanabhan, T., "2CAuth: A New Two Factor Authentication Scheme Using QR-Code," *International Journal of Engineering and Technology*, vol. 5, no. 2, pp. 1087-1094, 2013.

[5] J. Seto, Y. Wang, and X. Lin, "User-Habit-Oriented Authentication Model: Toward Secure, User-Friendly Authentication for Mobile Devices," *IEEE Transactions on Emerging Topics in Computing*, vol. 3, no. 1, pp. 107-118, March 2015. Article (CrossRef Link)

[6] N. Alomar, M. Alsaleh and A. Alarifi, "Someone in Your Contact List: Cued Recall-Based Textual Passwords," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2574-2589, Nov. 2017. Article (CrossRef Link)

[7] C. Wang, X. Guo, Y. Chen, Y. Wang, and B. Liu, "Personal PIN Leakage from Wearable Devices," *IEEE Transactions on Mobile Computing*, vol. 17, no. 3, pp. 646-660, March 2018. Article (CrossRef Link)

[8] D. Shukla and V. V. Phoha, "Stealing Passwords by Observing Hands Movement," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 12, pp. 3086-3101, Dec. 2019. Article (CrossRef Link)

[9] Simon S. Woo, Ron Artstein, Elsi Kaiser, Xiao Le, and Jelena Mirkovic, "Using Episodic Memory for User Authentication," *ACM Transactions on Privacy and Security*, vol. 22, no. 2, pp. 1-34, April 2019. Article (CrossRef Link)

[10] Bhaveer Bhana and Stephen Flowerday, "Passphrase and keystroke dynamics authentication: Usable security," *Computers & Security*, vol. 96, 2020. Article (CrossRef Link)

[11] L. Lu et al., "Lip Reading-Based User Authentication Through Acoustic Sensing on Smartphones," *ACM Transactions on Networking*, vol. 27, no. 1, pp. 447-460, Feb. 2019. Article (CrossRef Link)
[12] L. Wu, J. Yang, M. Zhou, Y. Chen and Q. Wang, "LVID: A Multimodal Biometrics Authentication System on Smartphones," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1572-1585, 2019. Article (CrossRef Link)
[13] Z. Rui and Z. Yan, "A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification," *IEEE Access*, vol. 7, pp. 5994-6009, 2018. Article (CrossRef Link)
[14] S. Ashraf, S. Saleem, T. Ahmed, Z. Aslam, and M. Shuaeeb, "Iris and Foot based Sustainable Biometric Identification Approach," in *Proc. of 2020 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pp. 1–6, 2020. Article (CrossRef Link)
[15] S. Ashraf, Z. Aslam, S. Saleem, S. Afnan, and M. Aamer, "Multi-biometric Sustainable Approach for Human Appellative," *Computational Research Progress in Applied Science & Engineering, CRPASE: Transactions of Electrical, Electronic and Computer Engineering*, vol. 6, no. 3, pp. 146-152, September 2020. Article (CrossRef Link)
[16] W. Kang, H. Liu, W. Luo, and F. Deng, "Study of a Full-View 3D Finger Vein Verification Technique," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1175-1189, 2020. Article (CrossRef Link)
[17] Sonwalkar, M.S., "CAPTCHA: novel approach to secure user," *Pramana Research Journal*, vol. 10, no. 1, pp. 106-114, 2020.
[18] Francine Foo and Elizabeth L. Johnson, "Music: The last thing we forget," *Neuroscience, Frontiers for Young Minds*, vol. 5, no. 1, 2017. Article (CrossRef Link)
[19] Haiduk F, Quigley C, and Fitch WT, "Song Is More Memorable Than Speech Prosody: Discrete Pitches Aid Auditory Working Memory," *Frontiers in Psychology*, vol. 11, Dec. 2020. Article (CrossRef Link)
[20] Jerome Sueur, "A very short introduction to sound analysis for those who like elephant trumpet calls or other wildlife sound," March 2022 [Online]. Available: https://cran.r-project.org/web/packages/seewave/vignettes/seewave_analysis.pdf
[21] J. W. Cooley and J. W. Tukey, "An Algorithm for the Machine Computation of Complex Fourier Series," *Mathematics Computation*, vol. 19, pp. 297-301, April 1965. Article (CrossRef Link)
[22] NIST, "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions," Computer Security (Cryptography), FIPS Pub. 202, NIST, 2015. Article (CrossRef Link)
[23] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "The KECCAK SHA-3 submission," vol. 3, January 2011 [Online]. Available: http://keccak.noekeon.org/Keccak-submission-3.pdf
[24] SciPy Community, "scipy.fft," SciPy 1.9.1 documentation, 2020 [Online]. Available: https://docs.scipy.org/doc/scipy/reference/fft.html
[25] Leo I Bluestein, "A Linear Filtering Approach to the Computation of Discrete Fourier Transform," *IEEE Transactions on Audio and Electroacoustics*, vol. 18, no. 4, pp. 451-455, December 1970. Article (CrossRef Link)
[26] Walt Kester (ed.), "Mixed Signal and DSP Design Techniques," *Newnes/Elsevier*, 2002.
[27] Bhavik, "Password strength classifier dataset," 2019 [Online]. Available: https://www.kaggle.com/datasets/bhavikbb/password-strength-classifier-dataset
[28] He, Y., Alem, E.E., and Wang, W., "Hybritus: a password strength checker by ensemble learning from the query feedbacks of websites," *Frontiers of Computer Science*, vol. 14, 143802, 2020. Article (CrossRef Link)
[29] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379-423, 1948. Article (CrossRef Link)
[30] W. Ma, J. Campbell, D. Tran, and D. Kleeman, "Password Entropy and Password Quality," in *Proc. of 2010 Fourth International Conference on Network and System Security*, pp. 583-587, 2010. Article (CrossRef Link)
[31] Zhi Li, Qibin Sun, Yong Lian and D. D. Giusto, "An Association-Based Graphical Password Design Resistant to Shoulder-Surfing Attack," in *Proc. of IEEE International Conference on Multimedia and Expo*, pp. 245-248, 2005. Article (CrossRef Link)

[32] K. B. Raja, R. Raghavendra, M. Stokkenes and C. Busch, "Smartphone authentication system using periocular biometrics," in *Proc. of 2014 International Conference of the Biometrics Special Interest Group (BIOSIG)*, pp. 1-8, 2014.
[33] Ding Wang, Qianchen Gu, Xinyi Huang, and Ping Wang, "Understanding Human-Chosen PINs: Characteristics, Distribution, and Security," in *Proc. of the 2017 ACM on Asia Conference on Computer and Communications Security (ASIA CCS '17)*, ACM, pp. 372-385, 2017. Article (CrossRef Link)
[34] Inthavisas, Keerati, and Daniel P. Lopresti., "Secure speech biometric templates for user authentication," *IET Biometrics*, vol. 1, pp. 46-54, 2012. Article (CrossRef Link)
[35] Van Oorschot, P.C., Wan, T., "TwoStep: An Authentication Method Combining Text and Graphical Passwords," in *Proc. of International Conference on E-Technologies: Innovation in an Open World, MCETECH 2009*, pp. 233-239, 2009. Article (CrossRef Link)
[36] NIST, "Authentication and life cycle management," Digital Identity Guidelines, Special Publication 800-63b, NIST, 2020. Article (CrossRef Link)
[37] Boulgouris, N.V., Plataniotis, K.N., Tzanakou, E.M., "Biometrics: Theory, Methods, and Applications," *Wiley-IEEE Press*, 2009.
[38] Pardon Blessings Maoneke, Stephen Flowerday, Naomi Isabirye, "Evaluating the strength of a multilingual passphrase policy," *Computers & Security*, vol. 92, 101746, 2020. Article (CrossRef Link)
[39] Jubin Raj Nirmal, Rajath B. Kiran, V. Hemamalini, "Improvised multi-factor user authentication mechanism using defense in depth strategy with integration of passphrase and keystroke dynamics," *Materials Today: Proceedings*, vol. 62, no. 7, pp. 4837-4843, 2022. Article (CrossRef Link)

Mohinder Singh B. is currently pursuing the Ph.D degree in the School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India. He completed his M.Tech in Computer Science and Engineering from JNT University, Hyderabad, India. His current research interests include Cryptography, Data Security, Cloud Computing, Blockchain, Machine Learning, Post-Quantum cryptography.

Dr. Jaisankar N. is working as a Professor in the School of Computer Science and Engineering at Vellore Institute of Technology, Vellore, India. Also he worked as program head for MTech(CSE) programme and division head for Computer Network division. He received his B.E. (Computer Science and Engineering) from Bharathiar University, M.E. (Computer Science and Engineering) from M.K.University and Ph.D (Computer Science and Engineering) from VIT University. He has 20+ years of experience in teaching and research. He received certification for CCNA Instructor and SUN certified JAVA instructor. He has reviewed many books titled Network Security, Data Mining, TCP/IP protocol suite and Programming in JAVA. He has participated as a coach in the International Programming Contest held at IIT, Kanpur, India. He has published many papers in International and National Journals and conferences on Network Security, Computer Networks and Data Mining. His research interest includes Computer Networks, Network Security, cloud computing, Data Mining. He has served in many peer reviewed International Journals as an editorial board member, Guest handling editor, advisory board member and reviewer etc. Also he has served in many international conferences as General chair, International advisory board member, technical program committee member, publication chair, organizing committee member, reviewer etc. He has worked in Neusoft Institute, Guangdong, China. He is a life member of Indian Society for Technical Education, Computer Society of India, International Association of Computer Science and Information Technology, International Society for Research in Science and Technology and member of International Association of Engineers.