A Stable and Secure One-Time-Password Generation Mechanism Using Fingerprint Features

Sajaad Ahmed Lone, A. H. Mir

Abstract: ***The growth of online application used for financial transactions and transferring personal information is increasingly common on internet and in mobile communication. These applications require authenticating legitimate users by assigning digital identities. Static passwords are perhaps most common type of credentials used today to authenticate the users. To avoid tedious task of remembering passwords, users often behave less securely by using low entropy and weak passwords, thus presenting security threats to online services. Various solutions have been provided to eliminate the need of users to create and manage passwords' typical solution is based on generating one time password (OTP) for a single session or transaction. Unfortunately in most of the general mechanisms used for generating one time password (OTP) randomness of OTP system breaks after certain period of time and hence passwords become predictable. To solve this problem, in this paper a novel OTP generation method has been proposed, which generates OTP from fingerprint features of the user. The OTP produced from the system is secure as it uses fingerprint features in the seed and RIPEMD160 hash function in OTP generation procedure.***

Index Terms: authentication, fingerprint, one-time-password, OTP generation, poincare index.

I. INTRODUCTION

Owing to the growing popularity of smart devices, security as well as privacy on such devices are of paramount importance since those act as a platform for online commerce besides their involvement in accessing crucial information [1-5]. Over time, smart devices have offered various superior functions that led to the growing interest of users in them but at the same time grew the vulnerability of users to fraud [6-8]. Accessing such crucial information and transacting securely necessitates safe measures that offer increased user adoptability as well as resistance to impending threats [2]. Ranging from a daily user of a personal computer to corporations, government departments, medical practitioners and businesses, security of file systems together with the protection of system from unprivileged access is a major security concern. Researchers and software companies are struggling in order to meet the improved demand of security of classified, confidential and sensitive information. In information security, one of the main concerns is the verification of an individual demanding access to confidential, classified and sensitive information as an authorized one. This can be achieved when that individual proves his identity by means of an authentication process. In other words, the individual should be able to justify his identity to access information and in case he fails to authenticate himself, access will not be granted. A vast number of applications are widespread on the internet that transfer sensitive information and financial transactions. Authentication of the users is a must in such applications in order to confirm their legitimacy. In general, an authorized user can be identified in three ways viz. what an individual knows, what an individual has, or what an individual is. Among the three, the usage of what a person knows i.e. passwords, etc. is the most common. The usage of what a person has i.e. One-Time-Password (OTP), tokens, smart cards, etc. is used for sophisticated authentication. The third method, what a person is, involves biometric technology [9]. In recent times, the most popular credentials used are static passwords. In order to evade the difficulty to remember complex passwords, users tend to behave heedlessly by setting up passwords that are easy to remember and are therefore weak as well as have low entropy. As a result, their poor and faulty password habits act as a security threat to online applications. Users have been provided with various solutions that are developed to rid them off the tedious task of creating and managing passwords. One of the most prevalent solutions is based on the generation of One Time Password (OTP) which is valid for a single transaction or session. However, the password generated remains afloat in the cellular network which has high chances of being intruded and this is the main security drawback in using OTP. Further, the majority of these authorization solutions does not comply with the usability and scalability constraints and thus become fragile in terms of continuality. As per Lux Research, there will be a dire need for the existing mobile payment systems to introduce biometrics for accelerating adoption and meeting the expectations of exorbitant growth rates. Their report infers that running a combination of biometric technologies on smart phones provided the best opportunity to advance growth rates of about 200 per cent in the year 2016 [9]. It has been observed that the usage of former two security schemes, which is called two-factor authentication, is not enough. As Per the latest DAG draft version, NIST (National Institute of Standards and Technology) acknowledges the proliferation of biometrics as an

Revised Manuscript Received on July 06, 2019.

Sajaad Ahmed Lone, Department of Electronics and Communication Engineering, National Institute of Technology, Srinagar, India.

A.H.Mir, Department of Electronics and Communication Engineering , National Institute of Technology, Srinagar, India.

authentication method SHALL be used with another authentication factor ('something you know' or 'something you have') [10]. Therefore, inclusion of biometric should be augmented to enhance the authentication strength by taking into consideration something the individual is. This implies utilizing some traits of the person that cannot be modified or mimicked easily, e.g. facial features, fingerprint, eyes, etc.

Biometric systems comprise of the following simple elements:

a) A sensor module for biometric data acquisition,
b) A feature extraction module for processing the acquired information to obtain feature vectors,
c) A matching module for comparison of feature vectors with the template ones,
d) A decision-making module meant for establishing the identity of a user or accepting/rejecting a claimed identity.

Any behavioral or physiological human feature may serve as a biometric trait if it fulfils the following four requisites:

a) Distinctiveness, i.e., no two must be identical,
b) Universality, i.e., each and every one must possess it.
c) Collectability.
d) Permanence, i.e. it should not vary over a given time-period.

As per the World Economic Report (WEF) [11], biometric features present a potential solution providing user convenience and security, especially in financial service. Nonetheless, there are many spots where biometric systems might be infringed [12]. Some of those threats have been taken up by researchers in the study [13], however, those systems have been found to be vulnerable to smudge and spoofing attacks. Although there are systems that offer security of biometric templates by biometric credential revocation, those solutions are limited, and underdeveloped standards prevail for evaluating those solutions. Regrettably, systems based on biometrics are highly vulnerable to replay attacks [14], thus, biometric based security solutions provide weaker security despite offering a high user adoptability. This study proposes the creation of one-time password generation mechanism based on fingerprint features using smart phones of identities.The paper is organized into following sections. Section II is an overview of related work, section III describes open issues in the existing systems. Section IV describes proposed OTP generation method using fingerprint features, Section V gives OTP generation algorithm. In the VI implementation of the proposed algorithm and section VII, VIII describes security analysis and conclusion respectively.

II. RELATED WORK

The various issues relevant to authentication and security of private and highly confidential information have been analyzed by many researchers. Research work presented in the paper highlights various techniques adopted in past to mitigate various types of attacks on the authentication system of users and solves the issue of securing entities.

Several methods have been put forward by researchers that replace the usage of complex passwords with smart cards, hardware tokens and chip modules [15-17] that offer enhanced security but have proven to be inconsistent, lack in user ergonomics and may be stolen, duplicated, lost or are difficult to manage or expensive thereby restricting their adoptability [14], [18]. In addition to this, security schemes in [19], [20] also exist that fail to function on devices with restricted resources like mobile phones which are mostly used for exchanging crucial information online thus making them highly susceptible [1], [21]. Besides, various facilities such as cloud technology focus on providing services to its users. But the approach employed by cloud technology for data sharing reveals several weaknesses thereby resulting in its vulnerability to many attacks [22-25]. Biometric systems automatically recognize a person based on his/her action and physical features. Biometrics is a field that authenticates an individual's traits, studies his/her measurable features, or recognizes his/her character [26]. Every individual has a fingerprint that is unique and does not vary. A fingerprint comprises of furrows and ridges of the finger's surface and has categories based on various key patterns including arches, loops and whirlpools [27], [28]. The depression and prominence and the minutiae point determine the fingerprint characteristics. Minutiae points refer to the topical characteristics at the endpoints of the ridges. Comparing all the visible information on the fingerprint is the best way of comparing fingerprints. Nevertheless, it is not possible realistically since it needs large amount of data to compare all the visible information which is infeasible for making a commercial system. The real commercial systems store the fingerprint characteristics, codes related to the locations of those points and not the fingerprint itself. When it comes to fingerprint authentication, it is a hot research topic particularly when employed in mobile devices. Various authentication mechanisms have been implemented on mobile devices that emerged as user adoptable solutions to identify the identity of an individual. A fingerprint authentication system was proposed in [13] that ran on mobile phones and was implemented on Android platform. They introduced three authentication algorithms to process the fingerprints and evaluated the speed and accuracy of each one of them. Another robust, cheap and secure fingerprint authentication mechanism was proposed in [29] that was implemented using Android and Open CV (Computer Vision) library. They employed the RGB matching algorithm. A new authentication system has been given in [30] that uses Contactless Smart Card (CSC) for holding the biometric traits, i.e., fingerprint recognition and iris scan. Such an authentication system has various fields of application such as airline information, logical access, law enforcement, border security, etc. These authentication systems seem easy-to-use, cheap and don't consume much battery of mobile devices. However, such schemes as based on fingerprints still lag because of absence of hardware on the mobile device for acquiring whole fingerprint together with the incongruity of the matching algorithms in case of cuts or dirt on a finger.

In the process of examining various mechanisms that were taken up in the past and existing systems, it was observed that the utilization of OTP appears to promise enhanced access management security in private and public network [21]. While performing a transaction unit, OTP is valid for a single attempt of access. The main advantage ofemploying OTP is the fail-proof security it provides against replay attack [31] that implies the unique password generated shall not be repeated ever again; thus, even if the password comes in the knowledge of attacker, it shall be futile. As a result, the usage of OTP has been examined for exploring a better prospect of making further developments in the process of authenticating a user [32][33]. Numerous authentication schemes have been put forward by researchers but those based on OTPs have been found to be the strongest among all. A mobile/web based authentication scheme for improving multi-factor authentication has been given by [34] which is compatible and secure. OTP keys have been generated using PingPong 128 stream ciphers that behave just like one time code. Dual communication channel i.e. GSM and TCP/ IP is used in this authentication scheme which is burdensome. A fuzzy vault scheme has been used by [35] for securing biometric data. A biometric authentication system based on speech recognition has been demonstrated in [36] but a single biometric used can be compromised by pre-recording the authenticated user's voice. An easy-to-implement framework for up-gradation of two factor authentication to three-factor authentication is proposed by [37]. The system makes use of three factors for user authentication i.e. password, smartcard and facial recognition. However, the system employs GSM besides being vulnerable to man-in-middle and imitation attacks. The security vulnerabilities of two factor authentications in ATM system have been explored in [38] and a three-factor authentication scheme is proposed for providing effective security to ATM banking transactions. However, the system uses a single biometric i.e. fingerprint information in addition to user PIN and smart-card. A onetime password key generation mechanism based on changed value and angle of fingerprint is proposed in [39]. This mechanism uses only one factor, that is, biometric to generate an OTP. Authors in [40] have presented an authentication mechanism based on smart card that preserves the characteristics of conventional authentication methods without any restriction on the log-in attempts. A one-way hash function has been utilized in this scheme, but the smart card emerges as additional hardware making the scheme expensive as well as inconvenient to the users and service provider alike. In [41], an OTP generation mechanism based on challenge response has been proposed by authors that functions on mobile phones and combines the authentication needed in various internet services. Therefore, the OTP MIDlet offers an automated solution to the users by reducing their burden. But this scheme requires multiple channels viz. internet and GSM for the exchange of authentication messages. Several OTP generation mechanisms [34][42] have been seen patented but their standardization is still a challenge owing to the assorted usage format as well as the architectures put forward by former protocol makers and researchers.

III. OPEN ISSUES

Some limitations have been found in the existing security solutions for access management by researchers that range from computational complexity to adoptability to the usage of different media. The review carried out in this section concludes with the deduction of open issues which have been given as:

1. Majority of the OTP generation methods used in study are based on time –synchronization between the authentication server and client, mathematical algorithms to generate new passwords based on previous password and mathematical algorithm where new password is based on challenge. In these methods the randomness of OTP system breaks after a cretin long period of time and passwords can be predicted.
2. Additional hardware required in some authentication schemes [43][44] like smartcards cause inconvenience to the user and prove costly to service provider. As a result, such authentication schemes are not technically adoptable. Therefore, the technical adoptability of those systems is being hampered because they lack user-friendliness.
3. The contemporary authentication mechanisms [45][46] have been found to have several issues such as increased processing time, computational cost, reduced system speed and huge storage due to the employment of fuzzy vault schemes, public key operations and self-updating hash chains.
4. Employment of weak password generation techniques viz., AES, SHA-1, MD5, etc. in most of authentication systems [47][48] makes them vulnerable besides failing to support in due course of time owing to technological advancements
5. Popularly used biometrics like voice, iris scan and facial features encounter certain issues when used for authentication. The speech authentication system can be compromised as the intruder can record the voice of the authenticated user and use this recorded voice to break through speech recognition system on which the proposed authentication mechanism is based. Further, iris scanners need proper lighting else they can lead to false results [49].
6. Another possible scenario that has not been considered in the previous studies is the Man-in-the-Middle attack. This attack scenario employs an illicit proxy server located between theauthentication server and the communication channel. At thearrival of a service request, after authentication token generation, the token passes through the unsafe routes leading the crucial information to the attacker. And when the information is stolen, the attacker may configure the whole authentication system easily and thereon, the attacker would have permanent access to resources. Such attack scenarios have not been observed to be considered in the previous works thus being an open issue.

IV. PROPOSED OTP GENERATION MECHANISM

To secure most sensitive and critical information organizations are implementing multifactor authentication i.e. identifying users by validating two or more factors that are unique. From last several years SMS based one-time passwords were introduced as an additional factor in multifactor authentication to counter various types of attacks against authentication and authorization of internet services. From the study, it has been observed that majority of the OTP generation mechanism are based on time-synchronization, mathematical algorithm to generate one time random password. The randomness of these OTP systems break after certain long period and password becomes predictable. Moreover, utilization of hash functions such as SHA1, MD5 are used in certain OTP generation schemes which are no longer considered secure algorithms in cryptography.SHA-1 proffers many concerns when implemented on a public network and thus should not be chosen (or should be modified) by an investigator when the experimentations are to be performed in large public networks with an advanced level of unguided intrusion events. Thus, the study adopts RIPEMD160 in place of the error-prone and traditional SHA-1 algorithm. Biometrics authentication methods now a day is becoming protocol of prevention for unauthorized access, fraud and other kinds of attacks. These methods authenticate and authorize individuals based on their physiological/ behavioral characteristics [50]. These properties of these characteristics of the individuals are unique and reasonably permanent and do not change. The introduction of biometrics as the level of authentication added with two factors or multifactor authentication will undoubtedly enhance the efficiency of the authentication mechanism in comparison to the conventional usage of password, tokens/smartcards or their combination. The purpose of this study is the generation of human readable OTP based on biometric (fingerprint) that can be used for authentication purpose which will overcome the constraints mentioned above. One of the noteworthy enhancements that has been performed was ensuring a higher security incorporation.

V. THE PROPOSED OTP ALGORITHM

The data flow and architecture based on fingerprint-based OTP authentication technique is described in fig 1. Theproposed system utilizes fingerprint features of the user as an initial seed for generating one-time password. The algorithm progresses as follows.

1. The user or client registers with the authentication server their fingerprints which form the initial seed from which OTP is generated.
2. The features from fingerprint is extracted and converted into string. Complete process of extracting features and converting them into string is described in VI
3. The seed generated from the previous two steps is fed to RIPMED160 for hash generation. In the proposed algorithm 160-bit hashing and 160-bit random number shall be employed. It shall serve two advantages: i) 160-bit hash are more secure ii) TOTP already standardized a Dynamic Truncation method of 160-bit hash values for deriving 6 digit OTP numbers. For 160 bit hashes, SHA 1 is the most popular, but attacks are existing at the theoretical level with SHA 1. RIPEMD 160 thus emerges as a better choice.
4. The next step in the OTP generation process as shown in fig 1 involves a 160-bit random number generation that is XORed with the 160-bit message digest generated in the last step to yield a 160-bit pass.
5. Dynamic truncation is performed to convert this 160-bit pass into 24-byte pass.
6. The 24-byte pass is converted into a 6 digit, human readable and user-friendly OTP.
7. The OTP generated can be then transmitted using SMS, push message, e-mail, etc

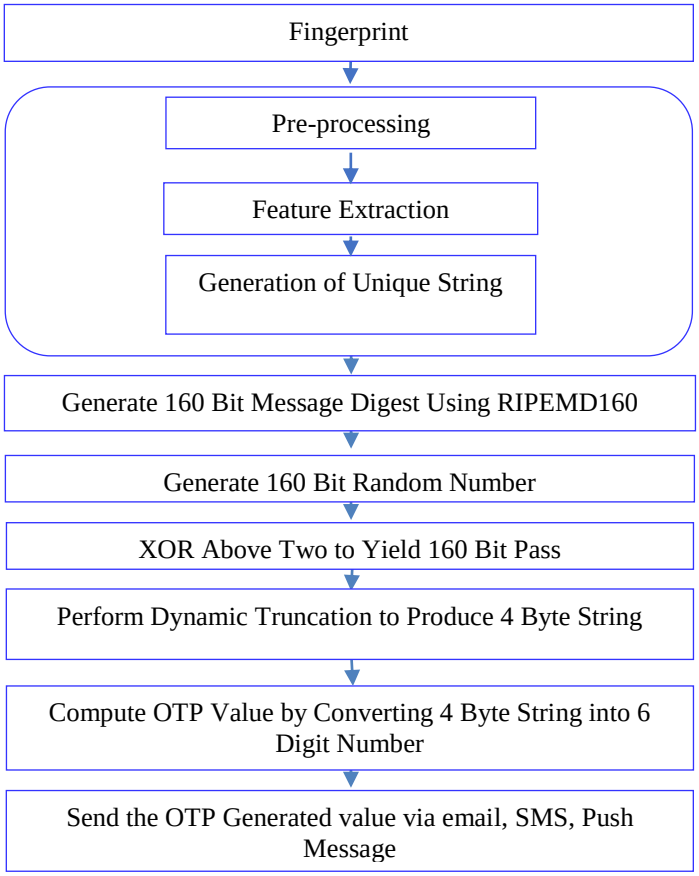

Fig 1Proposed OTP Generation Process

VI. UNIQUE STRING GENERATION FROM FINGERPRINT FEATURES

Fingerprints is most known biometric trait to authenticate people. It has been used by government and law enforcement agencies for a long time and is considered as a unique and reliable identifier. When subjected to testing, fingerprint has proven to have the highest level of securityand no effort to fool the device has been reported. Though there may be some factors like dirt, cosmetics, age that lead to false positives and false negatives but generally, the error rate has been found to be 1 in 500+ making this feature relatively better than other biometrics [50]. A fingerprint is distinct pattern of ridges and valleys on finger surface of an individual. Ridge is raised portion of the epidermis on the fingers and is continual throughout the individual's life. Whereas valley is the area between two adjacent

ridges. Ridges and valleys often run in parallel; sometimes they bifurcate and sometimes they terminate. Based on the pattern of ridge formation fingerprints are classified into three basic categories namely arch, loop and whorl as shown in fig 2.

Fig. 2. Fingerprint Categories

On the fingerprint surface ridge ending, minutiae points that is ridge bifurcation or spots (ridge ending) etc. are most evident structural characteristics which can be determined very easily. The uniqueness of the fingerprint is determined by these features. The fingerprint also contains two important areas 'core' and 'delta' points also referred as singular points at these points there is abrupt change in ridge pattern and curvature of ridge is higher than normal. These points are strongly stable and scale invariant and are therefore most important global characteristics of a fingerprint. Core points are the most reliable among the singular points as they can be found in most fingerprints. It is topmost point of the innermost ridge lines and has highest curvature in fingerprint ridge. Core points is unique point in fingerprint which can serve as reference points to calculate other minutiae points with this point as origin. Two different fingerprints are differentiated from each other by examining and comparing the minutiae characteristics where they occupy the same relative area and position. Many approaches have been proposed in the study for the detecting singular points based on orientation field image. In the proposed study, Poincare Index Method is used which is popular and practical method to detect these points from the fingerprint [51]. To apply Poincare Index Method image on input image it must be transformed in orientation field image. The Poincare Index is defined for each point in the orientation field image and generally computed by considering some elements around the point. Poincare index is calculated by taking the consecutive points field angle difference and summing it, the point enclosed by a digital curve (Core Point) will have highest Poincare index. We consider the case where 8 positions are taken around a particular target point. For a position (i, j), let $(i_0, j_0) = (i, j + 1)$, $(i1, j1) = (i + 1, j + 1)$, $(i2, j2) = (i + 1, j)$, $(i3, j3) = (i + 1, j-1)$, $(i4, j4) = (i, j-1)$, $(i5, j5) = (i-1, j-1)$, $(i6, j6) = (i-1, j)$, and $(i7, j7) = (i-1, j+1)$. Let $\theta(i, j)$ be the (i, j)-element of an orientation field image and $0 \leq \theta(i, j) < 2\pi$ for any (i,j).

$$\text{Let } \delta k(i, j) = \theta(i_{k+1}, j_{k+1}) - \theta(i_k, j_k) \qquad (1)$$

for $0 \leq k \leq 6$ and $\delta 7 = \theta(i_0, j_0) - \theta(i_7, j_7)$. Then the Poincare Index of an element (i,j) is defined to be

$$P(i, j) = 1/2\pi \sum_{k=0}^{7} \Delta_k(i, j) \qquad (2)$$

where

$$\Delta_k(i, j) = \begin{cases} \delta_k(i, j) & \text{if } |\delta_k(i, j)| < \pi/2 \\ \pi + \delta_k(i, j) & \text{if } \delta_k(i, j) \leq -\pi/2 \\ \pi - \delta_k(i, j) & \text{otherwise} \end{cases} \qquad (3)$$

The Poincare Index have the value ½ ,0,- ½ or 1.The core point is expected to occur at the point where Poincare Index value is ½ . Once core point is extracted it is easy to find other minutiae points like ridge ending, termination, bifurcation etc. by taking core point as reference. For reliable extraction of the minutiae points in fingerprint quality of the input image is must. So, before extraction of fingerprint minutiae features quality of the input image is enhanced by going through pre-processing step by applying certain filters like 2-D median and 2-D adaptive wiener filter to remove noise and image quality. After applying these filters ridge pattern of fingerprint can be clearly seen and feature points can be properly extracted. After image enhancement fingerprint minutiae extraction begins with converting enhanced image into binary image that is converting each pixel into 0 and 1. Ridge thinning also known as skeletonisation is done to make entire ridge line one pixel thick and shows a single line skeletal view of the fingerprint ridge pattern. The next step to be followed to extract minutiae points from fingerprint is minutiae marking and is important step which involves the concept of cross number. Cross number is most widely used method for minutiae extraction in the thinned binarized image. Rutovitz's definition of crossing number for pixel P is given by (4)

$$C_n(P) = \frac{1}{2}\sum_{i=1}^{8} |P_i - P_{i+1}| \qquad (4)$$

Where Pi is the binary pixel value in the neighborhood of P with Pi=(0 or 1) and P1=P9. The crossing number $C_n(P)$ of a point P is defined as half of cumulative successive differences between pair of adjacent pixels belonging to 8 neighborhoods of P. The crossing number properties can be used to classify a ridge pixel as ending, bifurcation or non-minutia point. Following Table 1 shows property of crossing number.

Table 1 Property of Crossing Number

Cross Number $C_n(P)$	**Properties**
0	Isolated Point
1	Ridge End Point
2	Continuous Ridge Point/Normal Point
3	Bifurcation Point
4	Crossing Point

After minutiae marking the image has to undergo minutiae post processing step as there will be lot of spurious minutia introduced by the earlier stages. The different processes applied to image to eliminate spurious minutiae are as follows.

a) If the distance between one termination and one bifurcation is smaller than a particular distance D, these minutiae are removed.
b) If the distance between two bifurcation is less than D, these minutiae are removed.
c) If the distance between two termination is smaller than D, the minutiae are removed.

Where D is the Euclidean Distance which in this study is taken as 6 pixels. After removing the spurious minutiae image will be still having large number of unique minutiae which are needed to generate the unique string. For this only those minutiae which are centered around core point will be considered. Now the image only has a minimum number of minutia points. The position of the minutiae points centered around core point are described by their coordinates in the X-axis and Y-axis and orientation angle relative to the origin. Hence the minutiae points will be reshaped into NX3 matrix which will be having minutia x coordinate, y coordinate and orientation angle. This matrix is then converted into unique string.

VII. IMPLEMENTATION AND RESULTS

For implementation of the proposed algorithm Fingerprint Verification Database 2002 was used which contains approximately 800 images of 100 individuals with size 374X388 and resolution of 500 dpi. Core point which is used as a reference point in the proposed algorithm is provided of majority of the images in the data base. The fingerprint images after loading went through different pre-processing steps like enhancement, binarization, thinning before minutia points were extracted from the fingerprint. The matrix of NX3 is created to hold x,y coordinates and orientation angle of each minutia. The string generated from this matrix is used as initial seed in the proposed algorithm for OTP generation. The table 2 shows the fingerprint, corresponding message digest using RIPMD160 hash function and the final 6 digit OTP generated using proposed algorithm. The performance of proposed algorithm for OTP

Table 2 Fingerprint Samples, Message Digest and OTP's

Fingerprint	RIPEMD160 Hash	Final Six Digit OTP
	a85ba6e17194c0020f46df39c956a494ffd4a855	374139
	67e886366859f09ff1085cbe9433409db74739a9	325607
	91e2400d2f14ddf5636f24c303b3c75c2a23dc19	150657
	df1f33f553eb651c895d676aedc162770e1fbeb8	294435
	c27b990476f8c2f359e7855a2b458693f65e982e	126336

generation using fingerprint features is analyzed by with various parameters like False Acceptance Rate, False Rejection Rate etc.

a) False Acceptance Rate(FAR)-describes number of times someone is declared as legitimate user incorrectly
b) False Rejection Rate (FRR)- describes number of times someone is declared illegitimate user incorrectly.
c) True Acceptance Rate(TAR=1-FRR)-the frequency of a legitimate user accepted as true user.

In the proposed study the above parameters were calculated by taking threshold of 75%. The value mentioned in the table 3 were obtained for the proposed algorithm for FAR, FRR and True Acceptance Rate respectively.

Table 3 Performance of Proposed Algorithm

FAR	FRR	TAR
2%	2%	98%

VIII. SECURITY ANALYSIS

There are various mechanisms used for OTP generation proposed in the current study Most general OTP's are generated by authentication servers which are based on time or some mathematical algorithms. However, in these mechanisms randomness of the OTP systems breaks after certain longer period and passwords become predictable. So,

these OTP mechanisms have disadvantages of having to exchange OTP token after certain period. To remove such weakness OTP generation mechanism has been proposed which uses fingerprint features of user as seed to generate OTP. Selection of good seed is very critical for robustness of any security model hence use of fingerprint features in the proposed model as seed creates unpredictable outputs, thus defending it against guessing attacks. In the proposed method RIPEMD-160 is used as cryptographic hash function which produces strong 160-bit hash string from fingerprint features. RIPEMD-160 is cryptographic hash function suggested as drop in substitution of SHA-1. Even though RIPEMD-160 relies on same design principles as MD5 and SHA-1, the dual streamstructure makes RIPEMD-160 more secure against recent attacks on the other members of MD4 family. Brute force attack will be resisted by the proposed scheme as brute force depends only on the bit length of the hash value and not on the specific algorithm. In the proposed OTP generation scheme RIPEMD-160 bit hash function is used to produce hash fingerprint features which is then XORed with 160 bit random number .In order to find hash value adversary will need level of effort will be proportional to 2^{160}., An adversary has to exhaustively examine a search space of possible combination of which is equal to 2^{160} only to get hash value in worst case , more complexity is added for such an attack by XOR operation and dynamic truncation of the hash. The proposed scheme is not susceptible to reply attacks, man in middle and forged attacks as one time password generated through this scheme is valid only for one authorization or authentication request. Even if valid OTP is intercepted by adversary it cannot be used in subsequent login as OTP is restricted to short time window. The proposed scheme also makes it difficult for adversary to generate a new OTP from last observed one because of huge computational cost.

IX. CONCLUSION

Authenticating user on the internet websites is most important factor in any business. One of the most secure authentication mechanism compared to traditional password used by organizations to validate their users is OTP. Most of the general mechanisms used to generate these OTP's are based on time and mathematical algorithms**,** randomness of these OTP system breaks after certain period and hence passwords become predictable. Therefore, there is need to develop a secure and user friendly OTP generation process and one such method has been proposed in current study. The model uses fingerprint features of the user as the initial seed to generate OTP. The use of fingerprint features in the seed make it difficult for the intruder to predict the output and hence makes it secure against guessing attacks. In this system RIPEMD160 has been used as hash function to generate OTP, which is then send via email, SMS to the mobile number of the user. Although the basic design of our system can be rooted from the idea formulated by Eldefrawy, still it has some of the potential contributions of results and accomplishments which are quite unique in its nature. The base technique has used conventional One-Time password by means of two-factor authentication using the SHA1 algorithm. It has been strongly argued by NIST that currently, SHA1 is not the most potential cryptographic hash function. Therefore, our first contribution can be stated as incorporating of fingerprint features in the seed and a latest hash function RIPEMD160 in our system. Adopting this technique of enhancement will yield an OTP that is potentially strong compared to the basic approach.

REFERENCES

1. Islam SH, Biswas GP. A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. Journal of Systems and Software. 2011 Nov 1;84(11):1892-8.
2. Darwaish SF, Moradian E, Rahmani T, Knauer M. Biometric identification on Android smartphones. Procedia Computer Science. 2014 Jan 1; 35: 832-841.
3. Khan BUI, Olanrewaju RF, Baba AM, Langoo AA, Assad S. A compendious study of online payment systems: Past developments, present impact, and future considerations. International Journal of Advanced Computer Science and Applications. 2017 May 1; 8(5): 256-271.
4. Pampori BR, Mehraj T, Khan BUI, Baba AM, Najar ZA. Securely eradicating cellular dependency for e-banking applications. International Journal of Advanced Computer Science and Applications. 2018; 9(2): 385-398.
5. B. U. Islam Khan, R. F. Olanrewaju, F. Anwar and M. Yaacob, "Offline OTP Based Solution for Secure Internet Banking Access," *2018 IEEE Conference on e-Learning, e-Management and e-Services (IC3e)*, Langkawi Island, Malaysia, 2018, pp. 167-172.
6. De Marsico M, Galdi C, Nappi M, Riccio D. Firme: Face and iris recognition for mobile engagement. Image and Vision Computing. 2014 Dec 1; 32(12): 1161-1172.
7. Masihuddin M, Khan BUI, Mattoo MM, Olanrewaju RF. A survey on e-payment systems: elements, adoption, architecture, challenges and security concepts. Indian Journal of Science and Technology. 2017 May 25; 10(20) 1-19.
8. Olanrewaju RF, Khan BUI, Mattoo MM, Anwar F, Nordin AN, Mir RN. Securing electronic transactions via payment gateways–a systematic review. International Journal of Internet Technology and Secured Transactions. 2017; 7(3): 245-269.
9. "Mobile Payments Need Biometrics to Improve User Experience and Adoption", Luxresearchinc.com, 2016. [Online]. Available: http://www.luxresearchinc.com/news-and-events/press-releases/read/mobile-payments-need-biometrics-improve-user-experience-and. [Accessed: 05- Feb- 2019].
10. NIST Special Publication Digital Authentication Guidelines https://pages.nist.gov/800-63-3/sp800-63b.html [Acessed 10-Feb-2019].
11. McWaters R. A Blueprint for Digital Identity. World Economic Forum. 2016.
12. Ratha NK, Connell JH, Bolle RM. An analysis of minutiae matching strength. 3rd International Conference on Audio-and Video-Based Biometric Person Authentication (AVBPA). Springer, Berlin, Heidelberg. 2001 Jun 6: 223-228.
13. Conti V, Collotta M, Pau G, Vitabile S. Usability Analysis of a Novel Biometric Authentication Approach for Android-Based Mobile Devices. Journal of Telecommunications and Information Technology. 2014 Oct 1; (4): 34-43.
14. Smith DF, Wiliem A, Lovell BC. Face recognition on consumer devices: Reflections on replay attacks. IEEE Transactions on Information Forensics and Security. 2015 Apr; 10(4): 736-745.
15. Lee WH, Lee R. Implicit sensor-based authentication of smartphone users with smartwatch. Proceedings of the Hardware and Architectural Support for Security and Privacy. ACM. 2016 Jun 18: p. 9.
16. Aboud SJ. Secure Password Authentication System Using Smart Card. Journal of Emerging Trends & Technology in Computer Science (IJETTCS). 2014; 3(1): 75-79.
17. Jeong J, Chung MY, Choo H. Integrated OTP-based user authentication and access control scheme in home networks. Proceedings of the 41st Annual Hawaii International Conference on System Sciences. Springer, Berlin, Heidelberg. Waikoloa, HI. 2008: 1-7.
18. O'Gorman L. Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE. 2003 Dec; 91(12): 2021-2040.
19. Andreeva E. Secret sharing in continuous access control system, using heart sounds. 2012 XIII International

Symposium on Problems of Redundancy in Information and Control Systems (RED). IEEE. 2012 Sep 5: 5-6.
20. Meng W, Wong DS, Furnell S, Zhou J. Surveying the development of biometric user authentication on mobile phones. IEEE Communications Surveys & Tutorials. 2015 Jul 1; 17(3): 1268-1293.
21. Mehraj T, Rasool B, Khan BUI, Baba A, Lone P. Contemplation of Effective Security Measures in Access Management from Adoptability Perspective. International Journal of Advanced Computer Science and Applications. 2015; 6(8): 188-201.
22. Olanrewaju RF, Khan BUI, Mattoo MM, Anwar F, Nordin AN, Mir RN, Noor Z. Adoption of Cloud Computing in Higher Learning Institutions: A Systematic Review. Indian Journal of Science and Technology. 2017 Oct 25; 10(36): 1-19.
23. Olanrewaju RF, Khan BUI, Baba A, Mir RN, Lone SA. RFDA: Reliable framework for data administration based on split-merge policy. SAI Computing Conference (SAI). IEEE. 2016 Jul 13: 545-552.
24. Khan BU, Baba AM, Olanrewaju RF, Lone SA, Zulkurnain NF. SSM: Secure-Split-Merge data distribution in cloud infrastructure. 2015 IEEE Conference on Open Systems (ICOS). IEEE. 2015 Aug 24: 40-45.
25. Mir MS, Suhaimi B, Adam M, Khan BUI, Mattoo MMUI, Olanrewaju RF. Critical security challenges in cloud computing environment: an appraisal. Journal of Theoretical & Applied Information Technology. 2017 May 31; 95(10): 2234-2248.
26. Pankanti, S., Bolle, R. M., and Jain, A., Biometrics: The Future of Identification. IEEE Computer magazine, February, 2000.
27. L. Hong, A. K. Jain, ”Classification of Fingerprint Images”, MSU Technical Report, MSU Technical Report MSUCPS:TR98-18, June 1998.
28. Jain, A., and Pankanti, S., Fingerprint Classification and Matching. Handbook for Image and Video Processing, A. Bovik (ed.), Academic Press, April 2000.
29. Rathi K, Sawarkar S. Finger Print Matching Algorithm for Android. International Journal of Engineering Research & Technology (IJERT). 2013: 2(10): 3819-3823.
30. M. David, G. Hussein and K. Sakurai, “Secure Identity Authentication and Logical Access Control for Airport Information Systems”, Security Technology, 2003. Proceedings. IEEE 37th Annual 2003 International Carnahan Conference on, 2003, pp. 314 - 320.
31. "Mobile operating system", Wikipedia, 2016. [Online]. Available:http://en.wikipedia.org/wiki/Mobile_operating_system. [Accessed: 10- March- 2019].
32. X. Duan and B. Niu, "A change password attack resistant scheme for remote user authentication using smart card", 2016 IEEE International Conference of Online Analysis and Computing Science (ICOACS), 2016.
33. U. Deore and V. Waghmare, "Cyber security automation for controlling distributed data", 2016 International Conference on Information Communication and Embedded Systems (ICICES), 2016, pp. 1-4.
34. B. Davaanaym, Y. Lee, H. Lee and S. Lee, "A Ping-Pong Based One-Time-Passwords Authentication System", in INC, IMS and IDC, 2009. NCM '09. Fifth International Joint Conference on, Seoul, 2009, pp. 574-579.
35. K. Moon, D. Moon, J. Yoo and H. Cho, “Biometrics Information Protection Using Fuzzy Vault Scheme”, in Signal Image Technology and Internet Based Systems (SITIS), 2012 Eighth International Conference on, Naples, 2012, pp. 124 - 128.
36. H. Ma, S. Yan, X. Bai and Y. Zhu, “The Research and Design of Identity Authentication Based On Speech Feature”, in Sensor Network Security Technology and Privacy Communication System (SNS & PCS), 2013 International Conference on, Nangang, 2013, pp. 166 - 169.
37. P. R. Avhad and R. Satyanarayana, “A Three-Factor Authentication Scheme in ATM”, International Journal of Science and Research (IJSR), vol. 3, no. 4, pp. 656-659, April 2014.
38. J. N. Oruh, “Three-Factor Authentication for Automated Teller Machine System”, IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), vol. 4, no.6, pp. 160-166, December 2014.
39. Cha, Byung Rae, Yong Il Kim, and Jong Won Kim. "Design of new P2P-enabled Mobile-OTP system using fingerprint features." Telecommunication Systems 52.4 (2013): 2221-2236.
40. Y. Chang, C. Chang and J. Kuo, “A secure one-time password authentication scheme using smart cards without limiting login times”, SIGOPSOper. Syst. Rev., vol. 38, no. 4, pp. 80-90, 2004.
41. S. Hallsteinsen, I. Jørstad and D. Van Thanh, “Using the mobile phone as a security token for unified authentication”, in Systems and Networks Communications, 2007. ICSNC 2007. Second International Conference on, Cap Esterel, 2007, p. 68.
42. V. Shivraj, M. Rajan, M. Singh and P. Balamuralidhar, "One time password authentication scheme based on elliptic curves for Internet of Things (IoT)", 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW), 2015, pp. 1-6.
43. W. Hsieh and J. Leu, "Design of a Time and Location Based One-Time Password Authentication Scheme", in *Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International*, Istanbul, 2011, pp. 201-206
44. S. Aboud, "Secure Password Authentication System Using Smart Card", *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, vol. 3, no. 1, pp. 75-79, 2014.
45. X. Duan and B. Niu, "A change password attack resistant scheme for remote user authentication using smart card", *2016 IEEE International Conference of Online Analysis and Computing Science (ICOACS)*, 2016.
46. S. Aboud, "Secure Password Authentication System Using Smart Card", *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, vol. 3, no. 1, pp. 75-79, 2014.
47. U. Deore and V. Waghmare, "Cyber security automation for controlling distributed data", *2016 International Conference on Information Communication and Embedded Systems (ICICES)*, 2016, pp. 1-4.
48. M. Alzomai and A. Josang, "The Mobile Phone as a Multi OTP Device Using Trusted Computing", in *Network and System Security (NSS), 2010 4th International Conference on*, Melbourne, VIC, 2010, pp. 75-82.
49. H. Ma, S. Yan, X. Bai and Y. Zhu, “The Research and Design of Identity Authentication Based On Speech Feature”, in Sensor Network Security Technology and Privacy Communication System (SNS & PCS), 2013 International Conference on, Nangang, 2013, pp. 166 - 169.
50. Jain, Anil K., Patrick Flynn, and Arun A. Ross, eds. *Handbook of biometrics*. Springer Science & Business Media, 2007
51. Bo, Jin, Tang Hua Ping, and Xu Ming Lan. "Fingerprint singular point detection algorithm by Poincaré Index." *WSEAS Transactions on Systems* 7.12 (2008): 1453-1462.

AUTHORS PROFILE

Mr Sajaad Ahmed is research scholar at Department of Electronics and Communication Engineering, National Institute of Technology Srinagar, Jammu and Kashmir India. He received his Mastersin Information Technology from Guru Gobind Singh Indraprastha University, New Delhi, India. His research interests include network security anddigital imageprocessing.

Dr. Ajaz Hussain Mir is a Professor in the Department of Electronics and Communication Engineering at National Institute of Technology, Srinagar. He received his BE in Electrical Engineering with specialization in Electronics and Communication Engineering. He received his MTech and PhD in Computer Technology from the IIT Delhi (India) in 1989 and 1996 respectively. He is a Chief Investigator of Ministry of Communication and Information Technology, Govt. of India project: Information Security Education and Awareness (ISEA). He has been guiding PhD and MTech theses in digital image processing, computer networks and other related areas and has several international publications to his credit. His areas of interest are biometrics, image processing, security, wireless communication and networks.