Secured 6-Digit OTP Generation using B-Exponential Chaotic Map

Rasika Naik, Udayprakash Singh
Electronics and Communication Engineering,
Sir Padampat Singhania University, Udaipur,
Rajasthan, India 313001

***Abstract*—Today, the traditional username and password systems are becoming less popular on the internet due to their vulnerabilities. These systems are prone to replay attacks and eavesdropping. During the Coronavirus pandemic, most of the important transactions take place online. Hence we require a more secure method like one-time password generation to avoid any online frauds. one-time password generation has multiple techniques. With one-time password generation it has become possible to overcome the drawbacks posed by the traditional username and password systems. The one-time password is a two-way authentication technique and hence secure one-time password generation is very important. The current method of one-time password generation is time-consuming and consumes a lot of memory on backend servers. The 4-digit one-time password system limits its uses to 9999 users and with advance deep learning approaches and faster computing it is possible to break through the existing one-time password generation method. Hence we need a system that is not vulnerable to predictive learning algorithms. We propose a 6-digit one-time password generation technique based on a B-exponential chaotic map. The proposed 24-bit (6-digit) long one-time password system offers 120 times higher security as compared traditional 4-digit systems, with a faster backend computing system that selects 24-bits out of 10^8 bits in 89 seconds at 1.09 Kilo-bits per milliseconds. The proposed method can be used for online transactions, online banking, and even automated teller machines.**

Keywords*—*One-time password generation; B-exponential chaotic map; 6-digit one-time password; online transactions; security

I. Introduction

Our manuscript introduces a 6-digit OTP generation system using the B-exponential chaotic map. The methods that are currently used to generate OTPs such as time-based OTP and hash-based OTP are prone to brute force attacks, forging attacks, etc. This leads to the research question, "Whether there was another method that could be used to generate a highly secure OTP system that was less prone to such threats?". Chaotic maps that are widely used for their highly random behavior were chosen to check whether they can be used to produce highly random OTPs. Also, instead of 4-digit OTPs, our objective is to make a system that generates 6-digit OTPs with a limited validity time makes it extremely difficult for a general computer to crack the OTP with brute force.

To prevent unauthorized access, access restriction methodologies are used [1]. The unauthorized attacker should be prohibited from making any changes to the system, at the same time the authorized user should not face any difficulties in accessing or updating the system [2]. Traditional identification control used badges and passwords to control the access authentication and provided a security safeguard [3]. Money transfers, mobile merchanting, account checks, and payment of different types of expenses (school fees, medical bills, and residential maintenance) are some of the examples of rapidly expanding mobile banking operations. Because an attacker can perceive some part of the key, conventional passwords are vulnerable to replay attacks and type scheme assaults [4]. Although ID/password methods are vulnerable to eavesdropping and replay attacks they are still better than only password systems because of the added unknown factor of the user name [5]. Most of the users tend to forget their passwords and hence they write them down or store them on a PC. This poses a greater threat to the traditional security system. To overcome the weaknesses of the traditional method, the One-Time Password (OTP) solution has been proposed [6]. OTP is an additive system that requires a new key to be entered by the user every time along with the user name and password. OTP was initially called a One Time Authorization Code (OTAC) [7]. It is a dynamic password that remains valid for a certain amount of time or till the successful login within a session. In earlier days, the OTPs were sent to a keyring fobe device or pager. The OTP generation algorithm is typically a pseudo-random algorithm that is difficult to be guessed by the attacker. The additive cryptographic hash functions make it very difficult to derive or guess the OTP. Some of the recent literature [8] has shown time-dependent OTPs, thus making it hard for the attacker to guess them.

An OTP is suitable for signing in to sessions or financial deals on any digital device like a computer, mobile. OTPs avoid several flaws associated with traditional (static) password-based authentication; some implementations also include two-factor authentication by ensuring that the one-time password requires access to both something a person has (such as a device with the OTP calculator built-in, or a smartcard or specific cell phone) and something (such as a PIN).

This manuscript proposes a mechanism for generating an OTP using a bit file generated by a pseudo-random sequence generator. This pseudo-random sequence generator uses the B-exponential chaotic map. Each session generates a 6-digit random OTP that will provide more security than the 4-digit OTP systems.

Fig. 1 shows the conceptual diagram for 6-digit (24-bit) OTP generation using B-exponential chaotic map. As per this concept, after inserting an ATM card into the machine, the user enters the correct user name and password. After validating the username and password, the bank server generates a 6-digit

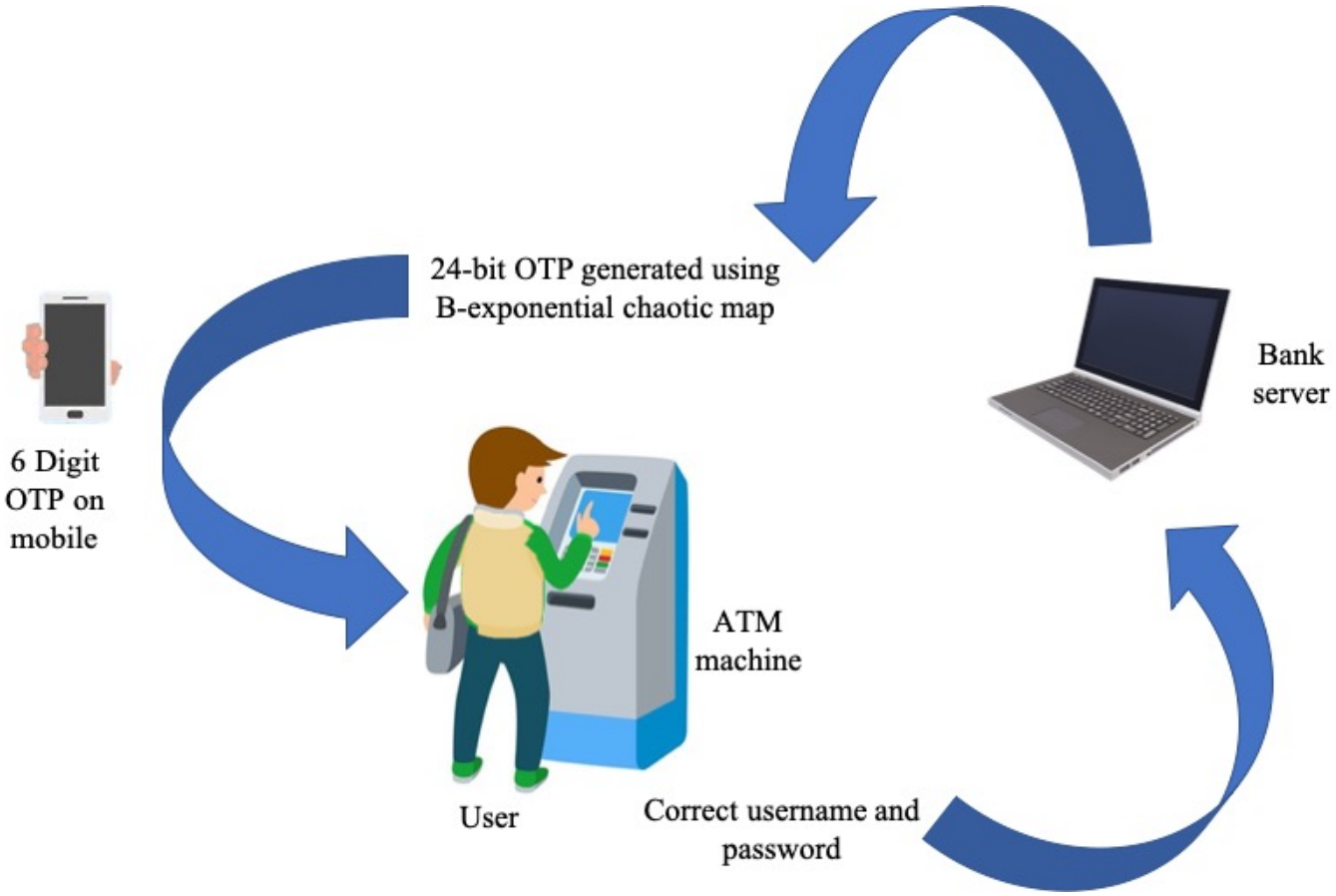

Fig. 1. Concept Diagram of 6-digit (24 bit) OTP Generation using B-exponential Chaotic Map. A user Enters the Correct User Name and Password after Inserting an ATM Card into the Machine. Upon Validation of Correct User Name and Password, Bank Server Generates 24-bit OTP using B-exponential Chaotic Map. This 6-digit OTP is sent on a Registered Mobile Number where the User will Enter the same in the ATM Machine.

(24-bit) OTP using a B-exponential chaotic map. This 6-digit OTP is sent to the user's registered mobile number, which the user enters into the ATM machine. This ensures a transfer to be secured on four levels. The first level is the user must have an ATM card. The second level is the user should know his or her personal username and password. Third, the mobile on which the OTP is sent should be in the network and in the same cell as the ATM machine. Finally, the B-exponential chaotic map is used to generate the time dependant OTP that makes the system more secured.

In this proposed methodology, we have shown how a 6-digit OTP can be generated using a novel B-exponential chaotic map method. Although this method was reported earlier in 2006, no one has ever used it generates a 6-digit OTP and validated using the NIST SP800-22.

We have proposed this system as with the increasing demand for online transactions, there is a need to develop a system that offered higher accuracy and security. The existing systems are more susceptible to brute force attacks. Also, as compared to 4-digit OTP systems 6-digit OTPs provide higher security. There are many ways that OTPs can be created but by using chaotic maps we provide a fast and simple method for OTP generation. Chaotic maps are simple to implement and also produce thousands of bits in a few milliseconds providing more security. They also have a special feature where they create a unique key that allows us to decode the OTP.

The manuscript has been organized into five distinct sections. The first section is the 'Introduction' section. It introduces the need to develop secure OTP systems and also highlights how chaotic maps can be used in them. The 'Literature review' section summarizes the most recent literature available on OTP generation systems. The 'Methodology' section explains in detail the steps we followed to implement our proposed OTP generation system. The 'Results and discussions' section mentions all the results that were obtained while implementing the system and also discusses these results and the future scope of the system. The final 'Conclusion' section briefly summarizes the entire manuscript.

II. Literature Review

Many efforts have been taken by different research groups in order to develop robust OTPs.

Most of the OTP generation techniques suggest time-based OTP [9], [8] and others have used Hash-based Message Authentication Code (HMAC) [10]. Recently, a captcha based OTP [11], real-time eye-tracking based OTP [12] where also proposed. Some of the researchers have also tried a combination of hashed and time-based OTP [9], [13]. RSA SecureID time-bas generates a safe OTP after specific seconds based on

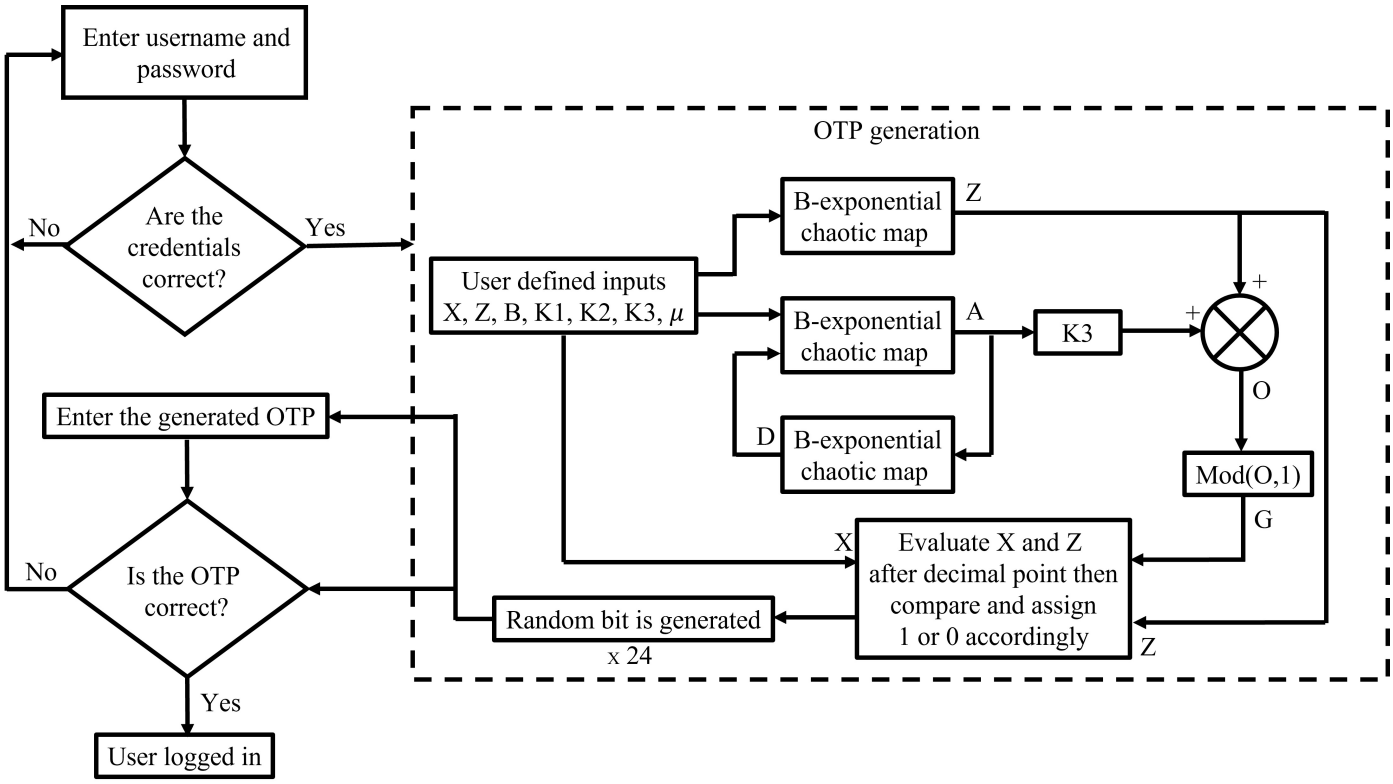

Fig. 2. Flow Diagram of OTP Generation using B-exponential Chaotic Map. The User Enters the User Name and Passwords and its Credentials are Checked. If the Credentials are False then the user is asked to Enter User Name and Password again. If the Credentials are Correct then the OTP Generation Algorithm is called on the Server-side. Once the OTP is Generated, User is asked to Enter that OTP and its Validation is Done. If the User Enters a Valid OTP then the OTP System allows him to Log in, else User Name if prompted for User Name and Password again. During the OTP Generation, User-defined Inputs are Passed through Three B-exponential Chaotic Maps. A Closed-loop Output of the B-exponential Chaotic Map Loop is Weighted and then Added to the Non-loop Output. This Summation is Modulo Operated and then Generated Bit is Evaluated against User Input and B-exponential Chaotic Map Output. The Final Evaluation is One Random Bit and this Process is Repeated 24 Times to Get the Final OTP.

arithmetic functions using the internal clock and stored seed. Each token carries its own initial value or conditions. However, these codes can be hacked because there is no reciprocal authentication. Time-based OTPs suffer from man-in-the-middle attacks. There were some attempts made to generate soft-token systems having unrivaled tamper resistance. Hardware tokens or keyring fobe devices or USB-based tokens with embedded chips were also implemented.

Lamport's technique [14] is the most common algorithm to generate hash chain-based OTPs (HOTP). These techniques are either OTP mechanism based on time to produce the OTP, like the algorithms suggested by El *et al.* [15] and Nugroho *et al.* [16], or hardware-based HOTP algorithm, like Lamport's [14] or S/Key [17].

Despite the widespread use of HOTPs in protocols like Secure Socket Layer (SSL), IPsec, and others. Algorithms used in HOTPs are typically vulnerable to attacks like collision, forging, and birthday attacks [18]. In comparison to time dependant OTPs, HOTP systems have additional flaws like more hashing steps and complicated computations, thus increasing resource utilization. Nontraditional bilinear map-based OTP developed by Lee *et al.* [19] was found to be vulnerable to insider attacks.

Chaotic maps can also be used for implementing other applications. There are many chaotic maps that are available. Akgul *et al.* [20] have proposed a random number generator using chaotic order systems.They test the algorithm with NIST 800-22, Federal Information Processing Standards (FIPS) 140-1, and ENT. Flores *et al.* [21] implemented a chaotic cryptosystem using a multi-precision algorithm. They had used four chaotic maps Rossler, TinkerBell, logistic, and Henon. Saber *et al.* [22] have developed a PRNG using a Lemniscate Chaotic Map (LCM). Deng *et al.* [23] have used chaotic maps to encrypt digital images using a scrambling algorithm.

Chaotic maps are not the only mechanisms for OTP generation. There are many recently reported works that generate OTP in a novel manner. Kumar *et al.* [24] have built an OTP generation system that uses the Vigenère cipher algorithm. They use this algorithm as it is not complex and still provides very high randomness which is required for OTP generation. Goel *et al.* [25] have proposed a system that uses cryptography and cloud computing to create a secured connection for Internet of Things (IoT) systems. They implemented the algorithm on MATLAB software and compared it with other methods. Kadum *et al.* [26] developed a novel OTP generation algorithm by generating an unsystematic key. They have created a random number and then ciphered plaintext. The random key created can make different ciphering texts.

The OTP generation is not only useful for secure banking and transactions but can also be used in encryption as a key.

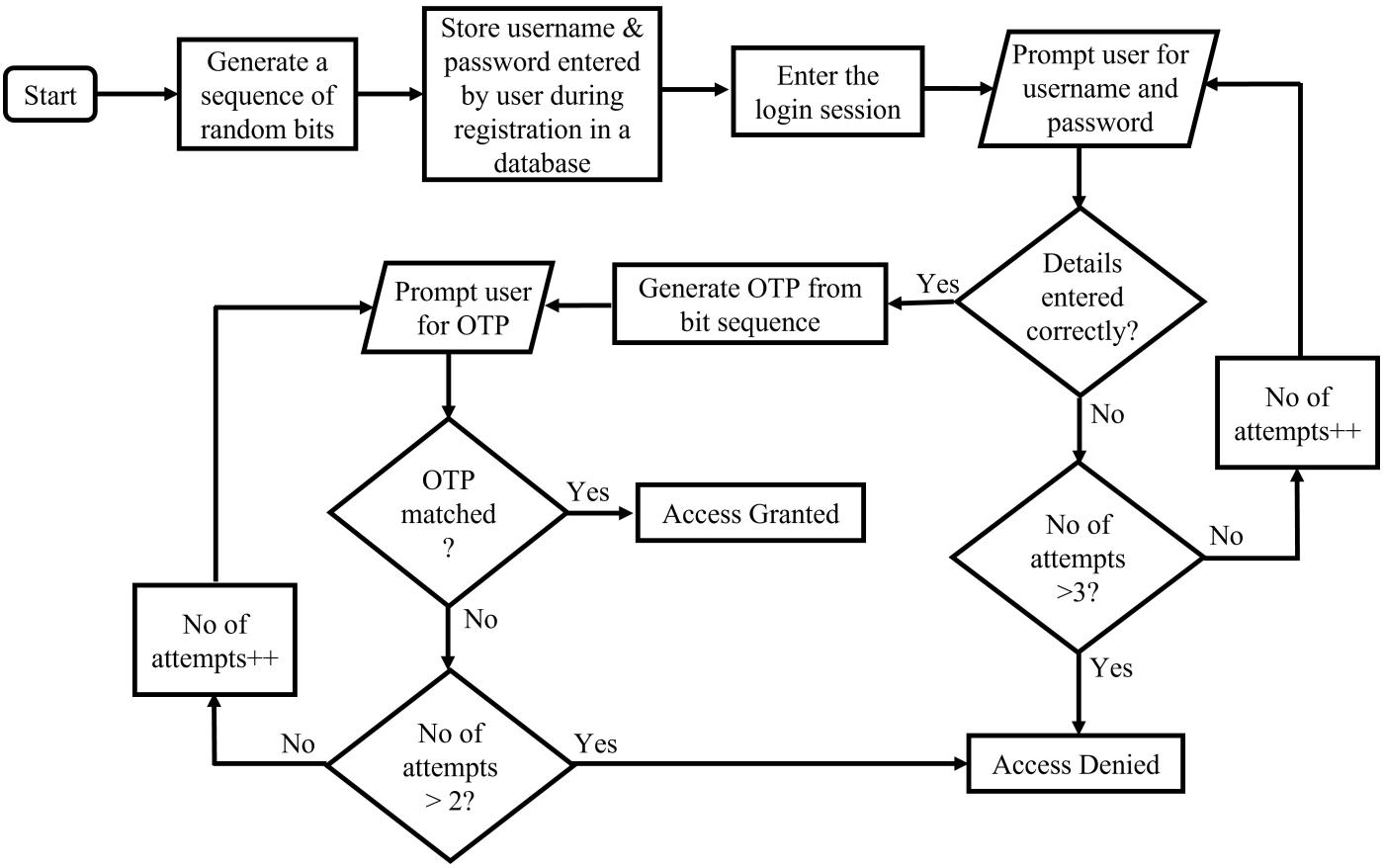

Fig. 3. Flowchart of the Proposed Methodology. A Random Bit Sequence is Generated Anticipatorily to Save Time during the Real-time Execution of the Proposed Method. A Database is Created to Store all the User Names and Passwords. All the Valid User Names and Passwords were Entered into the Database during Registration. A Login Session is Created for the User. The User is Prompted for the User Name and Password. If the Details are Entered Correctly then a 24-bit OTP is Generated else three more Attempts are given to the User before the Access is Denied. Once the OTP Generation is Completed, the User is Prompted for the OTP. If the OTP is Matched, the Access is Granted else two more Attempts are given to the User before the Access is Denied.

Thus a secure OTP generation algorithm will help in other applications as well. Recently, Shakir *et al.* [27] have developed an image encryption system. Using the Haar transform, One-Time Pad, and Playfair algorithms they have created an image encryption algorithm and then applied the Inverse Fourier Transform to get a ciphered image. The decryption is done by reversing the encryption method.

A. Challenges and Limitations of Existing Systems

A hash-based OTP suffers from an attacker who can position himself in front of hash and can access clear private information. A time-based OTP system relies on seed sequence and right counter. Such systems can be vulnerable if an attacker knows the right time and seed sequence. Although, it is very difficult to predict the time in advance as well as seed-sequence determination is still a challenge. physical token have concerns like being stolen, destroyed, running out of batteries, and clock drifting that takes hours to correct. There have been attacks reported using malware and sheet-based phishing.

From the survey done it was seen that the existing methods suffer from various attacks that can put private information at risk. Man-in-the-middle attacks and seed determination attacks are some of the major flaws of these OTP generation systems. Even tokens generated for OTP creation can be hacked into. To work on these drawbacks we have proposed a B-exponential chaotic map-based 6-digit OTP generation technique.

III. Methodology

Fig. 2 shows the flow diagram for OTP generation using a B-exponential chaotic map. According to the concept, when a user enters the username and password, the credentials are checked; if the credentials are incorrect, the user is prompted to enter the username and password again. If the credentials are correct, the server-side OTP generation algorithm is invoked. Once the OTP is generated, the user is prompted to enter it, and the OTP is validated. The OTP system allows the user to log in if he enters a valid OTP. If the OTP entered is incorrect then the user is prompted to enter the username and password again. User-defined inputs are passed through three B-exponential chaotic maps during the OTP generation process. The B-exponential chaotic map loop's closed-loop output is weighted and then added to the non-loop output. This summation is modulo-operated, and the generated bit is compared to the user input and the output of the B-exponential chaotic map. The final evaluation is one random bit, and the process is repeated 24 times to produce the final OTP.

Fig. 4. Different Output Cases. Case (a): In the First Attempt, the User Enters the Wrong Password after which the User is Prompted to Enter the Login Details again. In the Second Attempt, the User Enters the Correct Credentials and is then Prompted to Enter the Generated OTP. Once the Correct OTP is Entered by the User in the First Attempt, they are Granted Access. Case (b): The User Enters the Wrong Credentials in the First Attempt. The User is then Prompted to Enter the Login Details for the Second Time. The Details Entered by the User are Invalid in this Attempt as Well and the User is then Offered a Third Chance. Since the Details Entered in the Third Attempt are also Incorrect, the User is Denied Access. Case (c): Initially the User Enters the Correct Credentials. The User is then Prompted to Enter the Generated OTP. The OTP Entered by the User is Wrong in the First and Second Attempts. Hence, the User is Diverted Back to the Login Page. This Time the User Enters the Correct Login Credentials and OTP and is given Access. Case (d): The User Enters the Incorrect Credentials in the First Two Attempts and is given a Third Chance to Enter the Right Details. Once the User Enters the Right Login Details in the Third Attempt they are Prompted to Enter the OTP. As the OTP Entered by, the OTP Matches the Randomly Generated OTP, the User is Granted Access.

A. OTP Generation using B-exponential Chaotic Map

During the OTP generation, user-defined inputs (X, Z, B, K1, K2, K3, μ) are passed through three B-exponential chaotic maps. The B-exponential chaotic map closed-loop output (A) is weighted (multiplied by K3) and then added to the non-loop output (Z). This summation (O) is modulo-operated by 1, and the generated bit (G) is compared to the user input (X) and the output of the B-exponential chaotic map (Z). The final evaluation is one random bit, and the process is repeated 24 times to produce the final OTP.

B. OTP Generation Process Flow

Fig. 3 shows the flowchart of the proposed methodology. As per this concept, to save time during the proposed method's real-time execution, a random bit sequence is generated ahead of time. A database is created to store all of the usernames and passwords. During registration, all valid usernames and passwords were entered into this database. For the user, a login session is created. The user is prompted to enter his or her username and password. If the details are entered correctly, a 24-bit OTP is generated; otherwise, the user is given three more attempts before access is denied. When the OTP generation is finished, the user is prompted to enter the OTP. If the OTP is matched, access is granted; otherwise, the user is given two more attempts before access is denied.

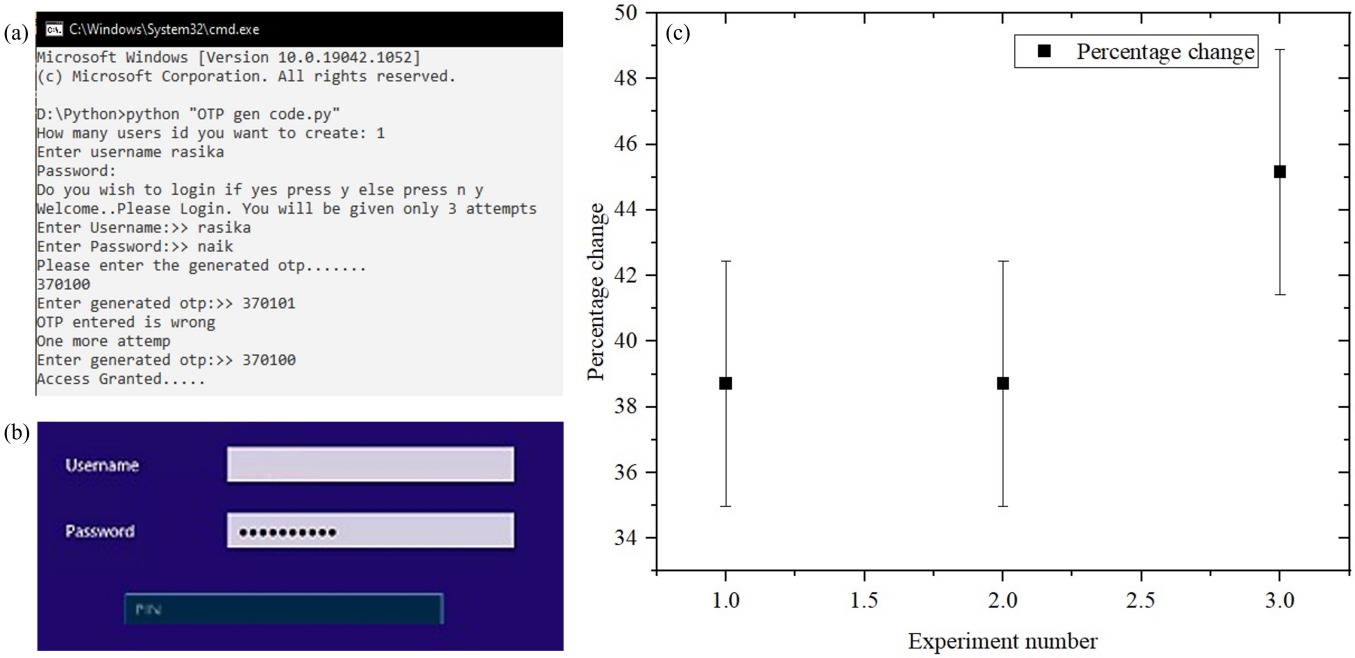

Fig. 5. (a) Console Output shows User has Entered the Right Password, one Wrong OTP and still gets Access Granted since the User has Entered Correct OTP on the Second Attempt. (b) Final Front-end UI showing User Name, Password and Pin. The Password is Masked and the Pin is Deactivated. (c) Different Experiments Carried with User Input Versus Percentage Change in Bits. In the First and Second Attempts, almost 40 % bits were Changed and in the Third Attempt, almost 46 % Bits Changed showing the Time Dependency on the OTP Generation for the same Set of Inputs.

TABLE I. VALIDATION OF BIT-STREAM GENERATED USING NIST SP800-22 TESTING PARAMETERS

Statistical case	P-Value	Proportion of passing	Result
ApproximateEntropy	0.437274	0.98	Success
BlockFrequency	0.153763	0.99	Success
CumulativeSums (Forward)	0.699313	0.97	Success
CumulativeSums (Backword)	0.595549	0.98	Success
(Fast Fourier Transform) FFT	0.304126	0.99	Success
Frequency	0.032923	0.98	Success
LinearComplexity	0.987896	0.98	Success
LongestRun	0.275709	0.98	Success
NonOverlappingTemplate	0.5125662466	0.98	Success
OverlappingTemplate	0.191687	0.98	Success
RandomExcursions	0.439636625	0.99	Success
RandomExcursionsVariant	0.645271	0.99	Success
Rank	0.678686	0.99	Success
Runs	0.401199	0.98	Success
Serial	0.1782745	0.975	Success
Universal	0.383827	0.97	Success

IV. RESULT AND DISCUSSION

Fig. 4 shows the various output scenarios obtained. Initially, the users are given the option to enter the number of login IDs they want to create. They are then asked to enter the login ID and password. This information is stored in a database. Fig. 4(a) shows the first case where the user enters the incorrect password on the first attempt. The user is now left with two more attempts to enter the right credentials. In the second attempt, the user enters the correct credentials. After this, he/she is prompted to enter the OTP generated by the proposed B-exponential chaotic map. The duration of the OTP generation process is 00:01:29 and the entire process takes 00:1:53. Once the OTP is generated by the system and received by the user, he/she is then prompted to enter the OTP. Since the OTP entered by the user matches the generated OTP, the user is granted access. Fig. 4(b) shows the second case where the user enters the incorrect credentials on the first try and is then left with two more attempts to enter the right credentials. On the second attempt, the user enters incorrect details again and is left with only one more try. Here on the third attempt, the user enters the wrong details again and is denied access. Fig. 4(c) shows the third case where the user initially enters the correct credentials. After that, the user is prompted to enter the OTP generated by the proposed B-exponential chaotic map. In the first attempt, the user's OTP is incorrect. This leaves the user with one more attempt to enter the OTP. As the OTP entered by the user does not match the generated OTP, he/she is redirected to the login page. The user is then prompted to enter the login credentials once again. Upon entering the correct credentials in the first attempt the user is prompted to enter the generated OTP. Once the OTP entered by the user matches the generated

TABLE II. COMPARISON BETWEEN THE EXISTING STUDIES REPORTED IN LITERATURE AND THE PROPOSED METHOD. THE ACCURACY IS OBTAINED FROM THE NIST TEST SUITE. OUR PROPOSED METHOD DEMONSTRATED BETTER CORRELATION COEFFICIENT AND ENTROPY THAN THE ONES REPORTED

Method	Accuracy (%)	Correlation coefficient	Entropy
De *et al.* [28]	99	-	-
Flores *et al.* [21]	98.39	-	-
Saber *et al.* [22]	-	0.0014	7.9980
Akgul *et al.* [20]	94	-	-
Tang *et al.* [29]	-	0.0857	7.990
Deng *et al.* [23]	-	0.0032	7.9931
Proposed method	98.45	0.00076	7.9999

OTP, he/she is granted access. This entire process takes a total time of 00:02:45 for completion. Here, the duration of the OTP generation process where the login details and OTP entered by the user are both entered correctly in the first attempt is 00:01:45. Fig. 4(d) shows the fourth case where the user enters the wrong credentials in the first attempt and is left with two more attempts to enter the correct details. As the details entered in the second try are incorrect the user is asked one last time to enter the right details. When the user enters the correct login information on the third try, they are prompted to enter the OTP. the entire process takes 00:1:53. Since the OTP entered by the user matches the OTP generated by the proposed B-exponential chaotic map the user is granted access.

Fig. 5 (a) shows the console output demonstrating the entries made by the user. The user entered the correct password, then entered one incorrect OTP but was still granted access because the correct OTP was entered on the second attempt. Fig. 5(b) shows the final front-end UI, displaying the username, password, and pin. The password has been masked, and the pin has been disabled. Fig. 5(c) shows the graph of user input versus percentage change in bits acquired from performing various experiments. In the first and second attempts, nearly 40 % of the bits were changed, and in the third attempt, nearly 46 % of the bits were changed, demonstrating the time dependency on OTP generation for the same set of inputs.

The proposed system was able to select 24-bits out of 10^8 bits in 89 seconds at 1.09 Kbits/ms. We have also checked the 4-digit password generation using the same B-exponential chaotic map and found that the probability of hacking 4-digital systems is 0.00012 using brute force attack. Whereas, the probability of hacking a 6-digit OTP generation system created using the B-exponential chaotic map was 0.000000991. This shows that the 6-digit OTP system provides 120 times higher security than a 4-digit OTP system. The maximum time-out period observed for the 6-digit OTP generation system was 15 minutes i.e. the OTP has to be reset within 15 minutes before it can become susceptible to brute force attack. The B-exponential chaotic map was also able to obtain a correlation coefficient of 0.00076 and an entropy of 7.9999. This proves that the chaotic map algorithm we have proposed is highly random and can produce secure output.

A. NIST Test Suite Result and Comparison

Table I shows the accuracy obtained for the bit-streams generated. The NIST SP800-22 testing parameters were used for validation purposes. The results obtained were, the system achieved a 98 % accuracy with a p-value of 0.43 and 196 successful attempts out of 200 for the approximate entropy statistical case. For the block frequency test, the system achieved a 99 % accuracy with 198 successful tests out of 200 with a p-value of 0.15. For the forward cumulative sums test, the system showed 97 % accuracy with 194 successful tests out of 200 with a p-value of 0.69. For the backward cumulative sums test, the system achieved a 98 % accuracy with 196 successful tests out of 200 with a p-value of 0.59. In the Fast Fourier Transform (FFT) test, the system successfully passed 196 attempts out of 200 with a 98 % accuracy and a p-value of 0.3. The system achieved 196 successful attempts out of 200 with a 98 % accuracy and p-value of 0.03 for the frequency test. For the linear complexity test, the system achieved a 98 % accuracy with 196 successful tests out of 200 with a p-value of 0.98. In the longest run test, the system successfully passed 196 attempts out of 200 with a 98 % accuracy and a p-value of 0.27. The system achieved 196 successful attempts out of 200 with a 98 % accuracy and p-value of 0.51 for the non-overlapping template test and also achieved 98 % accuracy for the overlapping template test with a p-value of 0.19. In the random excursions test, the system successfully passed 198 attempts out of 200 with a 99 % accuracy with a p-value of 0.43 and in the random excursions variant test it achieved a 99 % accuracy with a p-value of 0.64. The system also achieved a 99 % accuracy in rank parameter test with 198 successful attempts out of 200 and a p-value of 0.67. In the runs test the system was able to achieve a 98 % accuracy with 196 successful attempts out of 200 and a p-value of 0.4. The serial test showed an accuracy of 97.5 % with 195 successful attempts out of 200 with a p-value of 0.17 and the universal test achieved a p-value of 0.38 with a 97 % accuracy with 194 successful attempts out of 200. All the tests were passed with a successful result.

Table II provides a comparison between some of the works reported in the literature that use chaotic maps for different applications and our proposed method. The accuracy of 98.45 % which is obtained as a result of the NIST test suite indicates that our proposed system is one of the best. The correlation coefficient and entropy indicate the randomness of the proposed algorithm. It can be seen that with a 0.00076 correlation coefficient and 7.9999 entropy our system has outperformed the exiting works reported.

B. Data Science and OTP Generation

Chaotic maps are used in applications in which creating confusion in the initial data to encrypt it is required. They are dynamic systems. But due to their chaotic behavior, chaotic maps on their own are generators of huge amounts of random data. These maps lead to the generation of millions of unique

bits before repeating themselves due to their large periodicity. The huge amounts of data and random trajectory that the maps produce make it difficult for hackers to decipher them. Another application of chaotic maps relating to data science is that these maps are capable of encrypting the data available. A vast amount of data is available on the internet today and it is crucial to encrypt it to provide security and avoid hacking attacks. Chaotic maps are also valuable in encrypting images and audio files.

Due to the frequent usage of online websites and online transactions it has become important to secure data. OTP generation using chaotic maps plays a big role in this application. We have seen that OTP generated using chaotic maps is highly unpredictable and secure. This will allow users on the internet to continue secure browsing, protect their data and be safe from hackers.

V. Conclusion

Due to the vulnerabilities in traditional username and password systems, there was a need to develop a more secure system, especially due to the increased use of online transactions during the COVID-19 pandemic. We have developed a 6-digit OTP generation method over traditional 4-digit OTP using a novel B-exponential chaotic map. As the current methods of generating OTPs are time-consuming and uses a large amount of memory on backend servers, we developed a fast and less memory-consuming system. The 4-digit OTP system is limited to 9999 users, but with our 6-digit we could expand this database to 100 times more users which will be suitable for the upcoming 5G technology. The proposed 24-bit (6-digit) long OTP system was able to achieve 120 times more security than traditional 4-digit systems with a faster backend computing system that selected 24-bits out of 10^{8} bits in 89 seconds at 1.09 Kbits/ms. The proposed method is applicable to any online transactions or banking applications.

Declaration

Funding Information

No funding was involved in the present work.

Conflicts of Interest

Authors R. Naik and U. Singh declare that there has been no conflict of interest.

Code Availability

The codes will be made available upon reasonable request to the authors.

Authors' Contribution

Conceptualization was done by R. Naik (RN) and U. Singh (US). All the literature reading and data gathering were performed by RN. All the experiments and coding was performed by RN. The formal analysis was performed by RN and US. Manuscript writing- original draft preparation was done by RN. Review and editing was done by US. Visualization work was carried out by RN and US.

Ethics Approval

All authors consciously assure that the manuscript fulfills the following statements: 1) This material is the authors' own original work, which has not been previously published elsewhere. 2) The paper is not currently being considered for publication elsewhere. 3) The paper reflects the authors'own research and analysis in a truthful and complete manner. 4) The paper properly credits the meaningful contributions of co-authors and co-researchers. 5) The results are appropriately placed in the context of prior and existing research.

Consent to Participate

This article does not contain any studies with animals or humans performed by any of the authors. Informed consent was not required as there were no human participants. All the necessary permissions were obtained from Institute Ethical committee and concerned authorities.

Consent for Publication

Authors have taken all the necessary consents for publication from participants wherever required.

References

[1] T. Breaux and A. Antón, "Analyzing regulatory rules for privacy and security requirements," *IEEE transactions on software engineering*, vol. 34, no. 1, pp. 5–20, 2008.

[2] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner, "Smart locks: Lessons for securing commodity internet of things devices," in *Proceedings of the 11th ACM on Asia conference on computer and communications security*, 2016, pp. 461–472.

[3] A. Jøsang and S. Pope, "User centric identity management," in *AusCERT Asia Pacific information technology security conference*. Citeseer, 2005, p. 77.

[4] A. G. Chefranov, "One-time password authentication with infinite hash chains," in *Novel Algorithms and Techniques in Telecommunications, Automation and Industrial Electronics*. Springer, 2008, pp. 283–286.

[5] M. H. Barkadehi, M. Nilashi, O. Ibrahim, A. Z. Fardi, and S. Samad, "Authentication systems: A literature review and classification," *Telematics and Informatics*, vol. 35, no. 5, pp. 1491–1511, 2018.

[6] S.-D. Park, J.-C. Na, Y.-H. Kim, and D.-K. Kim, "Efficient otp (one time password) generation using aes-based mac," *Journal of Korea Multimedia Society*, vol. 11, no. 6, pp. 845–851, 2008.

[7] W. N. W. Muhamad, N. A. M. Razali, K. K. Ishak, N. A. Hasbullah, N. M. Zainudin, S. Ramli, M. Wook, Z. Ishak, and N. J. A. MSaad, "Enhance multi-factor authentication model for intelligence community access to critical surveillance data," in *International Visual Informatics Conference*. Springer, 2019, pp. 560–569.

[8] I. S. Shaik and M. Manoj, "Time based dynamic password (tbdp) system using variable insertion technique," *International Journal of Computer Applications*, vol. 113, no. 8, 2015.

[9] S. S. Gosavi and G. K. Shyam, "A novel approach of otp generation using time-based otp and randomization techniques," in *Data Science and Security*. Springer, 2021, pp. 159–167.

[10] S. ShanmugaPriya, A. Valarmathi, and D. Yuvaraj, "The personal authentication service and security enhancement for optimal strong password," *Concurrency and Computation: Practice and Experience*, vol. 31, no. 14, p. e5009, 2019.

[11] R. K. Devi, M. Muthukannan, S. H. Babu, A. Sivadasan, and S. Abinivesh, "Novel authentication mechanisms for hash code, captcha and otp in cyber security domain," in *2021 6th International Conference on Inventive Computation Technologies (ICICT)*. IEEE, 2021, pp. 62–68.

[12] H. K. SM, G. Pradyumna, B. Aishwarya, and C. Gayathri, "Development of personal identification number authorization algorithm using real-time eye tracking & dynamic keypad generation," in *2021 6th International Conference for Convergence in Technology (I2CT)*. IEEE, 2021, pp. 1–6.

[13] J. Keller and S. Wendzel, "Reversible and plausibly deniable covert channels in one-time passwords based on hash chains," *Applied Sciences*, vol. 11, no. 2, p. 731, 2021.

[14] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, 1981.

[15] S. A. El-Booz, G. Attiya, and N. El-Fishawy, "A secure cloud storage system combining time-based one-time password and automatic blocker protocol," *EURASIP Journal on Information Security*, vol. 2016, no. 1, pp. 1–13, 2016.

[16] E. P. Nugroho, R. R. J. Putra, and I. M. Ramadhan, "Sms authentication code generated by advance encryption standard (aes) 256 bits modification algorithm and one time password (otp) to activate new applicant account," in *2016 2nd International Conference on Science in Information Technology (ICSITech)*. IEEE, 2016, pp. 175–180.

[17] N. M. Haller, "The s/key (tm) one-time password system," in *Symposium on Network and Distributed System Security*, 1994, pp. 151–157.

[18] V. Shivraj, M. Rajan, M. Singh, and P. Balamuralidhar, "One time password authentication scheme based on elliptic curves for internet of things (iot)," in *2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW)*. IEEE, 2015, pp. 1–6.

[19] Y. Lee and H. Kim, "Insider attack-resistant otp (one-time password) based on bilinear maps," *International Journal of Computer and Communication Engineering*, vol. 2, no. 3, p. 304, 2013.

[20] A. AKGÜL, C. ARSLAN, and B. ARICIOĞLU, "Design of an interface for random number generators based on integer and fractional order chaotic systems," *Chaos Theory and Applications*, vol. 1, no. 1, pp. 1–18, 2019.

[21] A. Flores-Vergara, E. García-Guerrero, E. Inzunza-González, O. López-Bonilla, E. Rodríguez-Orozco, J. Cárdenas-Valdez, and E. Tlelo-Cuautle, "Implementing a chaotic cryptosystem in a 64-bit embedded system by using multiple-precision arithmetic," *Nonlinear Dynamics*, vol. 96, no. 1, pp. 497–516, 2019.

[22] M. Saber and M. M. Eid, "Low power pseudo-random number generator based on lemniscate chaotic map." *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 11, no. 1, 2021.

[23] Z. Deng and S. Zhong, "A digital image encryption algorithm based on chaotic mapping," *Journal of Algorithms & Computational Technology*, vol. 13, p. 1748302619853470, 2019.

[24] M. Kumar and S. Tripathi, "A new method for otp generation," in *Healthcare and Knowledge Management for Society 5.0*. CRC Press, pp. 213–228.

[25] A. Goel, D. K. Sharma, and K. D. Gupta, "Leobat: Lightweight encryption and otp based authentication technique for securing iot networks," *Expert Systems*, p. e12788, 2021.

[26] S. A. Kadum and S. M. K. Jawad, "New programmatic otp algorithm," in *Journal of Physics: Conference Series*, vol. 1818, no. 1. IOP Publishing, 2021, p. 012097.

[27] H. R. Shakir and S. A. Yassir, "Image encryption-compression method based on playfair, otp and dwt for secure image transmission," in *International Conference on Advances in Cyber Security*. Springer, 2021, pp. 95–113.

[28] L. G. de la Fraga, E. Torres-Pérez, E. Tlelo-Cuautle, and C. Mancillas-López, "Hardware implementation of pseudo-random number generators based on chaotic maps," *Nonlinear Dynamics*, vol. 90, no. 3, pp. 1661–1670, 2017.

[29] Z. Tang, Y. Yang, S. Xu, C. Yu, and X. Zhang, "Image encryption with double spiral scans and chaotic maps," *Security and Communication Networks*, vol. 2019, 2019.