iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.44573

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

Authentication Mechanisms in the Cyber Security Domain: Hash Code, OTP, and CAPTCHA

Smt. Chaya P[1], Neha Kowshik V[2], Deepthi Dhananjaya[3], Reshma[4]
[1]*Assistant Professor, Dept. of ISE, GSSSIETW, Mysore, India*
[2, 3, 4]*Dept. of ISE, GSSSIETW, Mysore, India*

Abstract: ***It is important to integrate security as part of system and software development. A computer can be accessed by anyone. Cyber security acts against hackers. Security begins with authentication. Access to systems, networks, databases, websites, and services are regulated using authentication. The most fundamental category of verification is done with usernames and passwords. In our paper, we propose new approaches to each of these authentication mechanisms, which include hash code message authentication, the Entirely Automated Public Turing Test to Notify Computer systems and Human beings Apart (CAPTCHA), and one-time passwords***

Keywords: Authentication, Cybersecurity, Fully Automated Public Turing Test to Distinguish Between Computers and Humans, hash codes, One-Time Passwords

I. INTRODUCTION

Internet is within the reach of every person. Cyber security acts against hackers. Cyber-attacks target other computers or networks. There are two kinds of cyber-attacks: those with the goal of shutting down computer operations and those which try to access computer data with administrative privileges. As a result, security is considered as part of the system and software development process. Authentication is critical as a security entry point. Authentication controls access to the secured resources system, communications system, database, website, and services. The most fundamental form of authentication involves the use of a password and username. Authentication mechanisms are used to validate users. Weak authentication results in the leakage of vulnerable documents such as credit and debit card numbers and identity. Some authentication mechanisms are 2-factor, multifactor, OTP, biometrics, and more. This paper concentrates on 3 authentication mechanisms: text verification utilizing hash code, Fully Automated Public Turing test to inform Computers and Humans Apart (CAPTCHA), & One Time Passwords, & recommends new methodologies for all.

II. OBJECTIVES OF THE PROJECT

1) To provide a secure and secured authentication system so that consumers may use the app without being concerned about cyber dangers.
2) Develop a novel technique like hash code generation, CAPTCHA and OTP to help in complete app protection.
3) Multiple security checks to reduce hacking and increase hacking time.

III. LITERATURE SURVEY

1) In this paper, the improved SHA-512 is used on web - based applications, specifically for password hashing. Hill cypher is used for the saline generation, in additional towards the hash function upgrade, to improve the strength of constructing hash tables which could be used as a cyberattack on the method. The evaluation of the similar passwords stored in the DB is used to generate hash collisions, which results in salt generation to generate an emerging hash message. The matrix encryption key generates 5 matrices based on the length of the concatenated user id, concatenated characters from the profile name and passcodes. In this procedure, the very exact password would produce a unique hash message, making it more reliable against potential attacks.
2) Because of the compression, non-linearity, confusion, & Neural Networks & diffusion properties of Chaos, a technological innovation based on Chaotic Neural Networks is being used to develop Hash functions in this paper. In contrast to present Hash functions based on CNN, the presented structure incorporates a robust Chaotic engenderer into neurons rather than relying on Chaotic maps that are basic. In truth, even against statistical attacks, simple chaotic maps are not very durable. To keep the strength of the hash function presented at the ICITST conference (2015) whilst reducing the complexity, a novel mechanism of Hash function is presented in the paper. In comparison to Secured Hash Algorithm-two & various Chaos-based Hash functions, the theoretical analysis & actual results show that the implemented structure is more efficient with reference to High Sensitivity of Message & strong Collision Resistance.

3) The novel one-way hash method will be constructed in two steps in this work. To begin, process the input data to a system of matrix by performing the necessary transformations to obtain the starting hash value. Next, use the result of the previous process to generate a summary for all these information and create the encrypted hash value conclusively. They converted the data into a matrix structure by employing each and every necessary modification to develop the original hash value. The output of first process in generating a summary is used to construct a secure hash value.

4) This document discusses Keccak, a SHA-3 (safe hash algorithm) module that includes padding and permutation. It's a one-way encryption method. This algorithm exhibits a high level of parallelism. FPGA was used to implement this. The implementation procedure is both quick and efficient. The goal of the method is to increase throughput while reducing the area. This would be a one-way encrypting procedure, and the technique demonstrated parallelism. This has been implemented on an FPGA. The procedure for carrying out the execution was exceedingly rapid and effective.

5) The production of fingerprint image Hash codes using the Freeman Chain code & message-digest algorithm derived on the binary representation is discussed in this research. The Freeman chain code collects as much information as feasible. The Freeman chain code gathers all possible picture boundaries and sets the initial x and y coordinates to x0 and y0. Hashcode by itself is insufficient for authentication or verification purposes, however it can be used in conjunction with a multifactor security architecture or it is only half secure. We use MATLAB2015a to execute Hash code generation. This research demonstrates why dactylograms Hash code can be used to uniquely identify a user or as an index-key or identity-key. The MATLAB investigation demonstrated why fingerprints hash code can detect a client quite well.

6) They propose to provide a new hash function strategy that use several chaotic maps to produce efficient differential hash functions in this paper. The message is split into 4 partitions, each of which is understood by a separate 1 Dimensional chaotic map unit to generate a hash code intermediate. The 4 codes are merged into 2 blocks, all of which is processed by a two-dimensional chaotic map unit separately. Uniting 2 parts of hash codes that yields the ultimate hash value. Simulation investigations are carried out, including hash distribution, statistical features of diffusion & perplexity, messages and keys sensitivities, collision tolerance, and flexibility. When compared to various current chaos-predicted hash algorithms, the findings show that the suggested expected hash scheme are simple, efficient, and has comparable characteristics.

7) This study proposes Style Area Captcha (SACaptcha), a novel image-based Captcha based on the interpretation of semantic data, deep learning algorithms & pixel-level segmentation. CAPTCHA was created to distinguish between computers and humans as a result of developers ability to enter PC frameworks using Pcs assault programs & bots. The work provided security against malicious PC applications & bots. This paper provided breakthrough evidence that present content CAPTCHAs are insufficient, whether for traditional CAPTCHAs focused on English letters & Arab numbers nor for CAPTCHAs based over an infinite letter set of languages.

8) This article resolves the issue by assessing the usability of CAPTCHAs which is a new-generation human-friendly mini game. The task was a challenge-reaction analysis to guarantee that the response was made solely by humans, rather than by modernised robots. The work provided protection against vengeful Computer programs and bots. This work provided compelling evidence that the customer's time is often reduced when compared to the old process, because the previous technique relied on content, whilst the new approach relies on games, and customer can attend the sport to authenticate as a personal.

9) They suggest a novel strategy to implementing the CAPTCHA technique with 3 Dimensional animation in this work, based on the limitation of computer's vision, that makes it resistant to cyberattacks and easy for users to recognize, and they utilized this method to create a 3 Dimensional animation verification code. The work allowed for the provision of a 3-dimensional liveliness confirmation code. This problem cannot be solved using a 2-dimentional still image confirmation code. CAPTCHAs were becoming increasingly popular as a result of the employment of advanced design recognition & Artificial Intelligence calculations, which made it possible to understand less difficult CAPTCHAs.

10) This study proposes a method for creating CAPTCHAs that emphasizes on the use of Arabic script. The suggested solution uses unique Arabic font types to generate CAPTCHAs. This CAPTCHA takes use of the limitations of Arab OCRs in deciphering Arabic text. In Arabic-speaking countries, the proposed approach is quite beneficial in terms of safeguarding resources from the internet. A scheme's usability survey was undertaken and was found to be adequate. The goal of the project was to master a variety of online administrations, such as email, internet shopping, web journals, and other forms of online involvement. A review of over a hundred and fifty persons was conducted to determine the coherence rate of CAPTCHA images. Those who took part in the survey came from non-Arabic-speaking countries and Arabic South Asian countries that could comprehend the Arabic content. Some tests were conducted in order to determine the CAPTCHA's empowering vigor.

11) They investigate the use of hand written recognition in the creation of CAPTCHAs for cybersecurity in this article. CAPTCHAs are automated reversed Turing tests that are programmed to pass almost all humans but fail cutting-edge computer systems. CAPTCHAs that are printed by machine and text-based which is increasing the widely used to thwart robot assaults. The work on automatic recognition of unrestricted penmanship continues to be a demanding examination task. The study looked into the use of handwriting recognition in the creation of digital security through CAPTCHAs. To examine the significance of CAPTCHA images, a group of over 100 participants was assembled.

12) They use a two-factor authentication approach called Time-Based OTP (TOTP) and a SHA 1 in this research. With this technique, Authentication of systems of an online site or site does not rely just on the password and username to access the accounts customer, but also on the customer receiving a token or code to sign in to the customer's profile. The authentication method that uses 2-Factor Authentication can handle possible future attacks on customer access rights misuse after being tested hundreds of times. To prevent client password abuse, the researchers employed 2-factor authentication study with the TOTP password & SHA 1 algorithm. Using a time-based single-time secret phrase & Sha1 Calculation 1 for site login validation security. The client submits a secret key & username gain access to the system. If the other side is scamming by capturing client passwords, the pass-key becomes insecure.

13) Using dynamically changing secure passwords and validation keys will undoubtedly make it much more difficult. Furthermore, OTP generators which are loaded with specific data are frequently predictable. The paper introduces a unique OTP generator that uses inputs that change randomly. After that, the suggested generator is deployed on a Smartphone, & the output is tested and reviewed. With randomly shifting inputs, an algorithm was run. The final product was evaluated and found to be suitable for use in IOT authentication services.

14) They propose leveraging changing position and angles of fingerprints features to generate a one-time password key for OTP in this study. Fingerprints are powerful personal authentication elements, and they can be used to generate a changeable password key for use just once. They also ran a simulation to test the proposed randomized password key generating process. The OTP method makes use of the placement and orientation of fingerprint characteristics. Using Dendrogram JMSL library, the prediction model is simulated. The study created unlimited secret password keys using nine homomorphic graphs. The research was compared to nine different graphs to show that it performed better than the other methods.

15) They suggest a way for generating 1 time password keys for OTP utilizing fingerprint features in this study. Fingerprints are effective personal authentication elements, and they can be used to generate a dynamic password key for a single occasion based on fingerprint traits. They also ran a simulation to test the suggested password key generating process. The initiative aided in the production of a one-of-a-kind OTP password key. The OTP system generates passwords based on fingerprint traits.

IV. COMPARISION TABLE

TITLE	AUTHOR	DESCRIPTION	DATE
Implementation of enhanced secure hash algorithm towards a secured web portal	E. De Guzman	Improved SH calculation-512 was used in word hashing for web applications.	2019
Secure hash algorithm based on efficient chaotic neural network	N. Abdoun, Khalil	In comparison to Secured Hash Algorithm 2 & Chaos-based Hash functions, the investigation revealed the structure's proficiency When it comes to strong Collision Resistant & High Message Sensitivities.	2016
New one way hash algorithm using non-invertible matrix	M. Abutaha	They converted the data into something like a matrix framework via combining all of the necessary transformations to create the first hash value. The first stage in creating a summary's output is used to construct a secure hash value.	2013
Design and implementation of keccak hash function for cryptography	M.A. Patil	It was a 1-way encryption procedure, and the technique demonstrated parallelism. This has been implemented on an FPGA. The procedure for carrying out the execution was exceedingly rapid and effective.	2015
A study on fingerprint hash code generation based on MD5 algorithm and freeman chain code	K. Prasad	The MATLAB investigation demonstrated why fingerprint hash code can detect a client quite well.	2018

A simple secure hash function scheme using multiple chaotic maps	M. Ahmad	To construct efficient variable-sized hash functions, this research used a variety of chaotic maps.	2017
Breaking text-based captchas and designing image-based captcha	M. Tang	CAPTCHA was created to distinguish between humans and computers as a result of developers ability to enter PC frameworks using PC assaulting robots and projects.	2016
Gamification of internet security by next generation CAPTCHAs	S. A. Kumar	The experiment was a challenge-response test to guarantee that the answer was created entirely by people, rather than improved robots.	2017
A CAPTCHA implementation based on 3D animation	J. T. Mei	The research revealed a method for creating a 3-dimensional liveliness confirmation code. This problem cannot be solved using a 2-Dimentional still image confirmation code.	2009
Cyber security using arabic CAPTCHA scheme	B. Khan	The effort benefited a variety of online administrations, including email, internet buying, web journals, as well as other digital participation, among others.	2013
Generation and use of handwritten CAPTCHAs	A. Rusu	The study on an automated recognition of unrestricted penmanship continues to be a demanding examination challenge.	2010
Implement time based one time password and secure hash algorithm 1 for security of website login authentication	H. Seta	To prevent client password abuse, the researchers employed 2-factor authentication study with the Time-Based OTP & (SHA 1) algorithm.	2019
A new secure onetime password algorithm for mobile applications	H. S. Elganzoury	Randomly varying inputs were used to feed the algorithm. The result was evaluated and found to be suitable for use in Internet - Of - things authentication services.	2018
Random password generation of OTP system using changed location and angle of fingerprint features	B. Cha	The position and orientation of fingerprint features are used in the OTP approach.	2008
Password generation of OTP system using fingerprint features	C. Kim	The project aided in the creation of a flexible password key for One Time Password.	2008

V. METHODOLOGY

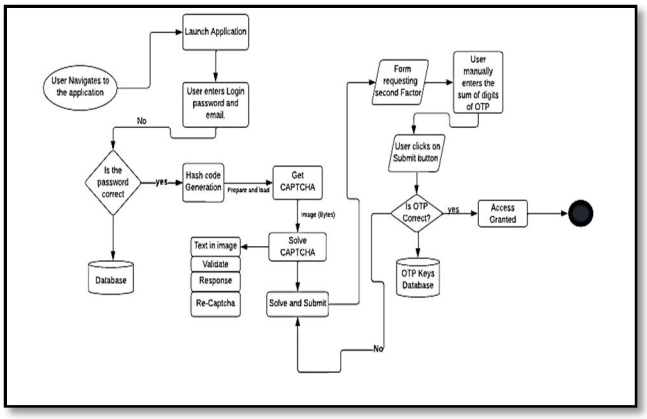


Figure 1: System Architecture

Figure 1 shows how the user interacts with the application represents the System Architecture of the entire application process. A user will interact with the web application with the front-end interface and will be login after providing valid credentials. The figure represents the front end and back end of the application. It represents the process of how hash code, CAPTCHA and OTP are generated.

The CAPTCHA code is generated using the site key and the action is based on score. The Hash code generated will be based on the time the user logs in and registers a complaint and that will unique for every person. The One-time password is generated after CAPTCHA code is entered. All the user's information is stored in MYSQL database. The OTP generated will be sent to mobile application and the user must type the sum of the digits in the text box which provides multiple security and safeguards the application.

A. Hash Code Generation

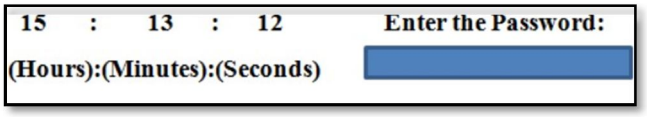


Figure 2: Time-based password Validation

The algorithm takes in the time when the user types in, and this will be unique for every user, substitution of each letter of the password will be made and this will used to generate hash code. Adler 32 is the algorithm which is being used to generate hash code. The substitution is done as follows.

Substitution Table
(included only lowercase letters)

a-x	j-x^2-y^2	s-xyz
b-y	k-y^2-x^2	t-y z x
c-z	l-z^2-x^2	u-zy x
d-x^2	m-x y	v-x^3
e-y^2	n-y z	w-y^3
f-z^2	o-z x	x-z^3
g-x + y	p-x^2+y^2	y-x^3+y^3+z^3
h-y + x	q-y^2+x^2	z-x^4
i-z + x	r-z^2+x^2	

Figure 3: Substitution table

Triple integration will be done after substitution to generate unique HASH CODE.

B. Captcha Generation

Figure 4: Scatter type CAPTCHA

Scatter type CAPTCHA is generated after Hash code generation is complete proving 2-step authentication.

C. OTP Generation

Present OTP Generations are just 4-digit and 6-digit OTPs which takes a few milliseconds to hack. The proposed technique involves 4-digit OTP which is being generated. When a user request for OTP, A 4-digit OTP will be generated and sent to the users registered device. This OTP is time-based OTP and will be valid only for that particular session. Once the OTP is generated a new technique is being introduced. Instead of just typing the received OTP in the text box, we implement a method as shown below.

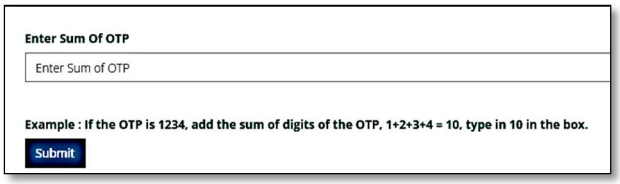


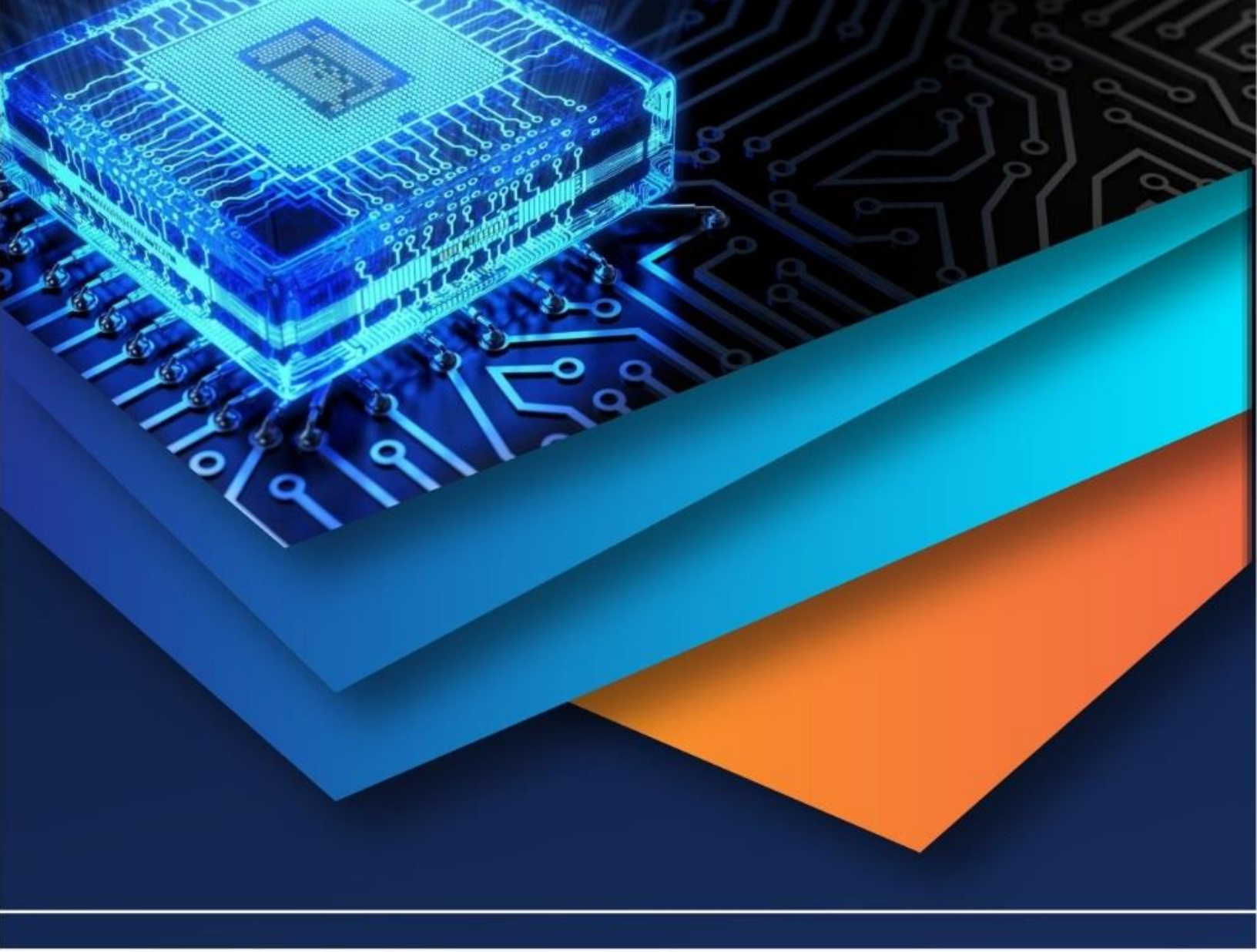
Figure 5: The sum of Digits in the OTP.

V. CONCLUSION

This study provides a revolutionary hash code, CAPTCHA, & One Time Password authentication mechanism that compresses cybersecurity authentication mechanisms. The suggested hash code approach includes a time factor in order to build a message hash code that is difficult to crack. To prevent robots from obtaining access to web resources, the suggested CAPTCHA approach employs simple yet effective aesthetic elements. To make it difficult to crack, the suggested OTP creation process employs unusual characters and a larger number of digits. The presented solutions are basic but effective cybersecurity authentication technologies. For all of these suggested authentication systems, further critical mathematical techniques can be employed in the future. Also, an overview of the literature on objects in real-time and non-real-time environments using a diversification of methodologies. The major goal of this research is to discover the right technology in use and to determine which technique is ideal for obtaining a final outcome.

REFERENCES

[1] F. E. De Guzman : "Implementation of Enhanced Secure Hash Algorithm Towards a Secured Web Portal," 2019
[2] N. Abdoun : "Secure Hash Algorithm based on Efficient Chaotic Neural Network," 2016 International Conference on Communications
[3] M. Abutaha : "New one way hash algorithm using non-invertible matrix," 2013 International Conference
[4] M. A. Patil : "Design and implementation of keccak hash function for cryptography," 2015 International Conference
[5] Aithal, Sreeramana : “A Study on Fingerprint Hash Code Generation Based on MD5 Algorithm and Freeman Chain code”.
[6] Ahmad, M : “ Simple Secure Hash Function Scheme Using Multiple Chaotic Maps”.
[7] M. Tang, H. Gao : "Research on Deep Learning Techniques in Breaking Text-Based Captchas and Designing Image-Based Captcha,"
[8] S. A. Kumar : "Gamification of internet security by next generation CAPTCHAs," 2017 International Conference
[9] J. Cui, J. Mei : "A CAPTCHA Implementation Based on 3D Animation," 2009 International Conference
[10] Bilal Khan “Cyber Security Using Arabic CAPTCHA Scheme Center of Excellence” in Information Assurance
[11] Rusu, A : “Generation and use of handwritten CAPTCHAs.”
[12] H. Seta : "Implement Time Based One Time Password and Secure Hash Algorithm 1 for Security of Website Login Authentication," 2019 International Conference.
[13] H. S. Elganzoury: "A new secure one-time password algorithm for mobile applications," 2018 35th National Radio Science Conference
[14] ByungRae Cha : "Random password generation of OTP system using changed location and angle of fingerprint features," 2008 8th IEEE International Conference
[15] B. Cha : "Password Generation of OTP System using Fingerprint Features," 2008 International Conference



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY