



ENHANCED SECURITY WITH MULTILEVEL AUTHENTICATION FOR ACCESSING BIOMETRIC DATABASE

Bharathi S¹, Abarna A², Arun Pandeewaran RV³, Akil G⁴

Department of Electronics and Communication Engineering,

Dr. Mahalingam College of Engineering and Technology, Pollachi -642003

Email: ¹bharathi_mani@yahoo.com; ²abarna7600@gmail.com; ³arunpandi210301@gmail.com;

⁴akilgopalsamy2000@gmail.com

ABSTRACT

Security is the process of safeguarding private data against unwanted access and change. Security concerns may jeopardize an organization's data storage by hackers with hostile motives attempting to obtain access to critical information. Currently, multiple authentications are unavoidable on mobile phones, systems, and online applications. However, the present system has shortcomings, like low optimization, weak security for varied attack rates, and also low accuracy. As a consequence, there is a need to create stronger security with layered authentication that overcomes the limits of current systems. Here, an enhanced security system with three-level authentication mechanisms for accessing biometric data bases is proposed. At the first level, the registration procedure utilizes three stages of numerical and textual passwords with an access key; at the second level, fingerprint authentication is applied; and at the third level, a random number code is provided to their email id. A random number is confirmed on the login screen and then logged in. The experimental process reveals that the suggested system offers greater security than the current solutions.

Keywords: fingerprint, random number, authentication, enhanced security, biometric database

1. INTRODUCTION

In any organization, authentication is a significant process in order to have secured access of their resources. There are different types of authentication techniques are available based on texts, graphs, tokens and biometric traits [1, 2]. Currently it is necessary to use more than one password at different levels for secure authentication, so that, the possibility of spoofing such a password is mostly reduced. Hence multi-level authentication technique can be used for ensuring a more firm authentication. Undoubtedly, user authentication is the most crucial aspect in information security. Authentication techniques may range from basic password-based authentication systems to costly-computationally complex authentication systems. Passwords are not only a key, but they also serve for various roles. They safeguard our secrecy and secure our sensitive information. The password authenticates us into a

system that validates our identity. They also impose no-rejection, prohibiting us from afterwards rejecting the legitimacy of our password-authenticated transactions. But passwords have certain weaknesses, several persons might have their information at the same time. In addition, there is a perpetual possibility of losing your password to individuals with nefarious intent. In order to overcome this notion of multilayer authentication is proposed in this paper.

Generally, authentication techniques employed, include token-based authentication, biometric authentication, and knowledge-based authentication. It is one of the most critical security services supplied to the system by various authentication methods or algorithms that must be provided so that only authorized persons have the right to access or administer the system. The system and the data associated to this information system are entirely secret. Users may configure or upload their own photos; secure susceptible systems are the benefits of this suggestion method. The different authentication approaches included in this suggested system are as follows: text-based authentication, fingerprint-based authentication, and random number generation-based authentication for accessing database.

1.1 Novice Authentication

Basic authentication is the initial step, which comprises field and length validations. Text-based authentication requires the user to submit a user id and password. This has been the most popular strategy over the past three to four decades. This is owing to the fact that it is easy to adopt, economical, and familiar to nearly everyone. There are case-sensitive alphabet letters, numbers, and special symbols in a text password. Recognition of bot assaults is more significant. For added safety, multidimensional passwords may be used at many levels i.e. we may construct a new password by combining one or more passwords supplied at separate times [3]. Even if one of the passwords in the created string is known, the usage of passwords at multiple levels offers an appropriate protection and prevent unwanted access.

1.2 Biometric Authentication

Authentication of a person using his/her physiological and behavioural characteristics is called Biometric Authentication. For example, each of the person's fingers, even identical twins, has a different fingerprint. An individual's fingerprint has a unique pattern of ridges and valleys. Fingerprint recognition devices for PC access are one of the most readily available commercial biometric technologies, and they are affordable from a range of manufacturers. When a large number of users are involved, however, this authentication mechanism may become excessively sluggish and expensive. Unless the reader is totally safe and secured due to inalterability, when biometric information is compromised, it may be simply changed. Biometric data is difficult to change and may be mechanically copied. This is viewed as a severe disadvantage since the tainted data cannot be corrected once identified. The user's password may be simply changed, but his or her fingerprint cannot. Fingerprints, for example, may be trapped on sticky tape and copied in fake gelatine, or simple photos of them may be presented.

1.3 Random number authentication

A random number generator that does not rely on real-world activity to construct its sequence is referred to as a pseudorandom number generator (PRNG). The properties of PRNG-generated number sequences are analogous to those of random numbers. This technique is assessed by a limited set of beginning values. Using seed state pseudorandom number generator begins from a random beginning state. In a brief period of time, numerous numbers are created which may be generated later if the beginning point in the specified set is known. Thus, the numbers created are efficient and predictable. True random number generators transform entropy sources directly into sequences, but a pseudorandom number generator must find entropy to retain its unpredictability. We may obtain the entropy necessary for PRNGs by leveraging the time of day, the location or position of the mouse, or the activity on the keyboard. We may accomplish this source explanation by utilizing entropy as a substitute for human interaction. Because there's a potential that an attacker may purposely tamper with the system to make it biased. As a consequence, we tested our approach in a controlled setting.

Authentication Type	Effect
Text based	<ul style="list-style-type: none"> • Novice Authentication • Used over decades • Easier exposure to Brute force attacks
Biometric	<ul style="list-style-type: none"> • Unique features to every individual • More expensive • Less subjected to spoofing • Manipulation is difficult
RNG	<ul style="list-style-type: none"> • Entropy sources to sequences • Unpredictable • Potential bias by attacker
Proposed system (Combination of all three)	<ul style="list-style-type: none"> • More efficient as it utilizes the potential possibilities of all three types • Significant improvement in the security level

2. LITERATURE SURVEY

The review of various works on authentication is presented here. Commonly used strategies for authentication are based on textual, Graphical, Token-based and Biometric features or their combination at various levels. Combination of Textual and Graphical based Authentication Scheme using Virtual Environment is suggested by Deepika Gupta et.al[3]. They have enunciated about how graphical password protects in virtual environment of tiled

board. In their system, the size of password typed by the user and the number of movements made by the user are according to user in order to make the password safer. Megala and Natarajan [4] suggested a Secured Crypto-Biometric System Based on Session Key Navigation. They have merged biometric and cryptography in order to have greater advantage to the security of the system. The transaction key is created from the Finger Knuckle-Print and the system leverages Multi Instance Biometric characteristics to offer reliable transaction while delivering data across networks. Woong go et al., [5] presented a secure two-factor user authentication method based on fingerprint data and a password. The recommended technique safeguards against fingerprint reuse. It does not need an extra device, which enhances efficiency and accessibility. With a password, our method employs a partial fingerprint template from the original. This scheme's structure eliminates replay attacks, man-in-the-middle assaults, and so on. The recommended approach is projected to boost the security of the fingerprint as well as the existing fingerprint authentication system.

Tanvi Naik & Sheetal Koul[6] are suggested Multi-Dimensional and Multi-Level Authentication Techniques. They spoke about three dimensional and four dimensional pass words as Multi-Dimensional passwords and also how multilayer passwords may be utilized for Lateral and Hierarchical Applications. Their experimental findings demonstrated that the combination of multi-dimensional and multilevel delivers superior security. Wazid et al.,[7] created a unique efficient Three-factor User Authentication Scheme (TUAS RESG) for a Renewable Energy-based Smart Grid environment, which leverages lightweight cryptographic computations such as one-way hash functions, bitwise XOR operations, and elliptic curve cryptography (ECC). The security of TUAS-RESG has been rigorously evaluated, and it reveals that TUAS-RESG is capable of guarding against a number of known threats. Furthermore, TUAS-RESG includes extra functionality features such as password and biometric update phases, as well as smart meter addition phases. Syed Islam et al., [8] established an algorithm that increases the security of electronic transactions and makes them more trustworthy to the user. According to the author, conventional procedures are quickly evaded and unreliable. The author suggests a three-layer security architecture consisting of username, password, biometric security, and mobile security using SMS to increase the security of electronic transactions.

3. PROPOSED MULTILEVEL AUTHENTICATION

Multi-dimensional authentication integrates numerous authentication techniques into a single virtual environment. To authenticate oneself to the system, the user will go through a series of authentications. Authentication mechanisms such as textual and graphical passwords, tokens, and biometrics may be utilized in the virtual environment depending on the devices available. A textual password, fingerprint authentication, and random number generation are employed in the finest example of multi-dimensional authentication here.

The benefits of this system is user-friendly and has a simple UI, provides excellent protection against bot attacks or hackers, Users may set or upload their own photos and protects the system susceptible to assault. The Block diagram of the proposed Multilevel authentication system is shown in the figure 1.

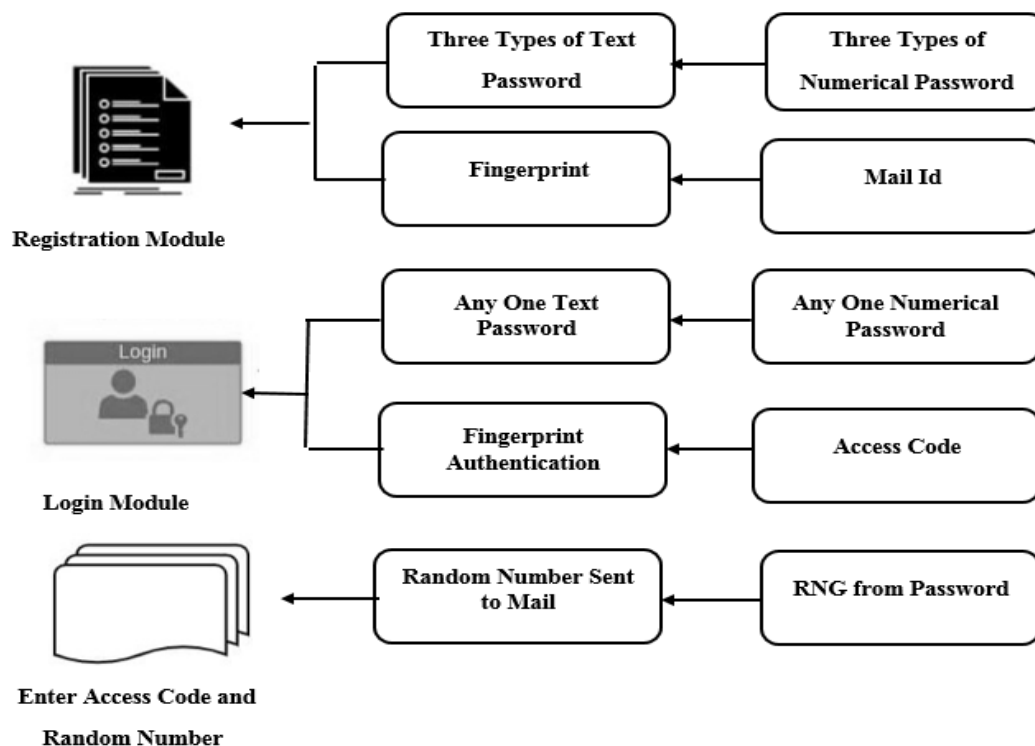


Fig.1. Block diagram of the proposed multilevel authentication system

3.1 REGISTRATION MODULE

Here the user needs to make registration using username, password, and operation type then they have to input level1, level2, and level3 passwords. For all the three levels of password, users may have a maximum of three characters for each level. Characters presented in one level should not be repeated for any other levels. In the meantime, the calculation is done using the operation type for value1, value2, value3 and random number generation is done on the server-side and presented in the user registration form. The various process involved in this module are:

- **Three Types of Text Passwords:** Each level of text password in the registration module requires a minimum of 4 characters to be completed manually by the user or admin.
- **Three Types of Numerical Passwords:** During the registration step, the user or admin must manually type a minimum of four numbers of any combinations in each level of the numerical password.
- **Fingerprint Registration:** The user's or admin fingerprint is scanned and added to the authentication process at this stage. It contributes to a higher level of security and reduces the chance of bot attacks.
- **E-Mail Registration:** In the registration form, the user or admin is requested to provide the email id to which the random number is to be sent during the login.

3.2 LOGIN MODULE

Users can make a login using username and password, once given success then level1, level2, and level3 will be displayed. Once level1 is chosen then pass and value1 with a random number should be entered. If it matches with the server value, then the level 1 password will be active. Then for the next login remaining level2 and level3 same process is continued and if all the three levels are completed then all the three levels will be activated. The various processes involved in this module are:

- **Level Selection:** User or admin is allowed to select any one level of password levels and only one level can be done at a time. An already chosen level cannot be allowed. Both text and numerical value password which is used in registration are to be entered in the selected level as same as in the registration phase.
- **Fingerprint Authentication:** The added fingerprint during the registration module is used here. The registered fingerprint is verified here. Only the registered user or admin can be authenticated to log in.
- **Access Code Generation:** The admin or user has to enter the access code which is generated during the registration phase, or they can copy the access number stored along with the registered database which can be seen by the person who knows the password to access the database.
- **Random Number Sent to Email:** After login, a pop-up window is shown in which the random number received in the registered email is to be entered. The user or admin can log in successfully to access the database after entering the correct random number.

3.3 SERVER SPECIFICATION

The following requirements apply to the server system environment:

- Microsoft Windows XP operating system supported by MS access
- A minimum of 512 MB RAM.
- A backup system with larger capacity (recommended).

3.4 CLIENT SPECIFICATION

The following requirements apply to the client system environment:

- Microsoft Windows XP
- 256 MB RAM

3.5 APACHE TOMCAT

- Apache Tomcat is a server container developed by Apache software foundation.
- Apache tomcat 6.0 implements servlet 2.5 and JSP 2.1 specification [9,10] for unified expression language.
- Apache tomcat includes tools for configuration and management.

4. DATABASE DESIGN

The details of registered users are shown in figure 2. It shows the account name with three level passwords and access character which is only seen by the admin.

account	types	l1pwd	l2pwd	l3pwd	l1rgd	l2rgd	l3rgd	l1cal	l2cal
1000	Addition	Test1	Test2	Test3	660	810	434	12	9
1001	Addition	as123	ad123	af123	368	767	250	17	20
1003	Addition	1234	5678	9123	92	897	840	11	24
1004	Addition	ASDF	GHJK	ZXCV	365	5	388	14	5
1	Addition	QWER	ASDF	ZXCV	944	499	171	17	22
2	Addition	ASVP	ZXCV	QWER	849	868	270	21	22
4	Addition	qwer	asdf	zxcv	937	546	990	19	15
5	Addition	zxcv	asdf	qwer	283	647	815	13	17
6	Addition	QWER	ASDF	ZXCV	452	717	112	11	15
7	Addition	akil	abar	arun	102	110	29	3	2
8	Addition	arun	abar	akil	702	797	673	9	23

Field Name	Mandatory Field	Characteristics	Status
Username	Yes	<ol style="list-style-type: none"> Should not blank Should not accept more than 15 characters. Should not be zero 	<ol style="list-style-type: none"> Success Success Success
Password	Yes	<ol style="list-style-type: none"> Should not blank Should not accept more than 15 characters. Should not be zero 	<ol style="list-style-type: none"> Success Success Success

Fig.2 Registered user details

4.1 Log in phase test case

Table 1 Log in phase test case

4.2 Registration phase test case

Table 2 Registration phase test case

Field Name	Mandatory Field	Characteristics	Status
		1. Should not blank	1. Success

Username	Yes	2. Should not accept more than 15 characters 3. Should not be zero	2. Success 3. Success
Password	Yes	1. Should not blank. 2. Should not accept more than 15 Characters. 3. Should not be zero.	1. Success. 2. Success. 3. Success.
Conformed Password	Yes	1. Should not blank. 2. Should not accept more than 15 Characters. 3. Should not be zero.	1. Success. 2. Success. 3. Success.
Email Id	Yes	1. Should not blank. 2. Should not accept more than 20 Characters. 3. Should not be zero.	1. Success. 2. Success. 3. Success.

5. EXPERIMENTAL RESULTS

REGISTRATION FORM

Fig.3 Registration form

The login form box pops up after using the NetBeans tools, as shown in figure 3. The registration form must be used by a new user to create an account. The login form must be completed by an existing user or admin.

TEXTUAL PASSWORD



The screenshot shows a registration form titled "REGISTER FORM". It contains the following fields:

- Account No:** 11
- Type:** Addition (dropdown menu)
- Level 1:** Password field (****), Access Number: 31, Example Password: 1234
- Level 2:** Password field (****), Access Number: 713, Example Password: 4567
- Level 3:** Password field (****), Access Number: 397, Example Password: 7890

Fig.4 Textual password levels

In the registration form, the password has to be filled for each level and a fingerprint has to be added for authentication. Level 1, level 2, and level 3 are filled with text and numerical passwords. The access number is automatically shown at each level as shown in Figure 4.

E-MAIL REGISTRATION



The screenshot shows an email registration form with the following fields:

- Account No:** 11
- Type:** Addition (dropdown menu)
- Level 1:** Password field (****), Access Number: 31, Example Password: 1234
- Level 2:** Password field (****), Access Number: 713, Example Password: 4567
- Level 3:** Password field (****), Access Number: 397, Example Password: 7890
- Email:** projectab16@gmail.com

Fig.5 E-mail registration.

FINGERPRINT REGISTRATION

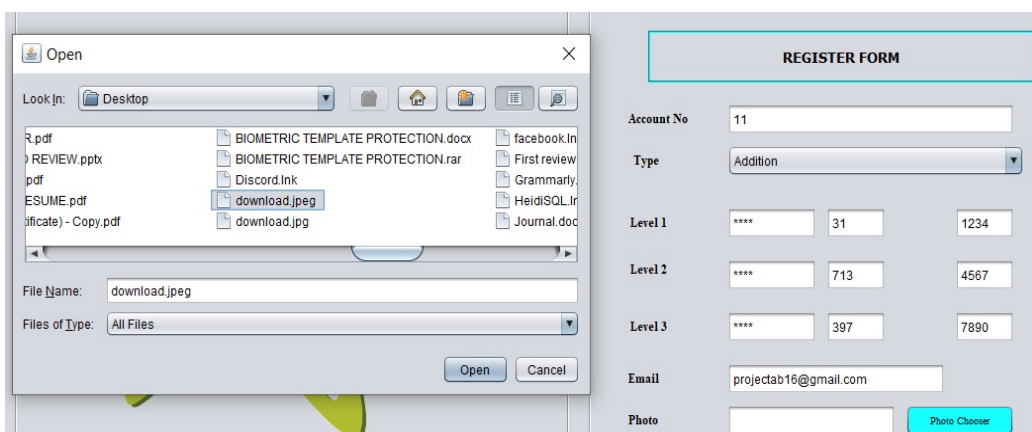


Fig.6 Adding Biometric trait (fingerprint)

After the successful completion of the registration, the user is seen with this login window shown in figure 7. The user has to fill in the details along with fingerprint and email id which is used for registration.

LOGIN FORM

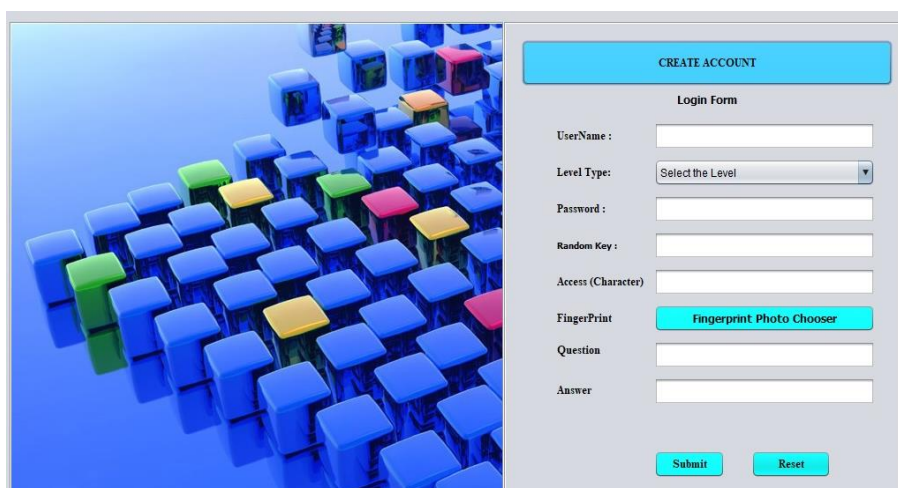
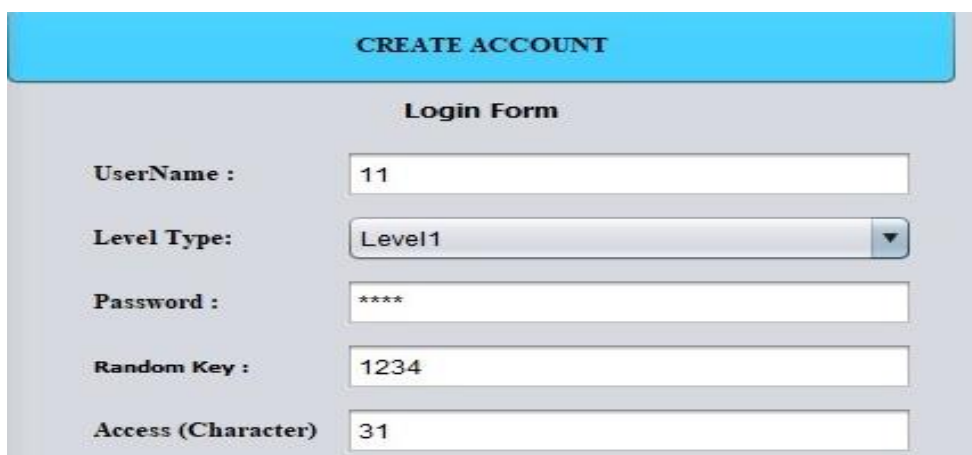


Fig.7 Login Form

After the completion of the registration, the user or admin is directed to the login page. The user or admin must complete the login form as illustrated in Fig. for accessing the database.

LEVEL SELECTION FOR TEXTUAL PASSWORD

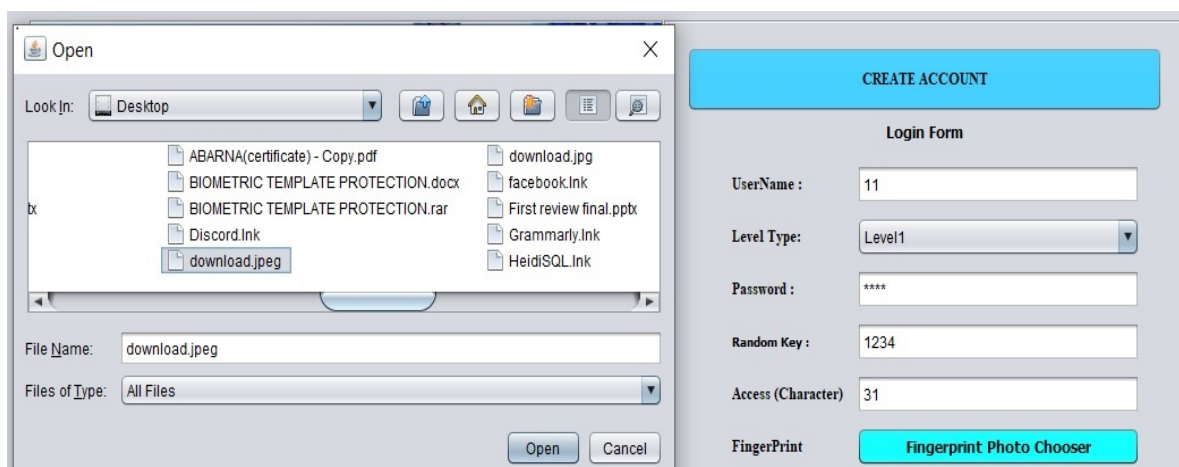


The screenshot shows a web interface for account creation. At the top is a blue button labeled 'CREATE ACCOUNT'. Below it is a 'Login Form' with the following fields: 'UserName' with the value '11', 'Level Type' with a dropdown menu set to 'Level1', 'Password' with masked characters '****', 'Random Key' with the value '1234', and 'Access (Character)' with the value '31'.

Fig.8 Selection of level during login

The user or admin has to enter the registered username and select any one level for entering the textual and numerical password along with the access key as same as the registered one as shown in figure 8.

FINGERPRINT VERIFICATION



The screenshot shows the same 'CREATE ACCOUNT' login form as in Fig. 8, but with a file explorer window open on top of it. The file explorer is titled 'Open' and shows the 'Desktop' location. It contains a list of files including 'ABARNA(certificate) - Copy.pdf', 'download.jpeg', 'facebook.lnk', 'First review final.pptx', 'Grammarly.lnk', 'HeidiSQL.lnk', 'BIOMETRIC TEMPLATE PROTECTION.docx', 'BIOMETRIC TEMPLATE PROTECTION.rar', and 'Discord.lnk'. The 'download.jpeg' file is selected. The file name field shows 'download.jpeg' and the file type is set to 'All Files'. The 'Open' button is highlighted. In the background, the login form is visible, and a new blue button labeled 'Fingerprint Photo Chooser' has been added below the 'Access (Character)' field.

Fig.9 Fingerprint verification during login

After entering the textual and numerical password along with the access number, fingerprint verification has to be done as shown in figure.9 for accessing the database. Then the random number is sent to the registered e-mail after the verification of fingerprint. Once the random is received in the mail, login has to be done using the random number in order to access the database.

RECEPTION OF RANDOM NUMBER

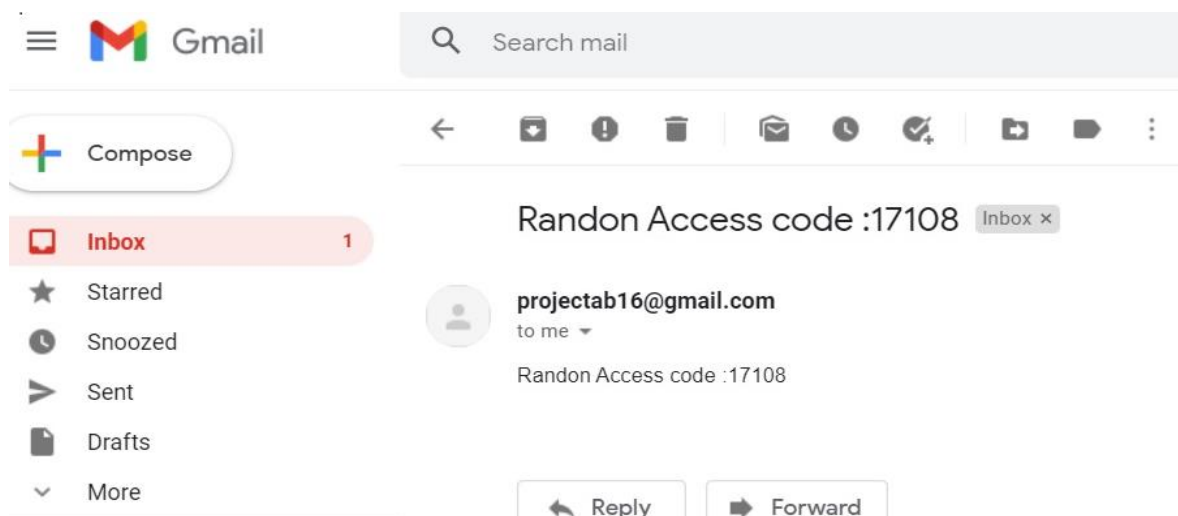


Fig.10 Reception of a random number

The screen shot of the mail box after receiving the random number and the login form using the same is shown in figures 10 and figure 11 respectively. Also the screen shots of the login completion and the database accessing are shown in figures 12 and 13.

LOGIN USING A RANDOM NUMBER

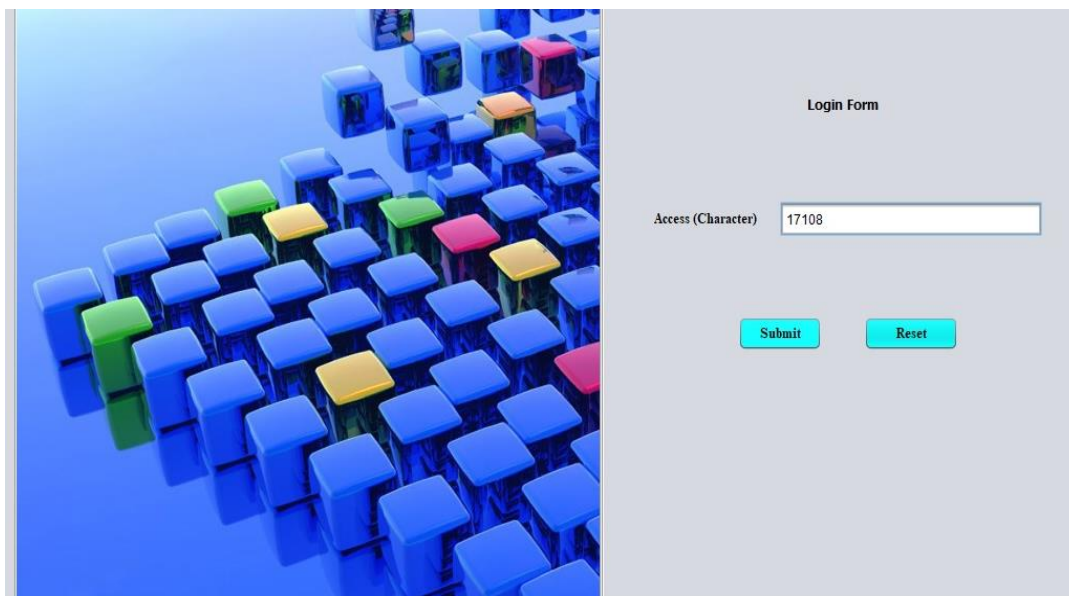


Fig.11 Login using random number

DATABASE ACCESS



Fig.12 Login completion



Fig.13 Database login

6. CONCLUSION

The recommended technique in this paper is to secure the database; the three level security makes it extremely steady at the side of being more consumer-pleasant owing to employing any one of the levels on the login form. This strategy will aid to guard against the robot attack, tempest assault, and brute-pressure assault on the client-side. Since the user or admin must complete the three levels of protection and needs to input the random number sent to his/her e-mail, it has particular protection. This technique could be used in locations wherever extremely high security is needed. The protection of the biometric databases of a company, in which case this approach would be most valuable to conserve and keep their critical and private information innocuous. This work can be extended not only by adding new capabilities in the near future and also are able to personalize our devices.

REFERENCES

- [1] Sadiq Almuairfi, PrakashVeeraraghavan, Naveen Chilamkurti, "A novel image-based implicit password authentication system (IPAS) for mobile and non-mobile devices", *Mathematical and Computer Modelling*, vol.58, no.1-2, pp.108-116, 2013.
- [2] Vidya Mhaske Dhamdhare, G. A. Patil," Three Dimensional Object Used for Data Security", *IEEE International Conference on Computational Intelligence and Communication networks*, 2010.
- [3] Deepika Gupta, Akhand Pratap Singh, Vishal Goar & Shikha Mathur, "Combination of Textual And Graphical Based Authentication Scheme Through Virtual Environment" 3rd *International Conference on Advances in Computing, Communication & Automation (ICACCA)*, 2017
- [4] T. Mekala and M.Natarajan, "Secured Crypto-Biometric System Based on Session Key Navigation", *IEEE International Conference on Computer Communication and Systems (ICCCS '14)*, Feb 20-21, 2014, Chennai, India.

- [5] Woong Go, Kwangwoo Lee, Jin Kwak “Construction of a secure two-factor user authentication system using fingerprint information and password”, *Journal of Intelligent Manufacturing*, vol.25, 2014.
- [6] Tanvi Naik and Sheetal Koul, “Multi-Dimensional and Multi-Level Authentication Techniques”, *International Journal of Computer Applications*, vol. 75, no.12, 2013
- [7] Wazid, M., Das, A.K., Kumar, N., & Rodrigues, J, “Secure Three-Factor User Authentication Scheme for Renewable-Energy-Based Smart Grid Environment”, *IEEE Transactions on Industrial Informatics*, vol.13, pp: 3144-3153, 2017.
- [8] Syeful Islam “An Algorithm for Electronic Money Transaction Security (Three Layer Security): A New Approach”, *International Journal of Information and Computer Security*, vol.9, no. 2, pp. 203-214, 2015.
- [9] Herbert Schildt, “Java 2 Complete Reference” Tata McGraw Hill Ltd, Fourth Edition, 2000.
- [10] Phil Hanna, “JSP 2.0 -The Complete Reference” Tata McGraw Hill Ltd, Second Edition, 2002.