International Journal of Global Engineering (IJGE) E- ISSN: 2456-3099

VOL 4 ISSUE 4 (2019) PAGES 1 - 10

Received: 05/05/2020. Published: 01/06/2020

A Revolutionary 5-factor Authentication Service using IoT Platform

Rahul Krishna B [1], Rahul S. Galgali [2], Dr. M. Kempanna [3]
Computer Science and Engineering, Bangalore Institute of Technology, Bengaluru. India
,rahulsai14231@gmail.com, galgalirahul99@gmail.com , kempsindia@gmail.com

Abstract—Static passwords are vulnerable to security breach. Hence biometric authentication techniques combined or in succession order form layered security resulting in a very secure transaction.This system is like a third party application to the target application thereby making it an enterprise level application which is cloud deployable.

Keywords—IoT, secure banking, biometric passwords, authorization protocols, secure e-commerce, authentication

I. INTRODUCTION

The Internet of Things is the scope of internet to extent to interconnect different objects. It is a vast network of inter-connected things and people, all of which collect and share data about their data usage and the environment around them. The main motive and aim of Internet of Things is achieve the goal of 'Connect the Unconnected' means that the things which are not connected to a network, mainly Internet, will be joined such that, enables them to communicate and exchange the information with other people and things in the network. Internet of Things is technology within which the devices are allowed to sense the physical environment and control them in an automated way which makes them smarter and intelligent by centralized communication on the Internet.

Internet of Things plays a crucial and vital role in the finance and banking industry. Research made by CNBC shows that there will be tremendous growth in the use of IoT systems in the banking and finance industries. Also the market growth is going to skyrocket to over $30billion in the upcoming years. As banks gather user data for authentication and validation purposes it is necessary that the data is not compromised. Hence world class IoT systems are made use to help with the data security for such industries. With the introduction of mobile banking, most of the banking operations and transactions can be done at home. All this is implemented by using biometric authentication or combinations of biometric data gathered from the users. This layered security approach is what makes mobile banking safe. With the help of IoT devices there are virtual assistants and bots designed specifically to cater to the queries. [1]

Security is the topmost priority in all financial sectors. Systems with IoT technologies help to improve security by detecting and identifying any flaw even before they occur or get any clue for the it to occur. By implementing IoT based technologies in their systems, financial institutions are now able to track the location of any financial crime, identify the type of device used for that crime. Cyber-crimes can be detected and prevented now if users are given wearable devices to help in authenticating the user data. Mostly using biometrics user authentication is always efficient, unique and there is no need to remember any passwords.

Received: 05/05/2020. Published: 01/06/2020

Gone are the days when you use cards for carrying out transactions. You are your own password i.e no need to remember lengthy cryptic passwords. Fingerprint, face scan, palm scan, vein scan are enough to have a perfectly cryptic data. That's what IoT does. IoT adds huge benefits to the financial industry, banking industry, in terms of lesser response time and greater response to transactions.

II. EXISTING SYSTEM

A. Conventional Authorization Techniques

Currently, secure authorization techniques involve combinations of password and OTP. But these passwords can compromized quite easily by various algorithms.

B. Benefits

The current system has quite a few benefits. It is known to people and hence finds it's way easily into most of the authentication systems. It is attractive to the mediating parties because of it remains inexpensive to develop. There is no need of expertise in cryptography to implement such a system. Yet we see that drawbacks outnumber the benefits.

C. Drawbacks

Risk of data and personal information of the customers being compromised is the main issue, as there are many algorithms built ready for hacking. In the banking and financial industries there cannot be a data loss or a possible data breach as they deal with real time monetary transactions between multinational companies, world government and normal people. But the existing system is proven to be vulnerable to passwords break down quite easily in a matter of minutes.

IoT systems require standardized hardware. The failure of IoT systems is due to the lack of a common benchmark standard as they are all produced by many companies around the globe.

III. RELATED WORK

The implementation of biometric techniques is the star feature of this paper. The amazing feature of OTPs is the best way of getting over lengthy cryptic passwords which no longer need to be remembered. The existing platform, during registration, the user's unique feature called fingerprint and face samples are collected and stored in the database. The procedure of authentication starts through acquisition and comparing fingerprints and facial features by running specific algorithms implemented by python libraries. The system will itself distinguish between original and fraud samples. Only the legitimate samples are authorized to carry out transaction from the target application.[2].

Biometric system is embedded with specific characteristics of an individual which always is individual, unique, efficient, accurate. Distinctive techniques of biometric systems include facial scans, palm scans, retinal and iris patterns. Biometric declaration is a prizewinner of techniques among the most commonly available basic frameworks for the cryptography, on account of its incontrovertible nature of uniqueness.[4].

In the proposed system consisting of three factor authentication which aims at providing security to the data. At first phase the facial feature of a user is extracted, then based on this extracted template a

Received: 05/05/2020. Published: 01/06/2020

biometric key is generated. This key is in turn used to encrypt another key to assess the legitimacy of the information[4].

IV. PROPOSED WORK

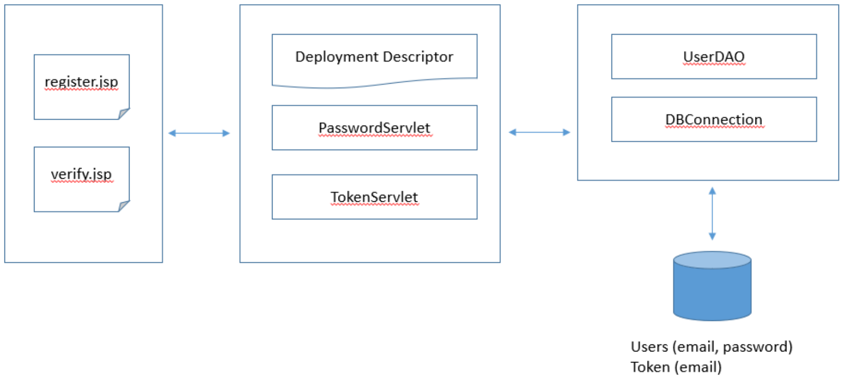
We bring to the light of biometric based authentication for most of the third-party applications such as banking, e-commerce applications such as flipkart, amazon etc. The OTP based system also includes the strong static password, biometric, facial recognition and also security device authentication. Security device authentication is most secure authentication which cannot be stolen or compromised. Most popular security devices are RSA Token, which is quite expensive, cost-effective one can be a pen-drive.

For the purpose of testing our we have developed an ATM application, for which access will be granted once we pass all the levels of authentication. It contains all the basic operations that are usually performed in a bank. It includes setting the PIN initially, the deposit the money, withdraw the money, fast cash, fund transfer, passbook. All the operations except setting the PIN needs to authenticate the PIN which is usually set initially and can be changed at any time.

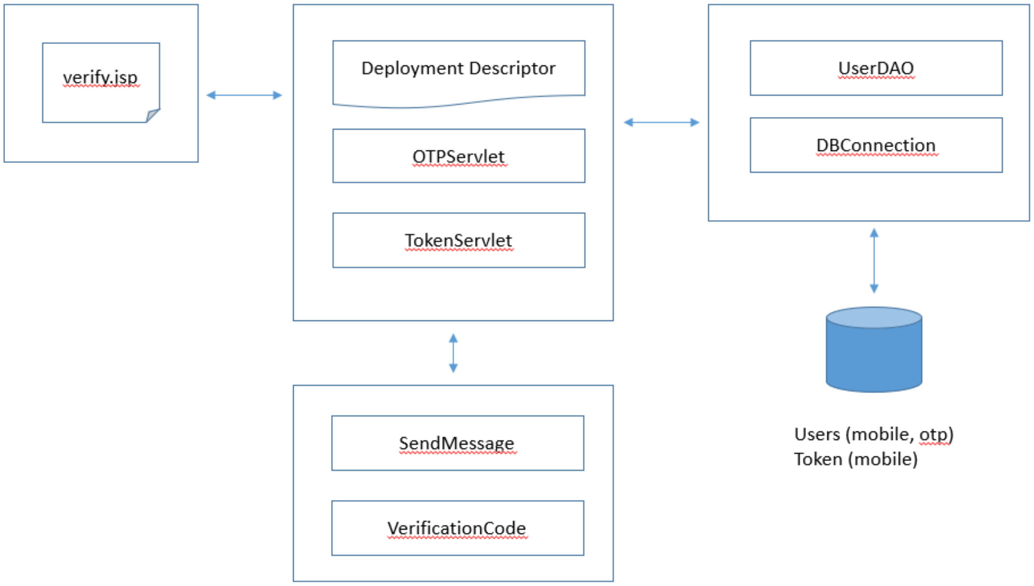
It has around five modules namely:

- Password based Authentication
- Fingerprint based Authentication
- OTP based Authentication
- Facial based Authentication
- Security device-based Authentication

1. Password based Authentication
   - Implements the Password based authentication scheme which will further be re-used by the MFA application as one of the steps in the multiple factors of the authentication scheme.
   - Requires the user to choose a strong password during the registration phase and which has to be provided again during the login phase to get access to the system. The user does not get to choose the email ID in this module. The email ID for the user will be provided by the master MFA application.
   - This module also provides an API to the MFA application to check if the password authentication is successful or not. This API will be used to grant the access to the prototype application at later stages.



2. OTP based Authentication
   - Implements the OTP based authentication scheme which will further be re-used by the MFA application as one of the steps in the multiple factors of the authentication scheme.
   - The OTP based authentication requires the user to enter the One Time Passcode received to his mobile phone during the login phase. This module is only applicable during the login phase. This is because the user does not have to provide any OTP during the registration phase. The mobile number of the user to this module will be provided by the MFA application.
   - This module also provides an API to the MFA application to check if the OTP authentication is successful or not. This API will be used to grant the access to the prototype application at later stages.

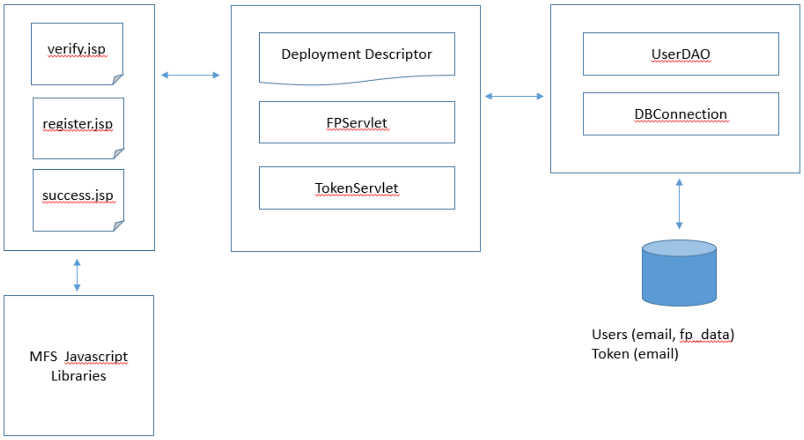


3. Fingerprint based Authentication
   - Implements the Fingerprint based authentication scheme which will further be re-used by the MFA application as one of the steps in the multiple factors of the authentication scheme.
   - Requires the user to register his/her biometric fingerprint data during the registration phase and which has to be proved again during the login phase to get access to the system.
   - To capture the fingerprint of the user in this module, we are using MFS100 device with the suitable hardware drivers.
   - This module also provides an API to the MFA application to check if the password authentication is successful or not. This API will be used to grant the access to the prototype application at later stages.

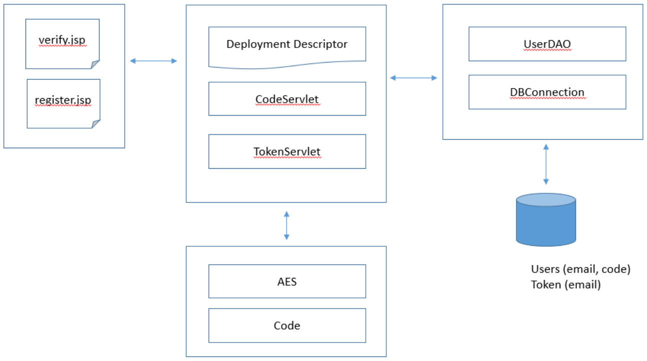
International Journal of Global Engineering (IJGE) E- ISSN: 2456-3099

VOL 4 ISSUE 4 (2019) PAGES 1 - 10

Received: 05/05/2020. Published: 01/06/2020

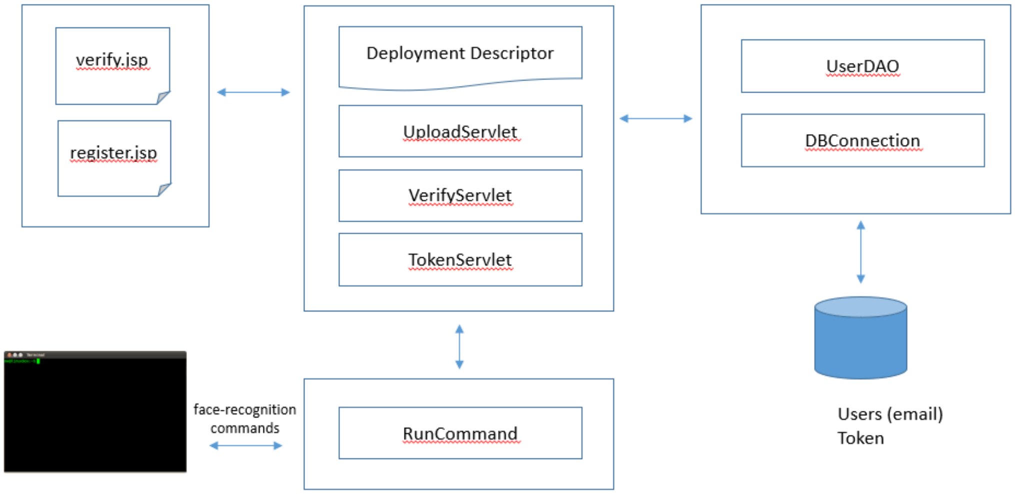


4. Security device-based Authentication
    - Implements the Security Device based authentication scheme.
    - Requires the user to register his/her personal device during the registration phase and which has to be provided again during the login phase to get access to the system.
    - The personal device can be an user's pen-drive, hard-disk, or any other portable disk drives. The user must ensure the device has read-write permission to this module in order to function properly.
    - This module also provides an API to the MFA application to check if the password authentication is successful or not. This API will be used to grant the access to the prototype application at later stages.



5. Facial based Authentication
    - Implements the Face Recognition Device based authentication scheme
    - Requires the user to register his/her facial features during the registration phase and which has to be provided again during the login phase to get access to the system
    - We use Python's face-recognition API to capture and verify the user's facial features during the registration and the login phase respectively. This library is proven to be 99.4% accurate and its comparatively faster than other libraries in the market.

- This module also provides an API to the MFA application to check if the password authentication is successful or not. This API will be used to grant the access to the prototype application at later stages.



A. Architecture

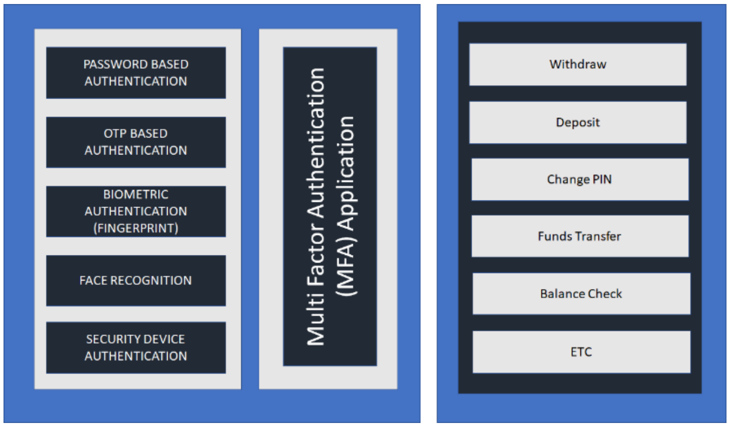
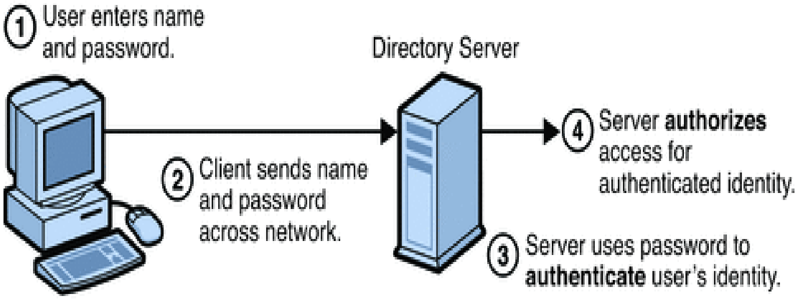

PASSWORD BASED AUTHENTICATION
OTP BASED AUTHENTICATION
BIOMETRIC AUTHENTICATION (FINGERPRINT)
FACE RECOGNITION
SECURITY DEVICE AUTHENTICATION
Multi Factor Authentication (MFA) Application
Withdraw
Deposit
Change PIN
Funds Transfer
Balance Check
ETC

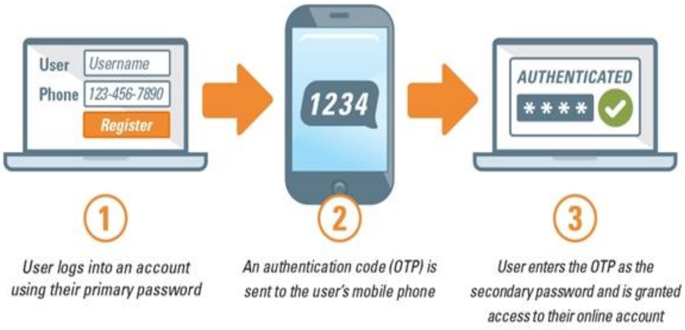
Figure shows the architecture of the proposed system, where the individual module such as Password, OTP, Biometric, Facial, Security based Authentications are considered to be individual and once integrated the pass tokens from one module to another module. All of these modules are controlled by MFA application which acts as gateway application for any of the applications which use this system (In this case ATM application). On the other hand, shows the ATM applications which shows all typical operations performed in an ATM or a bank ranging from Withdraw, Deposit, Change or Configure PIN, Funds Transfer, Balance Check and much more.

Received: 05/05/2020. Published: 01/06/2020

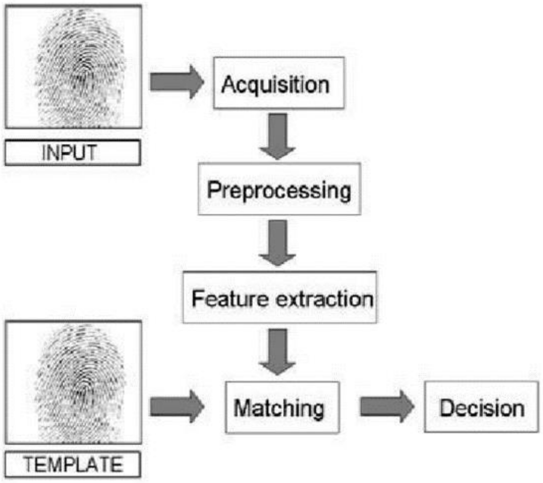
1. Password Based Authentication


1 User enters name and password.
Directory Server
2 Client sends name and password across network.
4 Server authorizes access for authenticated identity.
3 Server uses password to authenticate user's identity.

2. OTP Based Authentication

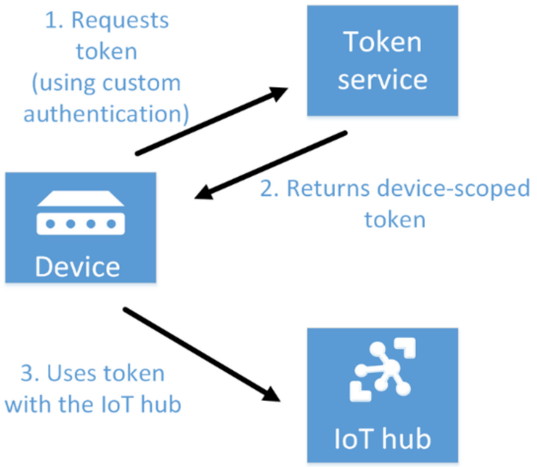

User
Username
Phone
123-456-7890
Register
1234
AUTHENTICATED
****
1
User logs into an account using their primary password
2
An authentication code (OTP) is sent to the user's mobile phone
3
User enters the OTP as the secondary password and is granted access to their online account

3. Fingerprint Based Authentication

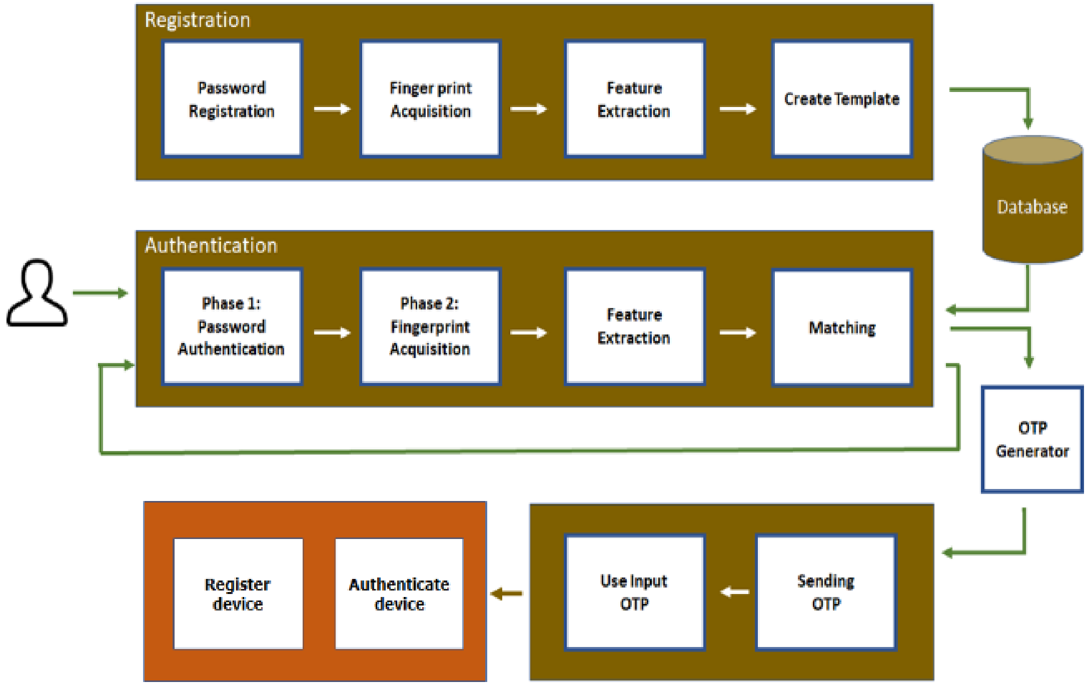


Received: 05/05/2020. Published: 01/06/2020

4. Security-Device Based Authentication


1. Requests token (using custom authentication)
Token service
2. Returns device-scoped token
Device
3. Uses token with the IoT hub
IoT hub

User Interface design is the most important aspect, which depicts the look and feel of system. The UI design must be efficient in all aspects of user experience. It must be responsive, not too flashy, very good performance. The reason for responsive is many users use the website or application from different devices like mobile, tablet and from laptop. The contents should not trimmed when viewed in low resolution devices.



The proposed System has 3 phases:

1. Enrollment (Registration)
2. Authentication
3. Login

During the Enrollment phase the user has to go through the various phases of enrollment. Initially he has to specify the password, register the fingerprint, register the face and finally register a security device such as pen-drive etc.

During the Authentication phase the user should specify the email-id and phone number initially. The one can start the verification steps like OTP, password, Security device and the face recognition.

Once all the phases of Authentication has been successfully passed then the user enters into the third-party application for which the security API has been deployed for.

V. Analysis of Results

During the implementation of the system locally, the system was tested with only limited combinations of the given modules. The system was found to work securely and up to the mark. This work ensured that the security was not compromised at any point of time, thereby while integrating different modules.

VI. Applications

- Fingerprint is unique to an individual.
- Fingerprint is more efficient, accurate and less expensive when compared with other biometrics.
- Fingerprint, Face login need not be memorized.
- Reduces the cost of authentication to business/enterprise applications.
- Layered security with Password, OTP, Fingerprint, Face and Security device.
- Perfect third-party application for banking and e-commerce.
- System where different techniques are combined in succession order to result in secure login and transaction.

VII. Conclusion

An efficient and secured Authentication Application is proposed based on multiple factors. The multiple factors include Password, OTP, Fingerprint, Security Device, and Facial Features. The solution is pluggable to any of the existing third-party applications without much coding efforts.

VIII. Future Work

In future, we intend to expose this solution as-a-service in the cloud model thus making it more effective in integration with the third-party application and also to cover the full ecosystem of the Registration and Verification process. The system was integrated only for limited combinations of modules. It should be tested for different combinations of the modules.

Received: 05/05/2020. Published: 01/06/2020

REFERENCES

[1] Soares, J. and Gaikwad, A.N., 2016, September. Fingerprint and iris biometric controlled smart banking machine embedded with GSM technology for OTP. In Automatic Control and Dynamic Optimization Techniques (ICACDOT), International Conference on (pp. 409-414).IEEE

[2] Popa, D. and Simion, E., 2017, June. Enhancing security by combining biometrics and cryptography. In Electronics, Computers and Artificial Intelligence (ECAI), 2017 9th International Conference on (pp. 1-7).IEEE

[3] Apurva Taralekar,Rutuja Tangade,Gopalsingh Chouhan,Nikhilkumar Shardoor,One Touch Multi-banking Transaction ATM System using Biometric and GSM Authentication,2017 International Conference on Big Data, IoT and Data Science (BID) Vishwakarma Institute of Technology, Pune, Dec 20-22, 2017

[4] S.Aanjanadevi,V.Palanisamy,S.Aanjankumar,An improved method for generating biometric-cryptographic system from face feature Proceedings of the Third International Conference on Trends in Electronics and Informatics (ICOEI 2019) IEEE Xplore Part Number: CFP19J32-ART; ISBN:78-1-5386-9439-8J.

[5] Enhanced E-commerce application security using Three-factor Authentication Binitha Ann Scaria Amrita Center for Cyber Security Systems and Networks Amrita Vishwa Vidhyapeetham, Amritapuri Campus Clappana P.O, 690525, Kollam, Kerala bini.annscaria879@gmail.com

[6] Secure Authentication for Data Protection in Cloud Computing using Color Schemes Manish M. Potey , Dr. C. A. Dhote, Deepak H. Sharma 2017 International Conference on Computational Systems and Information Systems for Sustainable Solutions.

[7] An improved method for generating Biometric-cryptographic system from face feature S.Aanjanadevi Ph.D Research scholar , V.Palanisamy, S.Aanjankumar Proceedings of the Third International Conference on Trends in Electronics and Informatics (ICOEI 2019) IEEE