

Biometric Security Using Cryptography for Insurance Data Retrieval with Additional OTP Generation and Verification

Prasad Pawar¹, Shreyas Datar², Nilay Ranade³, Kunal Thorat⁴, Prof.A.N.Gharu⁵

^{1,2,3,4} *Department of Computer Engineering, PVG's College of Engineering, Nashik*

⁵ *Asst. Professor, Department of Computer Engineering, PVG's College of Engineering, Nashik*

Abstract- The main aim of our system is to take Biometric security to a new level. A combination of biometric Fingerprint scanner, cryptography, OTP generation methods are being used for the application for betterment of the security. Fingerprint scanning followed by OTP generation on mobile and email address as well as OTP validation on the same are going to play a major role on basis of the above three mentioned the insurance data (Policy information) is going to be retrieved by the user. The fingerprint of every user is going to be stored in a database from where it is going to be compared for authentication. For retrieval of data and cryptography AES algorithms are used respectively. We are using all these security features to secure INSURANCE COMPANY's data retrieval in Application.

Index Terms- Biometric, Cryptography, OTP generation Authentication, Data retrieval, AES Algorithm.

1. INTRODUCTION

Information security's main goal is not letting any unauthorized user gain access to the information. We will be achieving this by developing new plans, algorithms, procedures and policies. Now-a-days securing information from unauthorized users and people with bad faith is extremely necessary. IoT brings everything connected to the internet, this leads to more vulnerabilities and threats, such as authentication, integrity or authorization attacks. Traditional fixed passwords and keys make systems weaker than those use dynamically changing passwords and keys. In the past few months, Ransomware attackers exploited traditional authentication techniques on computer devices, as some attackers, first, had used some password cracking techniques to guess victim's password and

then injected a trojan horse to encrypt victim's information. Without any doubt, using randomly changing strong passwords and authentication keys would make it much harder. One-time password generators that are fed with fixed data can be predictable as well. This paper introduces a new one-time password generator that is fed with randomly changing inputs. Then the proposed generator is implemented using Android-Based mobile device, after that, output is validated and assessed.

Also we have the biometric system in which its work based on the pattern recognition scheme to obtain a set of features as template of an enrolled person. A biometric template belongs to a real person and it can be never replaced by another one. This template will be stored to compare with the features of new users to be identified later. A biometric system includes the concept of fusion by which we are able to improve the performance and accuracy of an identification system in search of a set of features in the space of features of the enrolled persons [7]. Security of a biometric template may be threaten by attacks. Thus if an individual's template is revealed without any protection, the individual's biometric attributes should be used no longer for the authorization by the biometric system.

Moreover, a fused template stored in the system memory, can reveal more data about enrolled users. This is why that nowadays multi-biometric template protection is a serious challenge for researchers when they want to apply cryptographic methodologies to protect the templates stored in a biometric system. In the current study, we propose a new concept in biometric authentication called "digest". It saves a print of client biometric traits, which is output of a one-way function. Through applying the digest, we

do not need to encrypt and decrypt biometric information, as well as we can utilize many efficient properties including homomorphic and Hamming distance. Computing digest is fast and nobody can discover any primary biometric information using a digest.

2. LITERATURE REVIEW

- [1] Hisham S. Elganzoury, Ahmed A. Abdelhafez
The main goal of information security is to keep information out of unauthorized reach and modification. This can be achieved by developing policies, procedures, plans, and algorithms for achieving Confidentiality, Integrity and Authentication (CIA). Authentication assurance has become the most necessary target of information security as it is the first defense line in security systems, especially when Internet of Things (IoT) comes to the surface.
- [2] Dr. K. Mohan Kumar, G. BalaMurugan
Web applications play a major part in our day to day life. Every human being use computers for their transactions using web applications. Even personal information are stored in government websites. Banks are using web applications for the transactions. Due to lack of security lot of frauds are occurred every day. So, security issue is an important issue in our digital life. One time pass word is the solution for this issue. Many algorithms are used to generate OTP. Every algorithm has its own pros and cons. This study analyze seven algorithms and suggest the best OTP generation algorithm using various aspects.
- [3] Xindong Wu, Fellow.
Big Data concern large-volume, complex, growing data sets with multiple, autonomous sources. With the fast development of networking, data storage, and the data collection capacity, Big Data are now rapidly expanding in all science and engineering domains, including physical, biological and biomedical sciences. This paper presents a HACE theorem that characterizes the features of the Big Data revolution, and proposes a Big Data processing model, from the data mining perspective.
- [4] Mrvet Krc , Faezeh Sadat Babmir.
All biometric cryptographic algorithms need a secret key or a random number as an ID or biometric information to identify an individual that aims to enter the system. The biometric information is unique and trustable for making an authentication system.

Most of current schemes utilize encryption/decryption methods including RSA to make secure data from primary biometric information. Generally, encrypting and decrypting algorithms have slow and time-consuming operations. The digest value together with the systems parameters are used by the matching module for the authentication. Through the digest, nobody can capture any information of primary biometric traits. The properties mentioned above lead to increases of the accuracy, accessibility and easiness level of a biometric system.

3. PROBLEM DEFINITION

To design and implement an application using biometry and cryptography which will be used to retrieve insurance data by OTP generation using AES algorithm for cryptography.

4. PROPOSED SYSTEM

Firstly our system will be providing 2 login options: 1. Admin 2. Customer. After logging in as admin user, options like registration of user and managing information of the customer or client is given. In this system only an admin user is allowed to create or register a new client or customer. At the time of registration, the admin is mandatorily forced to take fingerprint of the customer scanned in front of him/her after authorizing the customer using his valid identification documents and also to retrieve and manage the already registered customers information he needs to get the biometric and OTP verification done. On the other hand, the normal customer login which will have comparatively low authorization, there will be options like managing his own information, paying premium for his own policies and checking his own transaction history. To retrieve the data required for all these options the customer will have to go through all the verification process which includes biometric fingerprint verification and OTP verification. This gives data of the company very high standard security. The OTP verification will be done in two phases as we will be generating OTPs that is on the registered email address and other the registered mobile number. This will provide 2 way authentications to the customer access. After all

this process is done then both login types will have logout option on each screen they go on-to.

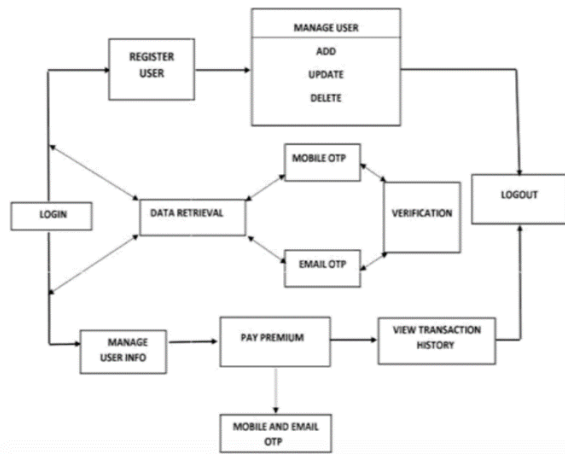


Figure 1. System Architecture

5. ALGORITHMS

1) ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM

AES comprises three block ciphers: AES-128, AES-192 and AES- 256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256-bits, respectively. The Rijndael cipher was designed to accept additional block sizes and key lengths, but for AES, those functions were not adopted. Symmetric (also known as secret-key) ciphers use the same key for encryption and decryption, so the sender and the receiver must both know – and use - the same secret key. All key lengths are deemed sufficient to protect classified information up to the 'Secret' level with "Top Secret" information requiring either 192 or 256 bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys a round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of cipher text. The AES encryption algorithm defines a number of transformations that are to be performed on data stored in an array. The first step of the cipher is to put the data into an array; after which the cipher transformations are repeated over a number of encryption rounds. The number of rounds is determined by the key length, with 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. The first transformation in

the AES encryption cipher is substitution of data using a substitution table; the second transformation shifts data rows, the third mixes columns. The last transformation is a simple exclusive or (XOR) operation performed on each column using a different part of the encryption key longer keys need more rounds to complete.

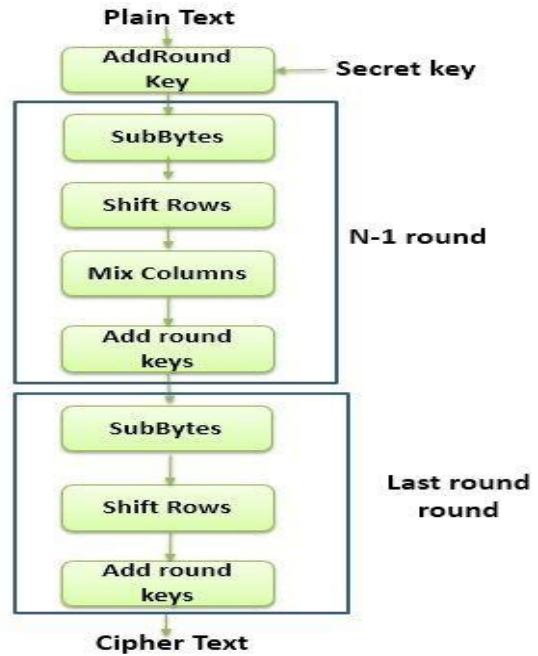


Figure 2. AES Algorithm

Steps for AES algorithm:

1. Initialize the state array with the block data (plaintext).
2. Add the initial round key to the starting state array.
3. Perform nine rounds of state manipulation.
4. Perform the tenth and final round of state manipulation.
5. Copy the final state array out as the encrypted data (ciphertext).

2) TOTP (TIME BASED ONE TIME PASSWORD) ALGORITHM:

TOTP is defined in RFC 6238. It is free and simple. There are many open-source implementations for both the client-side and server-side components. In particular, Google has developed an application that is freely available for Android, iOS and the web: Google Authenticator. This application allows us to integrate TOTP easily into our developments. By using the TOTP method, we are creating a one time

password on the user side (instead of server side) through a smartphone application. This means that users always have access to their one time password. So it prevents the server from sending a text message every time user tries to login. Also, the generated password changes after a certain time interval, so it behaves like an one-time password. The following could be a way of implementing this solution:

1. Backend server creates a secret key for that particular user.
2. Server then shares that secret key with the user's phone application.
3. Phone application initializes a counter.
4. Phone application generates a one-time password using that secret key and counter.
5. Phone application changes the counter after a certain interval and regenerates the one time password making it dynamic.

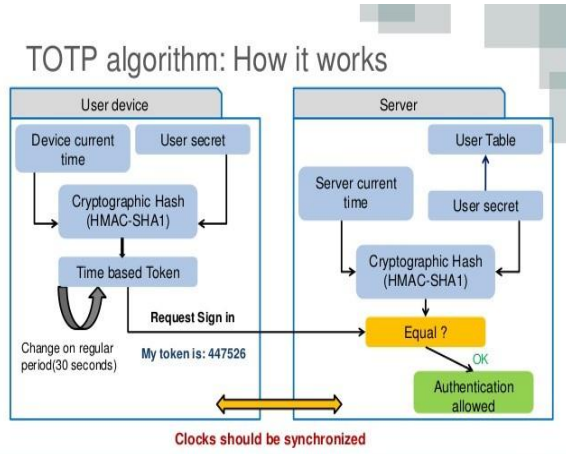
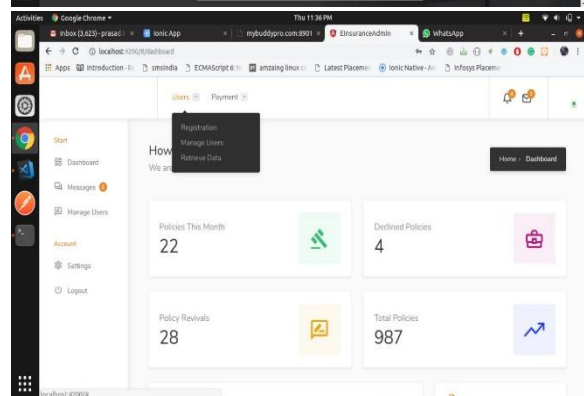
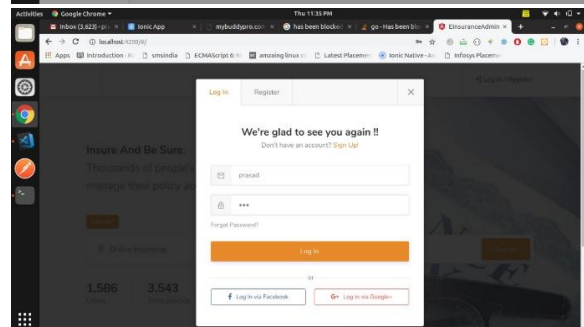
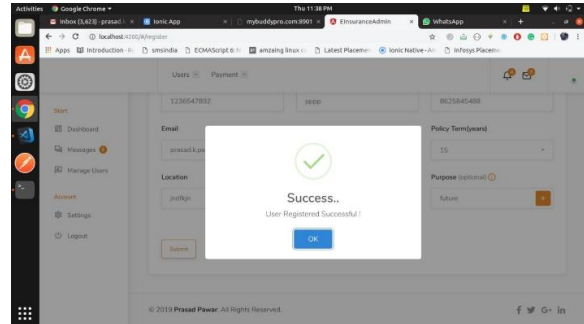
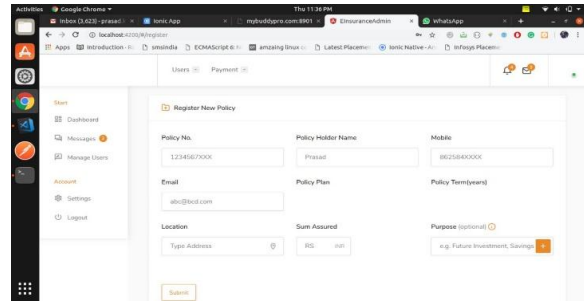
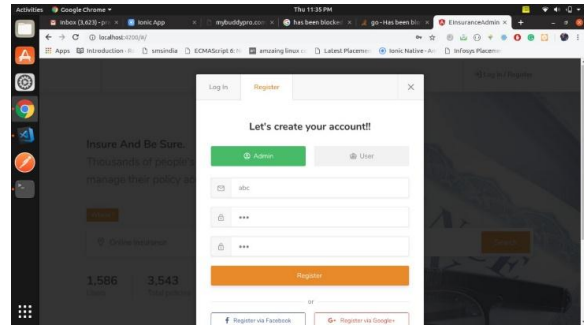
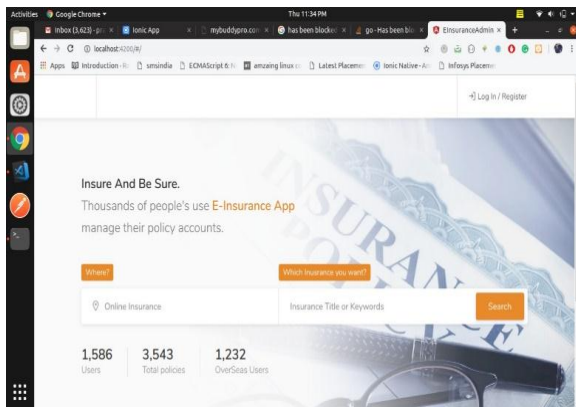
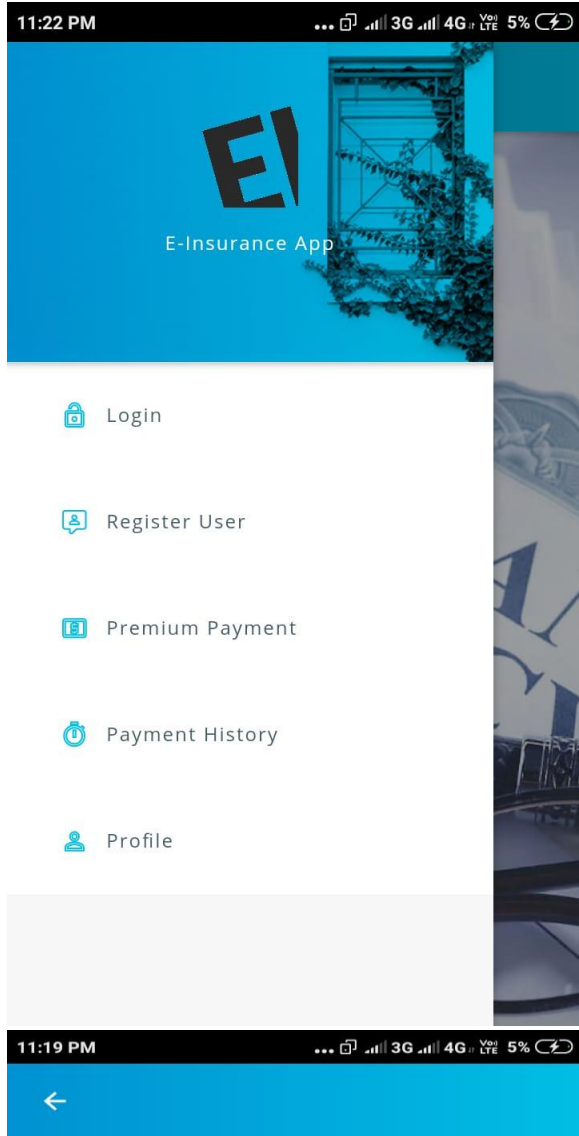



Figure 3. TOTP Algorithm

6. RESULT ANALYSIS





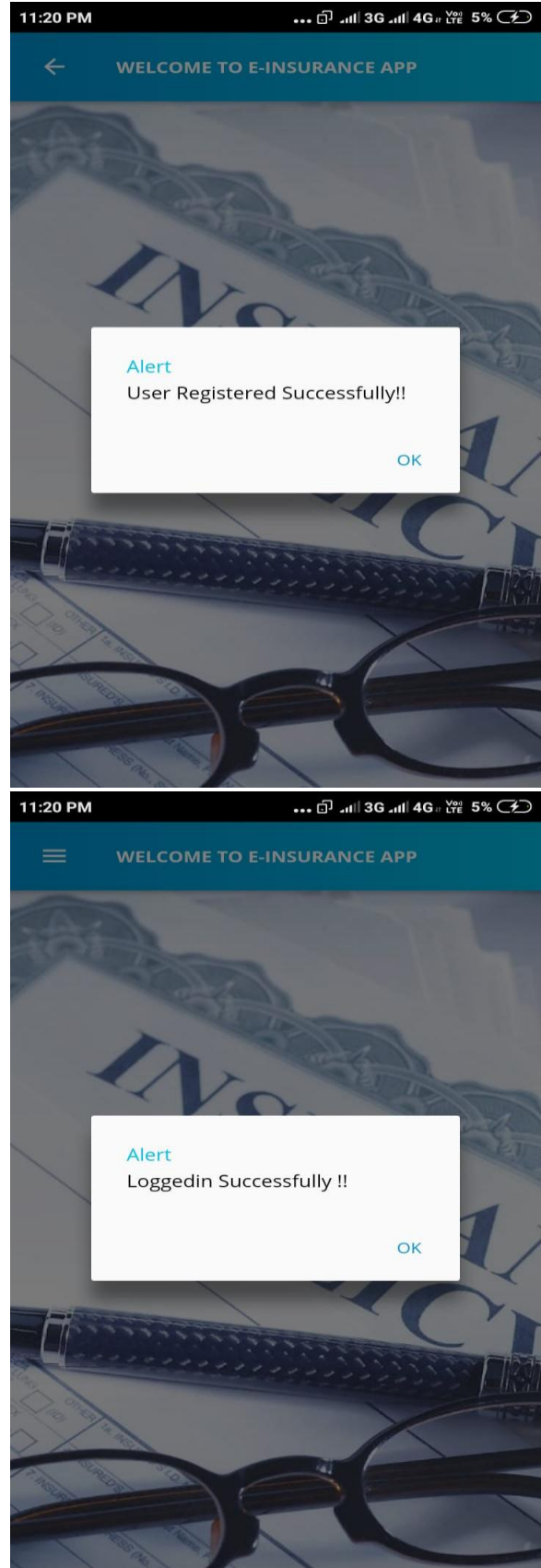
SKIP



Username

Password

LOGIN REGISTER



7. CONCLUSION

As a part of the prototype implementation, we have proposed a complete end-to-end solution that provides a security to sensitive data, with bio-metric for retrieval of the data and a mobile application as the user interface to the entire system. We are going to increase security to the data retrieval using biometrics and also reducing the complexity of data retrieval used in existing systems. Use of these technologies will improve the existing systems data retrieval security. The existing system for insurance company is not this secured, but it requires this security as the person with the credentials of policy can retrieve the data about policies and other data. Our security measures assures that the data can be retrieved only by the account holder or the admin of the system. We also thought of some new improvements in the proposed system. OTPs with combinations of string, numbers and special symbols will increase more security to the users data.

REFERENCES

- [1] Hisham S. Elganzoury, Ahmed A. Abdelhafez, Abdelfattah A. Hegazy A NewSecure One-Time Password Algorithm for Mobile Applications 2018, 35th NATIONAL RADIO SCIENCE CONFERENCE (NRSC 2018), March 20 - 22, 2018.
- [2] Dindayal Mahto and Dilip Kumar Yadav Security Improvement of One- Time Password Using Crypto-Biometric Model Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics, Smart Innovation, Systems and Technologies 44.
- [3] Rachita Dubey*, Jijo S.Nair, A Review on Secured One Time Password Based Authentication and Validation System, International Journal of Computer Sciences and Engineering E-ISSN: 2347-2693.
- [4] Diana Popa, Emil Simion, Enhancing Security by Combining Biometrics and Cryptography, ECAI 2017 International Conference 9th Edition Electronics, Computers and Artificial Intelligence 29 June - 01 July, 2017, Targoviste, ROMANIA.
- [5] Dr. K. Mohan Kumar, G. Balmurugan, COMPARITIVE STUDY ON ONE TIME PASSWORD ALGORITHMS, IJCSMC, Vol. 7, Issue. 8, August 2008, pg.37 52.
- [6] Shubham Srivastava , Sivasankar M, On The Generation of Alphanumeric One Time Passwords,India
- [7] Ranjith Jayapal, Pramod Govindan, Biometric Encryption System for Increased Security, Department of Electrical Engineering University of North Florida (UNF) Jacksonville, Florida, USA.
- [8] Mrvet Krc, Faezeh Sadat Babmir, A Digest-based Method for Efficiency Improvement of Security in Biometrical Cryptography Authentication, 2017 International Symposium on Computer Science and Software Engineering (CSSE).
- [9] Shichao Zhang, Senior Member, IEEE, Xuelong Li, Fellow, IEEE, Ming Zong, Xiaofeng Zhu, and Ruili Wang , Efficient KNN Classification With Different Numbers of Nearest Neighbors , IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS, VOL. 29, NO. 5, MAY 2018.
- [10] Xindong Wu, Fellow, IEEE, Xingquan Zhu, Senior Member, IEEE, Gong-Qing Wu, and Wei Ding, Senior Member, IEEE , Data Mining with Big Data , IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 26, NO. 1, JANUARY 2014.
- [11] Mouad.M.H.Ali , Vivek H. Mahale , Pravin Yannawar , A. T. Gaikwad , Fingerprint Recognition for Person Identification and Verification Based on Minutiae Matching , 2016 IEEE 6th International Conference on Advanced Computing.