World Journal of Engineering Research and Technology
WJERT
www.wjert.org
SJIF Impact Factor: 5.218

A MULTI-FACTOR SECURITY LEVEL IN E- INSURANCE SYSTEM DESIGN USING OTP AND BIOMETRICS AUTHENTICATION SYSTEM

Ele Sylvester I.*, O. A. Ofem and B. I. Ele

Department of Computer Science, University of Calabar, Nigeria.

Article Received on 10/04/2018 **Article Revised on 01/05/2018** **Article Accepted on 21/05/2018**

***Corresponding Author**
Ele Sylvester I.
Department of Computer Science, University of Calabar, Nigeria.

ABSTRACT

The aim of this research work is to Design and Model a Multifactor Security Level in Electronics Insurance System Using OTP (one Time Password) and Biometrics Authentication Systems. The objective is to model a system that would provide the highest level of data security by implementing a strong multi-factor authentication which will be the combination of level one(1) authentication (password) and either level two(2) authentication (verification code which will be appreciated by low tech device users) or any of the under listed level three(3) authentication (biometrics) for high tech users, such as face recognition for camera enabled mobile phone users and finger print for all finger print enabled device users. The prototype of the system, which is a web based system, was developed with the Microsoft ASP.NET C# programming language for the back end, using the Microsoft Visual Studio as the development environment (IDE), we employed the Microsoft SQL for database in WAMP server with some HTML codes used for the front end design of the application. The system was modeled using the Object Oriented Design and Analysis (OOAD). Unified Modeling Language (UML) was used as a graphical language to specify diagrams for documenting the behavior of the system. The prototype result was tested using several test data.

KEYWORDS: Biometrics Authentication, OTP, E-Insurance, Fingerprint Recognition, Insurance.

1. INTRODUCTION

Insurance terms and conditions are essentially complex and most people may need simple and enough explanation to understand them. To make a decision on purchasing an insurance policy online, a potential customer needs to understand the terms and conditions of each insurance policy presented. In most cases, the websites of insurance companies lack the capability to help the client understand the terms and make a decision on what product to buy and these result to discouragement of some potential customers.

Leadway Assurance Company Limited (Leadway) is one of Nigeria's foremost insurance service companies, with a reputation for service efficiency and customer reliability. For over 40 years, Leadway has honored its underwriting commitments and has earned its reputation of excellence in claims handling (Leadway, 2017). Leadway has a viable online presence, both on social media and a dedicated customer-centric website. This website definitely appeals to the average person because the layout is so simple but very effective. It is a clean website with a flawless look, and someone without any technical background would definitely appreciate it. The design is very professional and well done, the text and images are clearly and logically laid out, the appropriate use of their corporate colors and the company name and logo is highly commendable. It is easy to navigate this website because all of the links are right there on the top right hand side, and people without image-loading browsers can access the links via the text at the bottom which is very handy and essential for a good website. Graphics are kept to a minimum which is great because the load time is cut down. The mode of authentication used on the website for existing policy holder is the traditional password-based security approach, which is the normal trend for most e-commerce/e-insurance in Nigeria.

However, relying on a traditional, password-based approach as a security measure do not provide sufficient security against well-organized attackers with strong financial backing. Passwords can be lost, can be forgotten, can be stolen and used by a thief/intruder to access policy holder's data and manipulate their insurance portfolio. With increasing use of IT technology and need to protect data, we have multiple accounts/passwords for different online platforms. We can only remember few passwords, so we end up using things we know to create them (birthdays, wife/friends name, dog, cat, etc.). It is easy to crack passwords, because most of our passwords are weak. If we create strong passwords (that should be

meaningless to us) we will forget them and there is no way to remember multiple such passwords.

Study have revealed that the insurance industry is still relatively small and there are currently just over 650 Insurance Companies and about 46 African Reinsurance Companies operating on the Continent, of which about 38% of them are registered or domiciled in South Africa. Average insurance density of Africa in 2009 was about US$54 compared to the global density of US$596. The Continent's insurance penetration (measured as a percentage of insurance premium to GDP) ratio was about 3.5% compared to other regions such as Asia where the rate was about 6.1%. South Africa has the highest penetration ratio of 13.2% on the Continent while most African Countries are below 1%. Only about 7 countries on the Continent have penetration ratios exceeding 2%. Insurance penetration is abysmally low even in countries like Nigeria, a Country with the largest population of nearly 170 million and the second largest economy on the Continent. In July 2015, insurance penetration in Nigeria stood at 0.6% compared to neighboring African countries like South Africa, Namibia, and Kenya which have 15.4%, 7.7%, and 3.4% respectively. A recent survey on the uptake of insurance in Nigeria revealed that 9 in 10 Nigerians (86%) do not have any form of insurance cover (Ifeanyi, 2015).

As consumers increasingly shift from paper-base to computer, computers to smartphones, and smartphones to tablets, they can research, compare prices and buy anytime, anywhere. The easy access that Apple, Google and Amazon deliver is what consumers now expect from the financial service sector, particularly the insurance industry (Shaun, 2013). The main advantage of this approach (web app) is the fact that clients do not depend on the user' specific operating system; therefore, web applications are cross-platform services. Developers do not need to prepare different versions of the same app for Microsoft Window, Mac OS, Linux, etc. An app is created only once for any platform and it can work on any operating system. However, web app can work incorrectly because of the user's opportunity to change browser's settings in the way he wants. According to Oluwagbemi et al, (2011), there is now growing evidence that Knowledge-driven innovation is a decisive factor in the competitiveness of nations, industries, organizations and firms. Insurance industry has tapped into the emerging strategy for application software companies to provide web access to software previously distributed as local applications.

2. REVIEW OF RELATED LITERATURE

Access controls exist to prevent unauthorized access. Companies should ensure that unauthorized access is not allowed and also authorized users cannot make unnecessary modifications. The controls exist in a variety of forms, from Identification Badges and passwords to access authentication protocols and security measures (Himika, Nainan and Sumaiya, 2012).

Authentication is the act of confirming the truth of an attribute of a single piece of data claimed to be true by an entity. In contrast with identification, which refers to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing, authentication is the process of actually confirming an identity. It might involve confirming the identity of a person by validating their identity documents, biometrics, password etc. In other words, authentication often involves verifying the validity of at least one form of identification (Wikipedia, 2017).

Authentication can be accomplished in many ways. The importance of selecting an environment appropriate authentication method is perhaps the most crucial decision in designing secure systems (Richard, 2001). Authentication is a security process that began long before the age of computing. Only in our current parlance, does it seem linked to our personal digital security. There are three types/categories of factor for authentication.

Something you know: The something you know factor is the most common factor used and can be a password or a simple personal identification number (PIN). However, it is also the easiest to beat.

Something you have: Instead of relying on something that the user knows, secure authentication can also be achieved with something the user has in their possession, such as a mobile phone, smart card, hand-held token etc. A website using multifactor authentication can use SMS based text messaging as their second authentication factor because most people have easy access to mobile phone. So a web site would not only prompt the user to enter their username and password but also send code via SMS to their mobile phone. A smart card is a credit-card sized card that has an embedded certificate used to identify the holder. The user can insert the card into a smart card reader to authenticate the individual. Smart cards are commonly used with a PIN providing multi-factor authentication. The number displayed on the token changes regularly, such as every 60 seconds, and the authentication server always

knows the currently displayed number which make token another mode of achieving secure authentication.

Something you are: This is typically some form of biometric analysis, there are various forms of this, but some common forms are finger/palm print reader, face recognition and retina scan etc. In the past this form of authentication could only be found on things that required the highest level of security, but it became quite common. Most of the smartphones now require fingerprint scanning or face recognition before completing purchases (Darril, 2011) and (Ruchika, 2015).

2.1 Biometric Authentication System

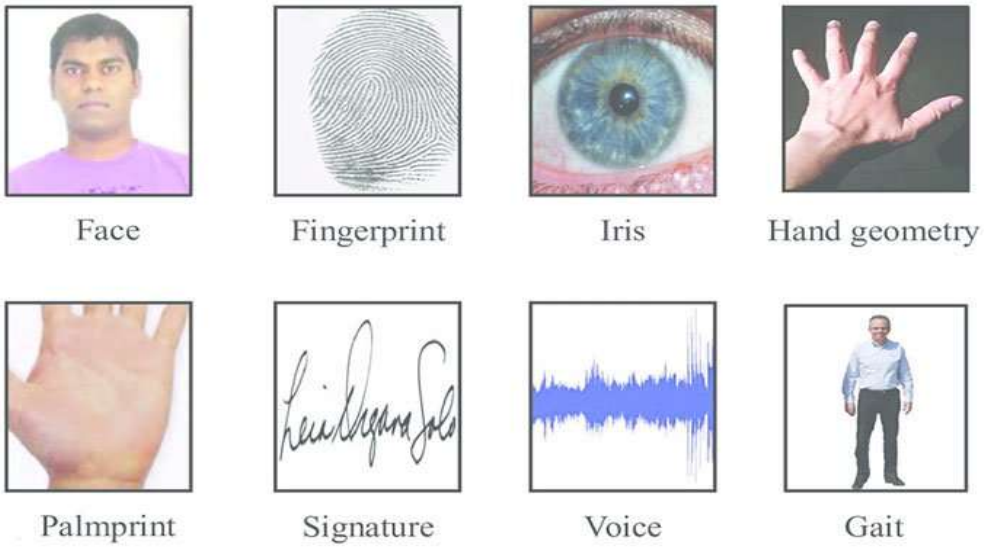
Biometrics refers to technologies for measuring and analyzing a person's physiological or behavioral characteristics. These characteristics are unique to individuals hence can be used to verify or identify a person (Marios, 2013).

There are two main types of biometric technology are:

- Physiological characteristics: The shape or composition of the body.
- Behavioral characteristics: The behavior of a person.

Physiological Biometrics is based on direct measurements and data derived from measurements of a part of the human body, Fingerprints, Face Recognition, Hand geometry, & Hand Bone Iris recognition, Retina Recognition. Behavioral characteristics are related to the pattern of behavior of a person, or data derived from human actions such as voice, gesture, typing rhythm and gait and Signature. Certain biometric identifiers, such s monitoring keystrokes or gait in real time, can be used to provide continuous authentication instead of a single one-off authentication check. Other areas that are being explored in the quest to improve biometric authentication include brainwave signals, electronic tattoos, and a password pill that contains a microchip powered by the acid present in the stomach (Hassanien, 2016).

Measuring and analyzing a person's physiological or behavioral characteristics involves identification and verification. Identification or Recognition implies checking whether a person is in the system’s database or not. This is called One-to-many search. Meanwhile, Verification or authentication implies checking the identity claim presented by a user, otherwise known as One-to-one search (Hassanien, 2016).



Different types of Biometrics Technologies.

Fingerprint recognition and iris scanning have become the most familiar types of biometric security. Conversely, facial recognition and (finger and palm) vein pattern recognition are also gaining in popularity. In this article we consider the pros and cons of all these different techniques. The technology of fingerprint is relatively cheap and easy to use. However, this quality can vary significantly from one fingerprint recognition system to another, with significant discrepancy between systems in terms of false acceptance and false rejection rates *(*Akhtar, 2012).. The following are common finger print readers.

Cross Match Verifier 300 LC 2.0

fingkey access fingerprint access control

Hamster-plus-fingerprint-scanner

u-are-u-4500-fingerprint-scanner

Biometric system architecture represents of a system as a whole, together with a mapping of system functionality to hardware and software mechanism, as well as the mapping of the software architecture to the hardware design, and human interaction with these mechanisms. The block diagram of Biometrics authentication system is presented in figure 1 below.

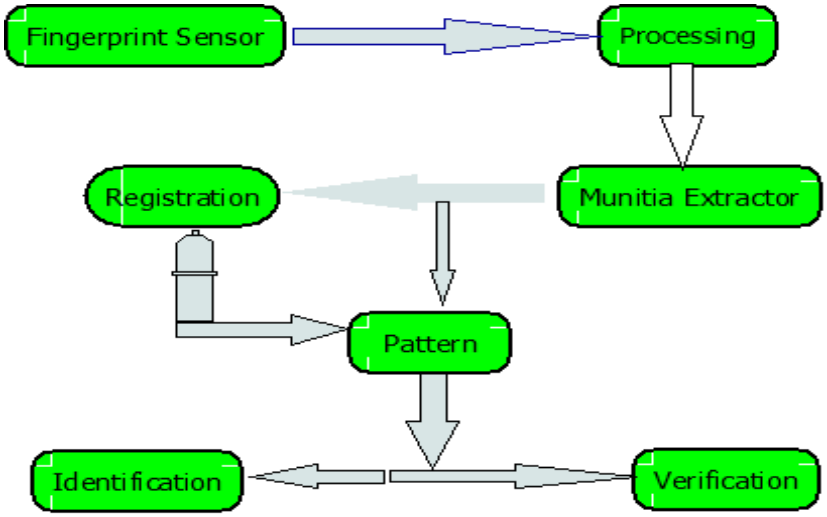


Figure 1: Diagram of Fingerprint Biometric Authentication System.

There are two kinds of errors that biometric systems do:
False rejection (Type 1 error) – a legitimate user is rejected (because the system does not find the user's current biometric data similar enough to the master template stored in the database).

False acceptance (Type 2 error) – an impostor is accepted as a legitimate user (because the system finds the impostors biometric data similar enough to the master template of a legitimate user).

In an ideal system, there are no false rejections and no false acceptances. In a real system, however, these numbers are non-zero and depend on the security threshold. The higher the threshold the more false rejections and less false acceptances and the lower the threshold the less false rejections and more false acceptances. The number of false rejections and the number of false acceptances are inversely proportional. The decision which threshold to use depends mainly on the purpose of the entire biometric system. It is chosen as a compromise between the security and the usability of the system. The number of false rejections/false acceptances is usually expressed as a percentage from the total number of authorized/unauthorized access attempts (Zdenek et al., 2000).

While biometrics technology provides a strong user authentication solution, there are other variables to be considered in the authentication protocol. When a high level of security is needed, it is recommended that we combine other authentication factors with biometrics. When we combine what you know, what you have, and what you are, we will have achieved the highest level of security in our e-insurance web application.

2.2 One Time Password (OTP)

OTP (One Time Passwords) is a string of characters or numeric values automatically created or generated to be used for one single login attempt. OTP can be sent to the user's phone through Short Message Service (SMS) or Push messaging and is used to secure web-based services, private credentials and data. OTP reduces the risk of counterfeit and unauthorized login attempts and consequently the threat of stolen data. OTP comes in various forms and dimensions, however, it always add an extra layer of authentication (Raak, 2017).

Initially, the majority of OTP were sent as SMS messages. This implies that users need reliable high quality SMS routes. The moment the user has initiated his login attempt, keying in his username and the right password, an SMS with the OTP is sent to the mobile number linked to the account. The user then enters this code shown on this phone in the login screen, finalizing the authentication process.

One time password can be generated in any of the two ways, Time-synchronized OTP and A counter-synchronized OTP: In time-synchronized OTPs, password should be entered by the user within a certain period of time, otherwise, it gets expired and another OTP have to be generated. While, with counter-synchronized OTPs, a counter is synchronized between the user's device and the server. The device counter is advanced each time an OTP is requested (Parmar, Nainan and Thaseen, 2012). OTPs are delivered via text messaging which is the common method used for the delivery of OTP. In other cases, it can also be delivered through Instant Message Services and Email. These services are almost common with minimum cost of usage.

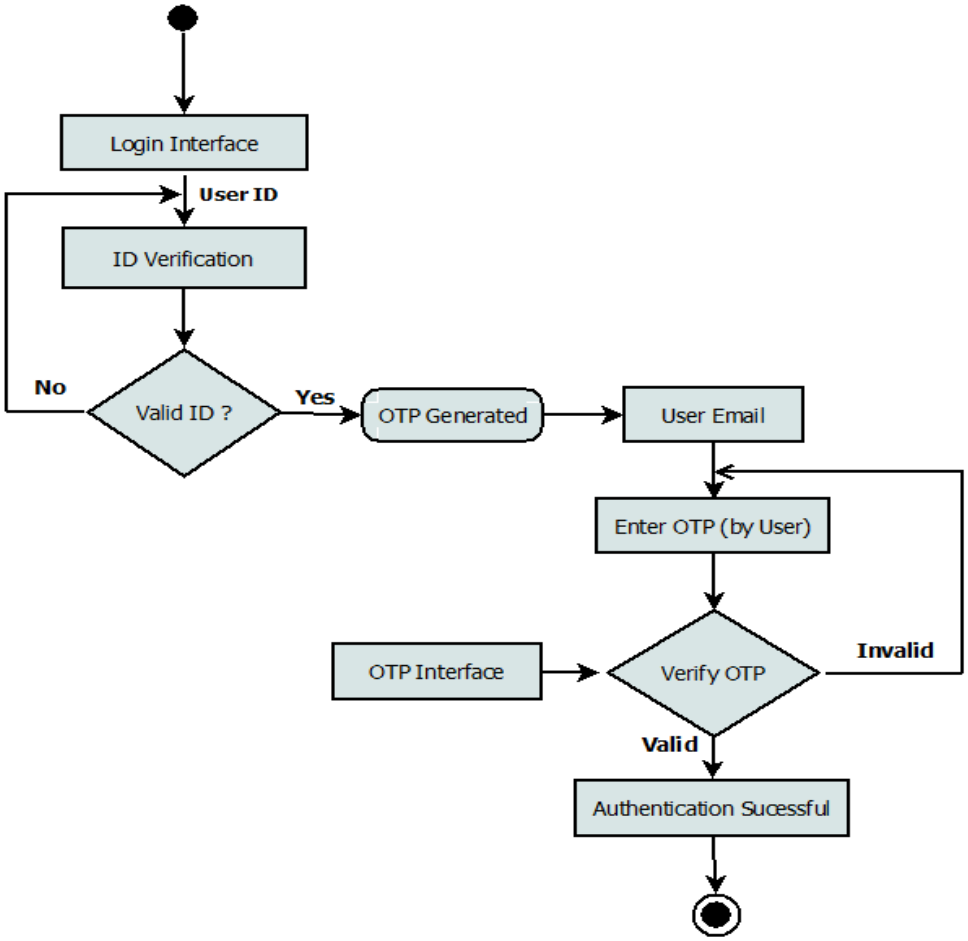
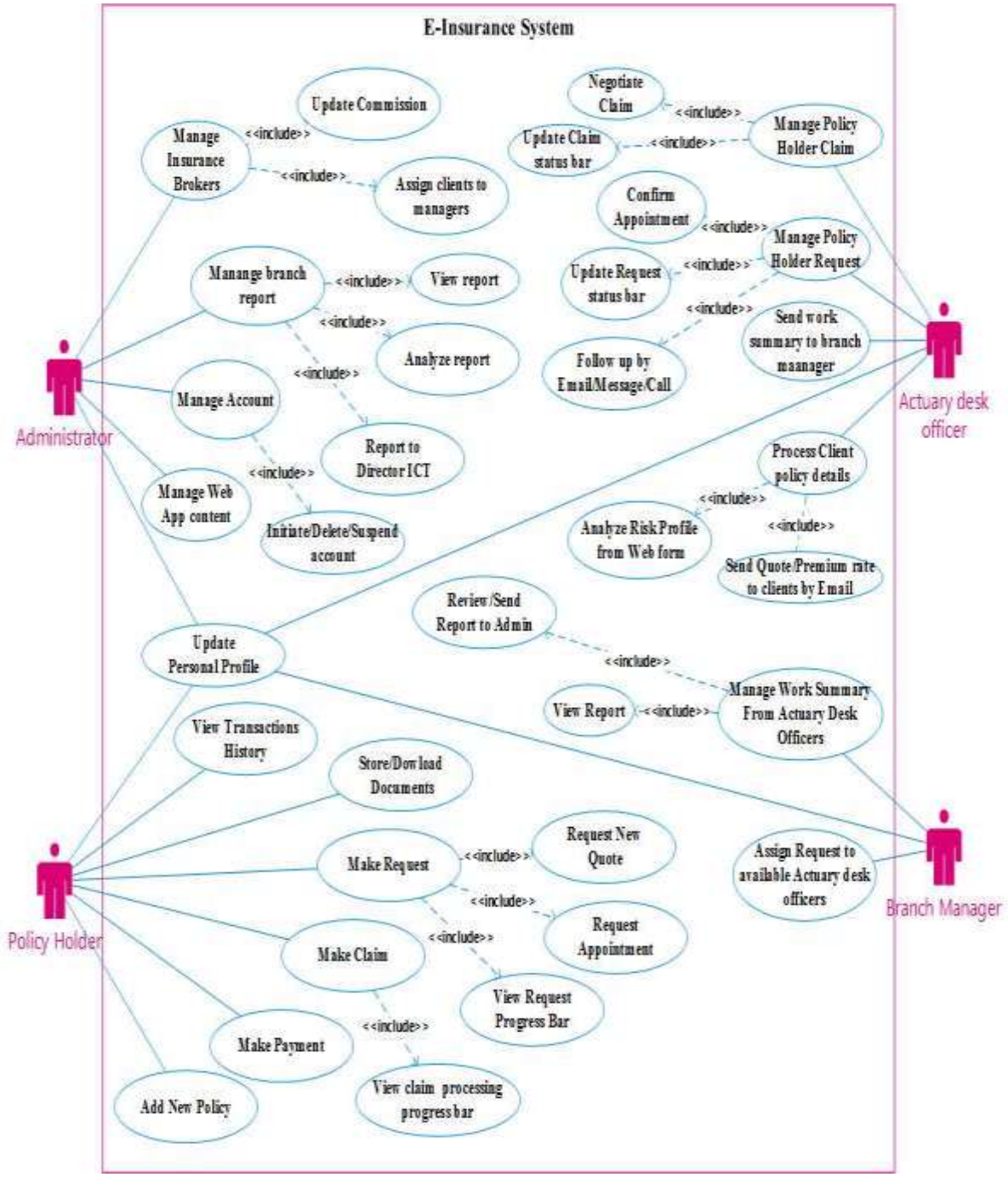


Figure 2: Model of Typical Activity Flow in OTP Authentication.

3. System Design

The proposed system is a planned secured automated web application for electronic insurance service, which would, provides variety of optional multi-level authentication mechanisms which includes either biometric authentication or one-time-password (OTP). This feature is thought of to prevent the security threat on policy holders' classified data/file that the existing systems fail to address. The system seeks to add to the conventional features made available to staff/representative and web administrator of the insurer, these features includes an automated quote engine, summary of the commission of affiliated insurance brokers and a concise report page of all claims made, list of online visitor and their operation; and accounting transaction such as receipts and payment details. This feature enables the management board to electronically evaluate the operation of the organization from a central location and make decisions based on real time data gathered from the proposed system via the report page.

a. Use Case Diagram



b. Activity Diagram

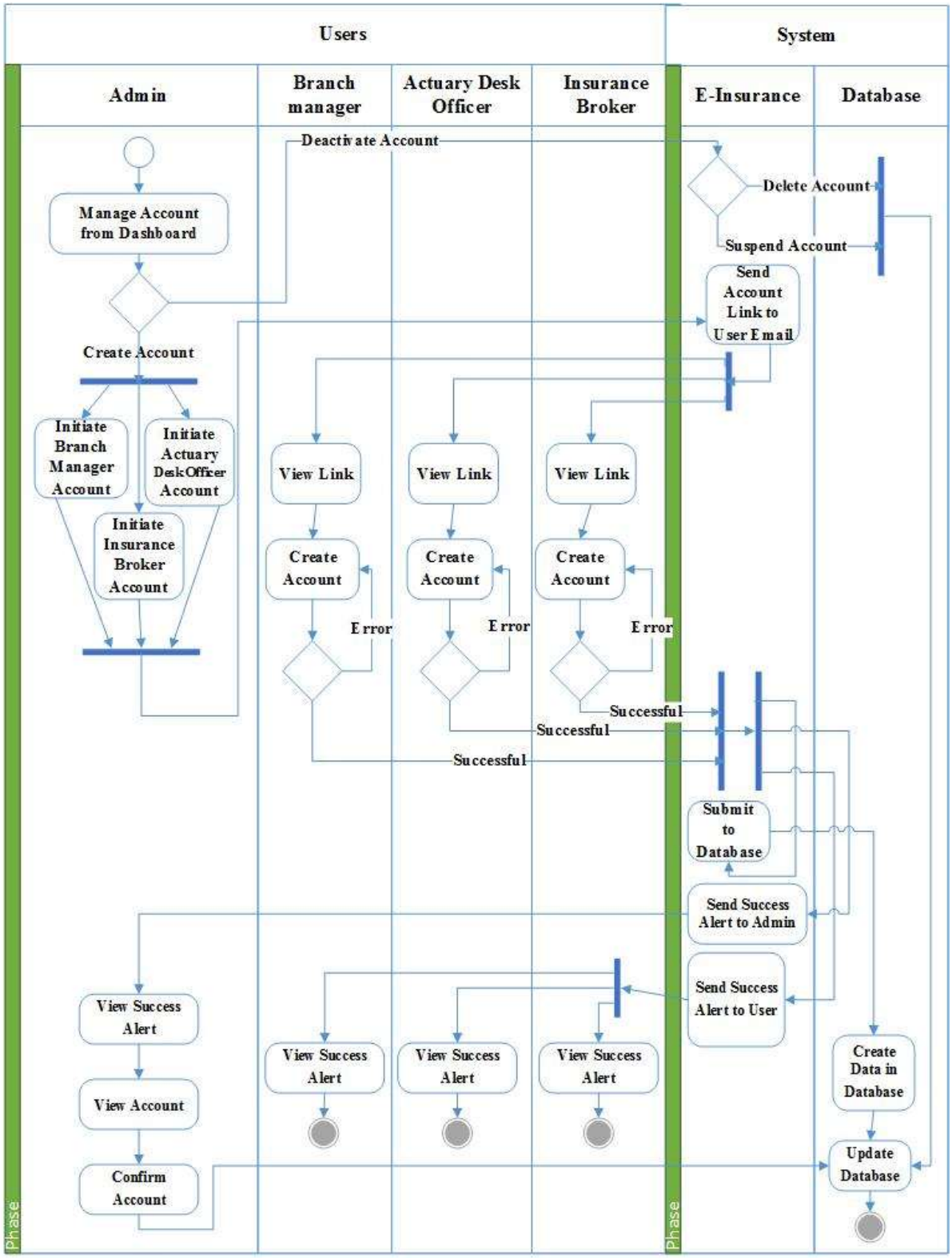


Figure 4: Activity diagram showing control flow of account creation for branch manager, actuary desk officer, and insurance broker.

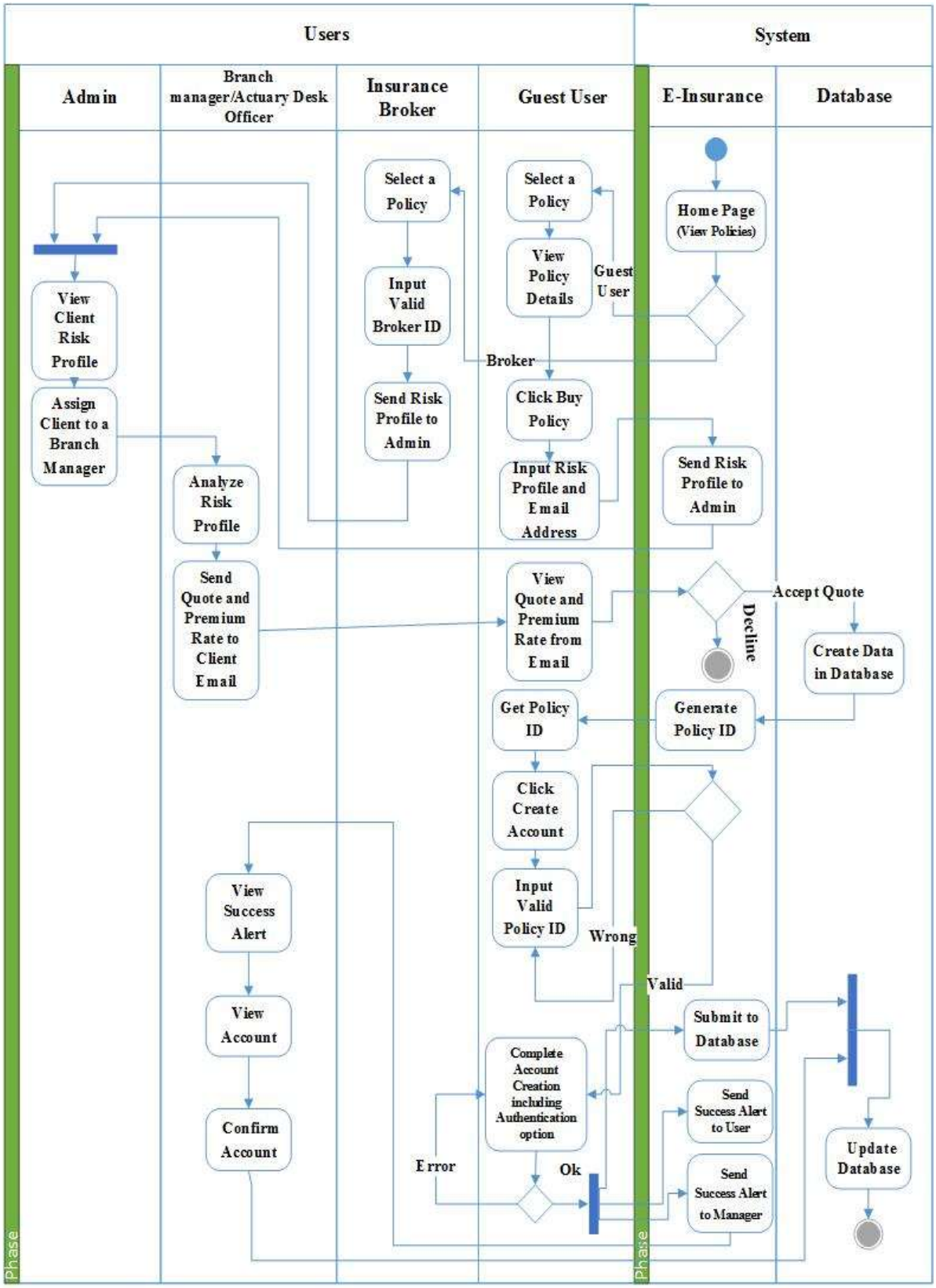


Figure 5: Activity diagram showing control flow of account creation for prospective policy holder.

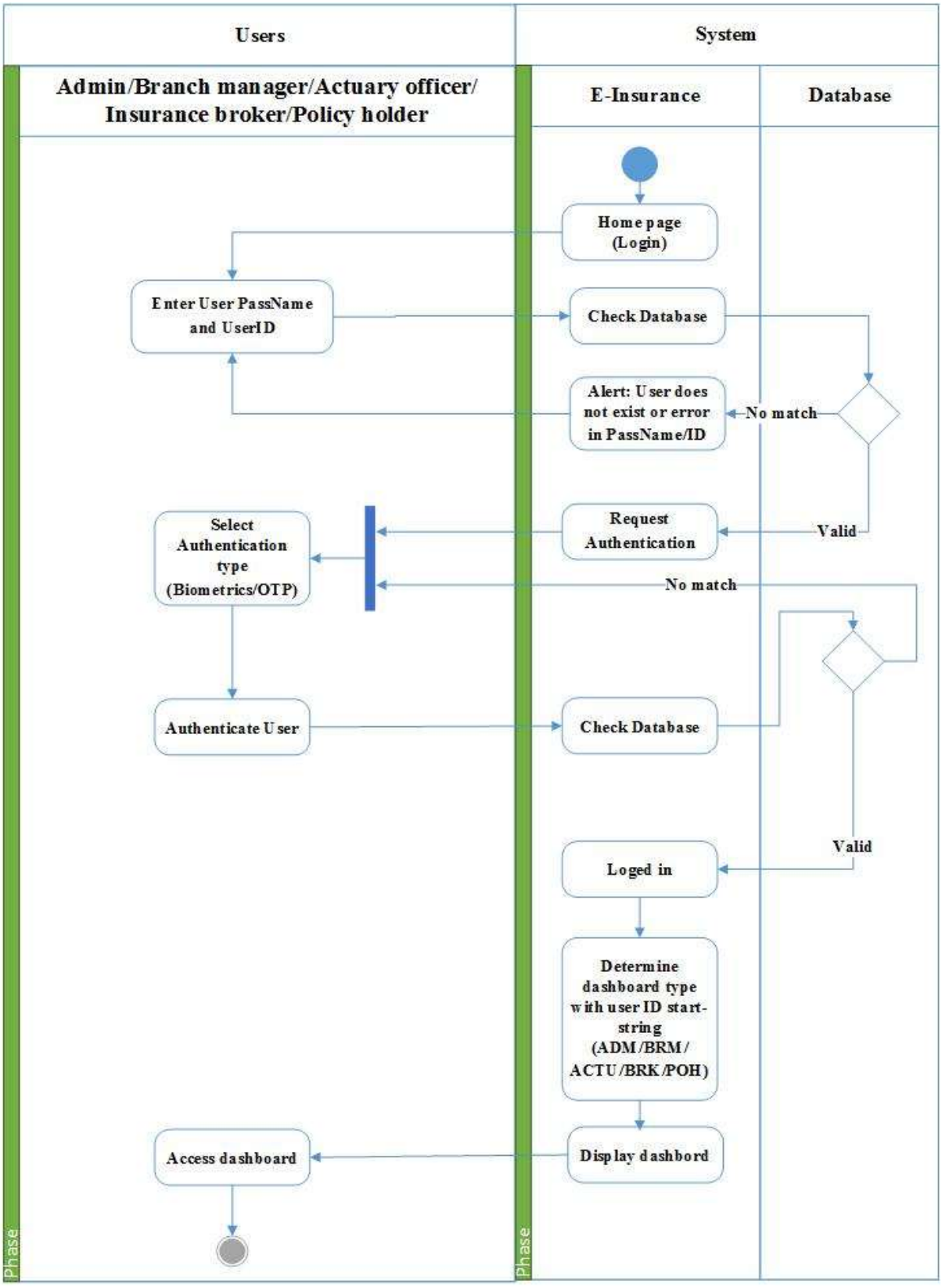


Figure 6: Activity diagram showing control flow of login system and authentication method.

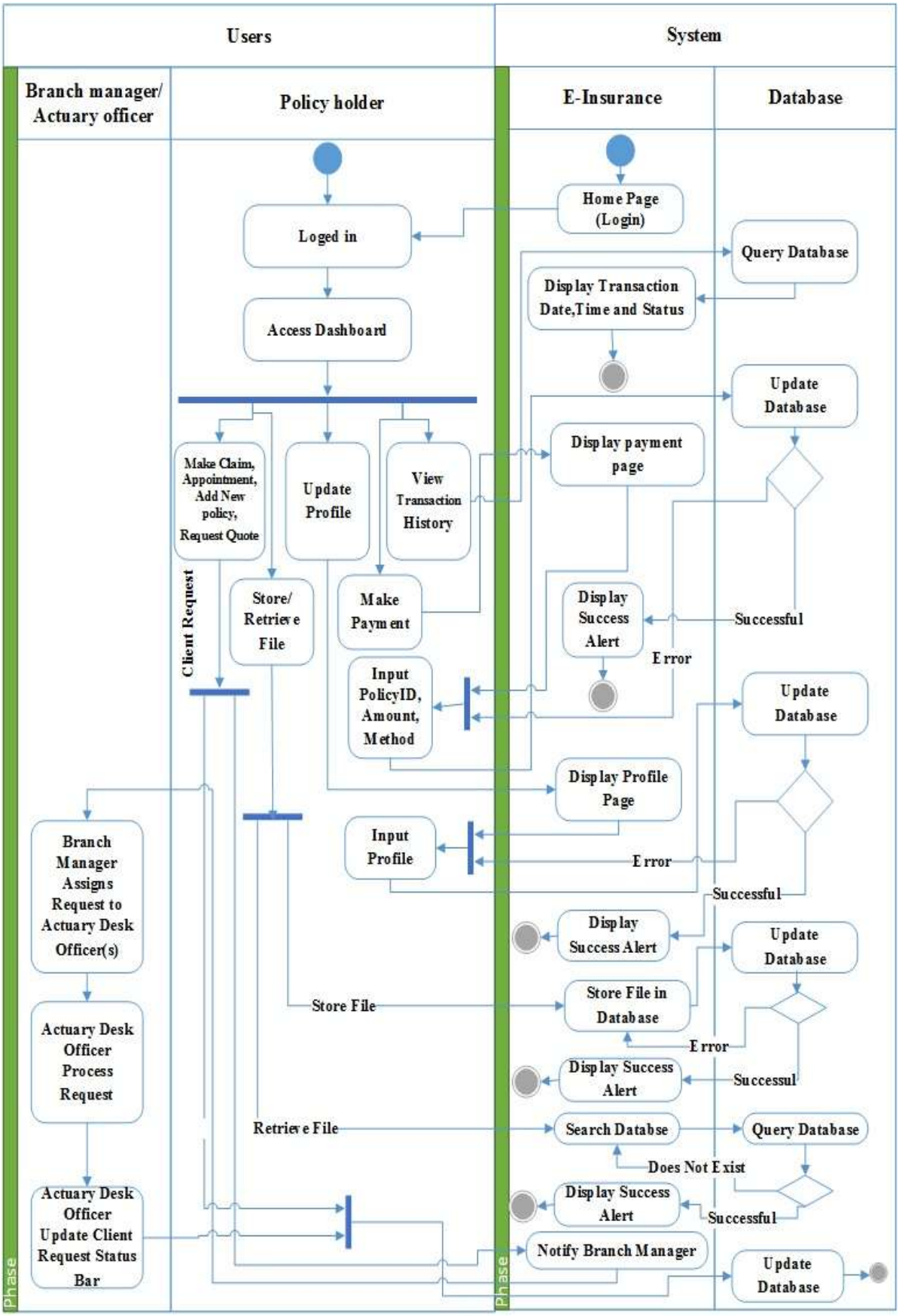


Figure 7: Activity diagram showing control flow of insurance value chain and user activity.

c. Database Design and Definition

A Data Dictionary, also called a Data Definition Matrix, provides detailed information about the business data, such as standard definitions of data elements, their meanings, and allowable values. While a conceptual or logical Entity Relationship Diagram will focus on the high-level business concepts, a Data Dictionary will provide more detail about each attribute of a business concept. Fundamentally, data dictionary provides a tool that enables you to communicate business stakeholder requirements in such a way that your technical team can more easily design a relational database or data structure to meet those requirements. It helps avoid project mishaps such as requiring information in a field that a business stakeholder can't reasonably be expected to provide, or expecting the wrong type of information in a field (Laura, 2017).

In the study, an Entity Relationship Diagram (ERD) is used to graphical represent entities in the system and their relationships to each other. An ER model provides a means for communication. An ERD contains different symbols and connectors that visualize two important information: The major entities within the system scope, and the inter-relationships among these entities.

Tables 1-2: User_Name and Authentication Tables.

UserName Table			
Column Name	**Constraint**	**Data Type**	**Description**
UserID	PK	Long	User ID generated by system
FirstName	Not Null	Varchar(15)	User first name
MiddleName	Not Null	Varchar(15)	User middle name
SurName	Not Null	Varchar(15)	User surname

Authentication Table			
Column Name	**Constraint**	**Data Type**	**Description**
User_PassName	PK	Varchar(10)	Something you know factor authentication
ID	Not Null	Int	Auto increment
UserID	FK,Not null	Long	Something you have factor authentication
Bio_Data		Blob	Something you are factor authentication
OTP		Varchar(10)	Something you don't know factor authentication

Tables 2–3: User_Policy and Req_ProgBar Tables.

UserPolicy Table			
Column Name	**Constraint**	**Data Type**	**Description**
PolicyNum	PK	Long	Policy number generated by the system while buying every policy newly
UserID	FK,Not Null	Long	`Foreign key of UserName table linking the First, Middle and Surname of policy holder to a policy
PolicyType	Not Null	Varchar(20)	Either Health, Education, Auto, Life or home Insurance,
IssuedDate	Not Null	DateTime	Date a policy was bought
IssuedTime	Not Null	DateTime	Time a policy was bought
Deductible	Not Null	Double	Amount paid before reimbursement of any claim
Premium	Not Null	Double	Amount a policy holder pays periodically
DueDate	Not Null	DateTime	Due date of paying premiums

Req_ProgBar Table			
Column Name	**Constraint**	**Data Type**	**Description**
Req_ProgID	PK	Int	Auto increment
UserID	FK,Not Null	Long	Foreign key of UserName table linking the First, Middle and Surname of policy holder to a request progress bar
PolicyNum	FK,Not Null	Long	Foreign key of UserPolicy table showing the policy type a request was made for
Status1		Varchar(15)	Acknowledged
Status2		Varchar(15)	Processing
Status3		Varchar(15)	concluding
Status4		Varchar(15)	Done

Table 5: Reference_Policy Table.

Ref_Policy Table			
Column Name	**Constraint**	**Data Type**	**Description**
Ref_PolicyID	PK	Long	Reference policy ID generated by the system
ID	Not Null	Int	Auto increment
BasePrice	Not Null	Double	Least amount that can purchase a policy base on risk profile provided
Description	Not Null	Varchar(MAX)	Short note on a type of policy
Coverage	Not Null	Varchar	The condition of service on a particular policy

Table 6: Risk_Profile Table.

RiskProfile Table			
Column Name	**Constraint**	**Data Type**	**Description**
ID	PK	Int	Auto increment
Ref_PolicyID	FK, Not Null	Long	Foreign key of Ref_Policy table linking the details of a policy which a client is providing risk profile for
Email	Not Null	Varchar(40)	A valid email address which will be used to complete the process of buying a policy
Address	Not Null	Varchar(100)	How to locate a client
DoBirth	Not Null	Varchar(10)	For determining premium rate and predictive analysis
Married	Not Null	Varchar(10)	For determining premium rate and predictive analysis
Num_Children	Not Null	Int	For determining premium rate and predictive analysis
Occupation	Not Null	Varhar(10)	For determining premium rate and predictive analysis
Entrepreneur	Not Null	Varchar(5)	For determining premium rate and predictive analysis
Employed	Not Null	Varchar(5)	For determining premium rate and predictive analysis
Retired	Not Null	Varchar(5)	For determining premium rate and predictive analysis
MonthlyIncome	Not Null	Double	For determining premium rate and predictive analysis
OwnAcar	Not Null	Varchar(5)	For determining premium rate and predictive analysis
OwnAhouse	Not Null	Varchar(5)	For determining premium rate and predictive analysis
AnyDebt	Not Null	Varchar(5)	For determining premium rate and predictive analysis
AnyInvestment	Not Null	Varchar(5)	For determining premium rate and predictive analysis
HealthChallenge	Not Null	Varchar(20)	For determining premium rate and predictive analysis
NumAccidentIn2yrs	Not Null	Int	For determining premium rate and predictive analysis
EstMonthlyExpenditure	Not Null	Double	For determining premium rate and predictive analysis
InterestedInAcademics	Not Null	Varchar(5)	For determining premium rate and predictive analysis

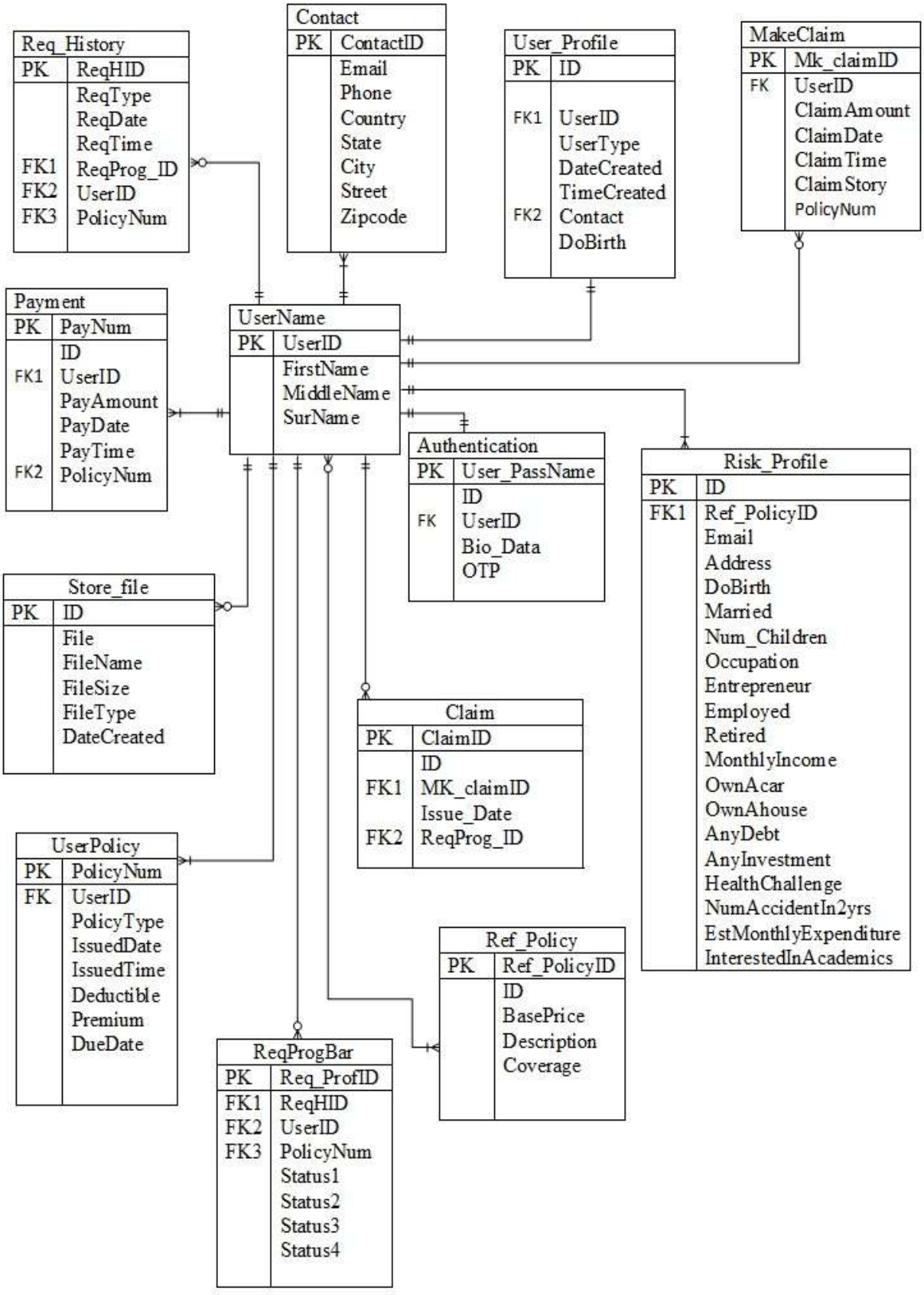


Figure 8: Entity Relation Diagram of the E-Insurance web application database.

REFERENCES

1. Akhtar, Z. (2012). Security of Multimodal Biometric Systems against Spoof Attacks. Department of Electrical and Electronic Engineering, University of Cagliari, Cagliari, Italy, 6 March 2012.
2. Darril G. (2011) "*Understanding the Three Factors of Authentication*" Publisher: Pearson.
3. Hassanien, A. E. (2016). Age verification in real time keeping children safe online biometric solution. https://www.slideshare.net/AboulEllaHassanien/age-verification-in-real-time-keeping-children-safe-online-biometric-solution.
4. Ifeanyi, N. (2015) *"Ways to Improve Insurance Penetration in Nigeria"* Retrieved from infoguidenigeria: https://infoguidenigeria.com/improve-insurance-penetration/.
5. Laura Brandenburg (2017)*"Requirements Models and Specifications"*Retrieved from: http://www.bridging-the-gap.com/data-dictionary/.
6. Leadway (2017) "*About Us*" Retrieved from Leadway Assurance: http://www.leadway.com/about-leadway-assurance/our-history/.
7. Marios S. (2013) "*Introduction to biometric technology and application*" Publisher: Carnegie Mellon University CyLab.
8. Oluwagbemi, O. et al, (2011) "*The Impact of Information Technology in Nigeria's Banking Industry*" Publisher: Journal of computer science and engineering.
9. Parmar, H, Nainan, N and Thaseen, S. (2012). Generation of Secure One-Time Password Based on Image Authentication. In the Journal of Computer Science & Information Technology (CS & IT). pp. 195–206, 2012. © CS & IT-CSCP 2012.
10. Raak, C.V. (2017). What is An OTP:. https://www.cm.com/blog/what-is-otp-one-time-password/.
11. Richard D. (2001) "*An Overview of Different Authentication Methods and Protocols*" Publisher: SANS Institute InfoSec Reading Room.
12. Ruchika M. (2015) "*Multifactor authentication capability*" Retrieved from: https://www.whitehatsec.com/blog/multi-factor-authentication-capabilities/.
13. Shaun, C. (2013) *"Insurance in a digital world: the time is now"* Publisher: EY Global InsuranceDigital Survey.
14. Wikipedia (2017) "what is Authentication" Retrieved from: https://en.wikipedia.org/wiki/Authentication.
15. Zdenek R. et al., (2000) "*Biometric Authentication Systems*" Publisher: Faculty of Informatics Masaryk University.