العدد الواحد والثلاثون
تاريخ الإصدار: 2 – آيار – 2021 م
www.ajsp.net
ISSN: 2663-5798

“A Verification System for Multi-Factor Authentication for E-Healthcare Architectures”

Researcher:

Eng. Ahmad Abdullah Alghamdi

MSc Computer Security and Forensics and Ph.D. student in Computer Science

King Abdulaziz University

Abstract:

E-health care or Electronic healthcare systems gained high attention in this highly technological and internet world in order to provide high quality healthcare service to the patients. Besides facing high attention, E-health care systems are also facing security issues due to the access of unauthorised users into the system. This research aimed at minimising these security issues faced by e-health care systems by developing a multi-factor authentication method. This multi-factor authentication method uses three aspects to authenticate a user namely password, dynamically generated NFC code and face recognition. This authentication system is implemented with the use of NFC smart card device to dynamically generate NFC code and AES 256 encryption method to encrypt password and random number displayed on screen. Java, Oracle forms and Oracle 10G (database) are used for the implementation purpose, which is later tested and evaluated in this research.

Chapter 1: Introduction

1.1 Introduction

Huge advancements in the field of networking and also technology have not only provided several opportunities in interconnecting the devices but also made computer security and network security a highly challenging issue. Authentication is widely considered as one of the best mechanisms to assure security to a standalone computer or a complete network. According to Bae et al (2017), an authentication system is defined as the one that verifies identify of an individual before allowing them to access a critical resource. Many studies in literature (Karimian et al, 2016) have shown high dependence of these authentication mechanisms on the individuals and their abilities as the main purpose of this authentication mechanism is to verify people identity. The increase in the web applications in this internet world has also increased the number of security breaches on the identity of authorized users, which thereby made majority of the web applications verify user identity even for remote applications. Among the various applications that have been developed in this information technology world, e-health care system is one of the most important one which involves in the adoption of internet and information technologies to offer health care services to the patients. According to Shahabadkar et al (2017), the main purpose of e-health care system lies in storing patient personal and medical information, providing a two way communication link between patients and physicians and providing the facility of e-prescriptions. Proper functioning of this e-health care system requires dealing with high critical and private information of the patients such as their personal details and medical history, which is restricted to be accessed only by specific set of people. Growing number of individual identify breaches in the current internet world shows the need of a strong authentication mechanism for these e-health care systems in order to ensure that only authorized users are able to access the database of patient information.

Lawrence et al (2017) indicated that all the existing authentication mechanisms of user identity are based on three types of information which includes what is known to the user, what is posed by the user, and what actually the user id. All these three types of information have resulted in the evaluation of knowledge based authentication systems, token based authentication systems and biometric authentications respectively. Each of these authentication systems possess their own merits and demerits, which made them to be used in a different type of applications based on application requirements. For instance knowledge based authentication is easy to implement but requires users to remember large number of lengthy passwords used to access their online accounts, emails and their personal computers. Chaudhry et al (2015) have specified this problem as ‘password problem’ in which people who are unable to remember lengthy and alphanumeric passwords end up with following poor password practises like setting up a weak password. However, Karimian et al (2016) indicated that the technology advancements have helped in overcoming this ‘password problem’ through the development of password management systems. According to Brumen et al (2016), the password management systems like LastPass and KeePass help its customers

to store their complex passwords in a secure manner by adding all the required applications in their secure vault (Lastpass, 2017). However, these password management systems also suffer from the weakness if the main account of LastPasss or KeePass is cracked. In this situation, the attacker will be able to access all the user accounts which are present in secure vault, thereby showing the need of a secure authentication system. Biometric authentication system is considered as more secure than knowledge based authentication system as this authentication system verifies user identity based on the unique features present in their human body such as fingerprints, palm prints, IRIS recognition, facial recognition and so on (Galbally et al, 2015). However, the high cost and effort associated with the implementation of this biometric authentication system has made it to be used only in high critical applications like military and homeland security.

Taking the need of providing a strong authentication system for e-health care system and also by considering the merits and demerits of the different existing authentication systems, this research involves in developing a multifactor authentication system for e-health care applications. The main aim of this multifactor authentication system is to verify user identify based on the combination of all the three authentication systems (knowledge, token and biometrics). Despite of this multifactor authentication system requiring higher resources, the need to secure patient information from unauthorized access has resulted in developing this multifactor authentication system.

1.2 Problem Statement

With the evolution and boom of information technology, the use of computer and smart devices has become an integral part of our day-to-day live, yet this has also provided an adverse opportunity for malicious users to assume fake identity to gain unauthorized access to system. Earlier use of knowledge centric authentication relied on PIN, pattern locks and passwords, has proven vulnerable to malicious attacks. The inadequacies necessitated a multi-factor authentication, which combine two or more types of authentication components. This research presents three components of knowledge, possessive and a biometrics (face recognition) method of user's authentication and verification for a secure e-healthcare system. It offers continuous user's authentication within a timely session during which is been used.

Therefore, a database will be created for a medical system, which contains patient-related information, e-mail and self-service display, and also helps identify the patient through identifying face features, with the aim of access to patient's information rapidly and accurately. Moreover, all system users are able to use email messages within the system, so that all communications are highly encrypted, in order to minimize any attempts of content access or obstruction. Through the system, the patient can set appointments with the doctor, and pay the treatment costs through card.

The system also provides high level of information and privacy protection, and accurate identification of system user, so that no piece of information can be accessed without first verifying the identity through three phases; namely (verifying identity through the face, verification through smart card, plus username and password). When the user is identified by the system through these three steps, secure access is made to the system, and after logging into the system, no information may be added, amended or deleted without again verifying the powers and identity, for the sake of ensuring integrity and authenticity of the information against manipulation.

1.3 Aim and Objectives

Design and implement of multi-factor authentication system for e-healthcare architecture.

The main objectives of this project are listed below**:**

1. To investigate the current e-healthcare systems implementations with particular emphasis on security, and privacy.
2. To design and implement face e-health face recognition system.

3. To implement face NFC based smart card/poster as part components for verification and access to patient data.
4. To deploy known asymmetric technique (AES256) for data and password encryption.
5. To test and evaluate the system operations and compare its features to existing systems.

1.4 Methodology Used

Rapid Application Methodology is used to carry out this project in structured way. By adopting this rapid application methodology, the current project is carried out in four main stages such as requirement analysis, system design, system development, testing and evaluation.

Requirement Analysis: This stage involves in critically analysing the existing works present in the literature of authentication system and e-health care application security. The functional and non-functional requirements of an authentication system are also identified in this step.

Design: This stage involves in designing the multifactor authentication system and presenting them with the help of unified modelling language diagrams.

System Development: Taking the design diagrams, Java ,Oracle Forms and Oracle 10G database are used to develop the multifactor authentication system.

Testing and Evaluation: This stage involves in testing the developed application using test cases and then evaluates it.

Chapter 2: Literature Review

2.1 Overview

This chapter covers the literature review of this project in which the findings of the existing reviews in the literature of e-healthcare system authentication are presented. The details of the proposed multi-factor authentication system are also presented in this chapter.

2.2 E -health Care System

Huge advancements in the internet technology and wireless connectivity have resulted in the use of internet across a wide range of applications. Health care is one such field that is greatly revolutionised with the use of information technologies and internet, there by resulting in the formation of e-health care applications. According to Boric-Lubecke et al (2014), e-health care is specified as the health care practise is providing with the use of various communication and electronic devices. Proper working of these e-health care applications requires use of several health care aspects such as electronic prescriptions, health management, electronic medical records and the remote monitoring. E-health care offers efficiency in collecting, storing, processing and also retrieving the patient information as patient data is highly stored in the form of electronic format. In this health care system, patient records are provided access either in centralized manner or in a decentralized manner. Centralized access is provided when database is accessed from a single location that is authorized and decentralized access is offered when data base is accessed from multiple locations that is authorized.

According to Pussewalage & Oleshchuk (2016), main objective of any type of e-health care system lies in offering an efficient way of managing patient health records instead of relying on manual way that is highly error prone. The huge importance gained by these e-health care systems is also due to its ability in providing delivery of high quality of service to the patients of e-health care services. Inspire of e-health care system dealing with highly crucial information about the patients, there is a need of providing high level of security to the data stored in e-health care system. Despite of this importance of e-health care security, there are several security challenges faced by some of the existing e-health care systems.

2.3 Security Issues of e-health care system

Critical review of some of the existing works in literature has identified some of the commonly occurring security problems among e-health care systems. All these security issues detailed below are mainly aimed at gaining access to the highly private information of the patients present in the database of e-health care system.

1. **Unauthorized Access- Threats on Password and Face Recognition**

One of the commonly occurring issues in majority of the e-health care applications is the provision of unauthorized access to the electronic records of the patients. This security issue occurs when the roles and the privileges of system users are not defined properly. This poor assignment of system user roles and privileges can result in one accessing the information present in the database and performing and performing any kind of malicious action. According to Ma & Han (2009), lack of proper authentication mechanisms is considered as one of the main reasons for this unauthorized access security issue.

2. **Attacks on Host Estates - Threats on NFC device and Email System**

The second type of security issue that is faced by majority of the e-health care systems is the attack on the host estates related to the e-health care system. These attacks are classified under three types namely hardware concession and the software concession. Hardware concession involves in the presence of faulty hardware that could generate high level of serious concerns on integrity of patient data. Software concession on the other hand deals with different types of the software updates. User concession involves in some of the attacks on patient medical information that might be launched when third party applications are installed by the patients their laptops, smart phone or in the shared devices where e-health care systems are accessed. All these three types of attacks can bring significant changes to the monitoring system of patient and can also affect system mal functioning. According to Alzahrani et al (2013) user concession type of attack can also result in user gaining unauthorized access to the data or network resources of the patient.

3. **Attacks on the health records of patients - Threats on encryption methods**

In a typical e-health care system involves in managing the storage, sharing and access to the patient health information. This process must be done in highly confidential and secured manner because of the involvement of high error prone electronic channels and the internet. A study carried out by Garrety et al (2014) indicated that gaining unauthorized access to the e-health care system by the attackers is the main reason for the attacks on patient health care records. Another study By Zhao et al (2016) indicated that attacks like man in the middle involves in the attacker gaining access to the patient health care information that is transmitted over the internet in unauthorized manner. Even though the health care records of the patients are becoming highly complex, they are mainly combined with information systems of the provider in order to provide proper communications where this e-health care information can be exchanged. In such kind of situation, attacks on personal health records of the patients causes serious issues to the complete e-health care system.

4. **Internet Security Based Attacks - Threats on password and encryption methods**

In the current technological world, internet has become of the main sources of information as it connects various individuals with the health experts for gaining high level of support. This use of internet as part of health care system enables in the provision of access to various services by several users across the world. Besides all these merits of using internet, it also possesses several vulnerabilities for e-health systems. Use of internet makes transmission of patient data over the internet either in encrypted or plan text format. The high penetration of internet has made everyone to access it irrespective of the level of security offered by the application. Launch of security attacks over the patient data transmitted over the internet can cause serious implication on the security of e-health care system.

5. **Tracking User Activities - Threats on data encryption, SMS and Password**

Ford and Graft (2014) in a study reported that tracking activities of the users present in e-health care system is one of the security issues faced by the present applications. As e-health care systems records the data about user activities that are performed when they are logged in, tracking such activity can result in accessing the system in unauthorized manner.

A study carried out by Wang et al (2014) indicated that improper assignment of user privileges can result in tracking these user activities in highly unauthorized manner.

2.4 Issues of System Security

These kinds of issues are launched because of less security protection offered to e-health care system with respect to its hardware, software, storage, data processing and human interface. Lack of offering proper protection mechanism for the data stored in e-health care system without considering the three aspects like secure processing, transmission and storage can result in the cause of this security issue.

2.5 Security requirements of e-health care system

Taking the key feature of e-health care system regarding the storage of highly private health care information of the patients, the current health care system consists of various security requirements. Some of the key security requirements of a typical e-health care system are (Pussewalage & Oleshchuk, 2016)

1. **Privacy**: This security requirement indicates that private information of the patients and the other users of e-health care system must not be accessed or misused by the attacker.
2. **Integrity**: the integrity security requirement of e-health care applications indicates the need of data consistency along with the requirement of high protection to the data from unintended level of alterations. This integrity requirement also takes the access to the resources of e-health care system into account.
3. **Authentication**: this is the third important security requirement of e-health care systems which deals with the process of verifying user identify before allowing the user to access the application or a particular resource in it. This security requirement also indicates that only authorized users must be allowed to access the e-health care system, data present in this system along with the different services provided in this system.

2.6 Authentication systems for E-health architecture

In the literature, a significant number of studies have focused on providing better authentication system for electronic healthcare applications. A study carried out by Frontoni et al (2014) developed Nu.Saframework called Nuvola Sanitaria framework that intends in providing security and also privacy for electronic health records using encryption algorithms. Every patient record is associated with a random patient identifier and only based on the verification of the patient identifier; this framework allows a user to access the patient records. A study carried out by Bhattasali et al (2014) developed a two factor authentication system for health care applications. In this authentication system biometrics is the first factor used and secret pin is the second factor used for verifying the identified of the user who is required to access the patient health records. The ability of this authentication mechanism in giving trust scores at each step of authentication process made this mechanism efficient in authenticating the end users based on the obtained final trust score. A study carried out by He et al (2015) developed an authentication system combined with key agreement mechanism suitable for mobile health care applications. This developed system consists of four main steps namely user registration, user login, authentication and the key update. In other words use of a randomly generated key is done in this authentication mechanism for authenticating the user in an efficient manner.

The cost effectiveness and less computational overhead have made this authentication mechanism suitable for mobile health care applications. A study carried out Kim et al (2014) developed smart card authentication system in order to protect the privacy of the patient medical details by allowing only authorized users to access the application. However, a study carried out by Chaudhry et al (2015) showed that this authentication mechanism is vulnerable to stolen smart card attack.

Karimian et al (2016) developed a biometrics based authentication system based on Photo Plethysmography (PPG). This study identified that PPG signals consists of unique properties that are useful for authenticating human identity and at the same time can be easily captured using the emerging IoT (Internet of Things) based sensors. He and Zeadally (2015) developed RFID (Radio Frequency Identification) based authentication system for e-healthcare applications that are deployed using IoT technologies. This authentication mechanism is proposed to use Elliptical Curve Cryptography that encrypts the data to restrict access from unauthorized users.

2.7 Existing Authentication Mechanisms

E-health is defined as a system that uses Information and Communication Technologies (ICTs) in order to deliver the healthcare services in an effective manner. E-health is also considered as the process of using the electronic and the telecommunication gadgets to provide sustainable health care services in an efficient manner. According to Zhang et al (2017), e-healthcare system through the provision of the access to the patient records in either centralised or decentralised way has provided scope of several applications such as e-prescribing and telemedicine. Besides e-healthcare systems offering several advantages, they are also associated with various security issues. A study carried out by Idoga et al (2016) identified some of the key security issues faced by e-healthcare applications such as unauthorized access to the patient records, attacks launched on patient records, and attacks on the host resources. One common thing that is identified to be present among all these security issues is the unauthorized access gained by the attacker into the e-healthcare applications.

Taking the review of existing security issues that are faced by e-health care systems and the security requirements of these e-health care system, it is evident that authentication is the high priority security requirement that must be provided by majority of the e-health care systems. The main reason for this is due to the authorized access being one of the main reasons for the launch of several security issues on e-health care system. Authentication system involves in the process of verifying identity of a user based on the information that is provided by the user. Odelu et al (2015) indicated that all the existing authentication mechanisms are based on the three types of information like the information that is known by the user, information that user has and information that the user actually is. Taking these three types of information authentication mechanisms are classified into knowledge based authentication, token based authentication and the biometric authentication system.

1. **Knowledge based authentication system**

Knowledge based authentication system works based on the knowledge of the user regarding the information that they remember about the secret information. Some of the existing authentication mechanisms that come under knowledge based authentication are traditional user id and password method, single sign-on authentication method and one time password. All these three authentication mechanisms work based on the information that is presented by the user in terms of a memorable thing which the user remembers. In case of traditional user id and password, the user is required to pre-register user name and password details which are required to be enter during login stage. One time password is another knowledge based authentication in which user is required to remember the pin in order to gain access to the system in authorized manner. Single sign on authentication method which involves in adopting one step authentication mechanism for the multiple applications also prompts the user to enter a secret password that is known to the user. Even though all these knowledge based authentication mechanism have advantages in terms of their easy implementation, their posts, serious issues when the static passwords are

the dynamic passwords that are generated or being stolen. According to Burger (2017), even the dynamic one time passwords are prone to security issues due to the assignment of small length and easily remembering password.

2. Token based authentication mechanisms

The second type of existing authentication mechanisms are token based methods in which user is required to present the information what he/she has in order to be authenticated. The authentication methods such as public key infrastructure, Kerberos and other cryptographic methods come under this category. In all these authentication mechanism, user will be authenticated when secret information such as private keys, tickets, tokens that they possess are presented. According to Huang et al (2015), this token based authentication method is mainly used as part of multifactor authentication instead of using individually as these authentication mechanisms suffer from single point failure. For example working of Kerberos and public key infrastructure requires a centralized authority like trusted third party to issue tickets and private key respectively. Single point failure of this trusted third party greatly affects the working of this authentication mechanism.

3. Biometrics

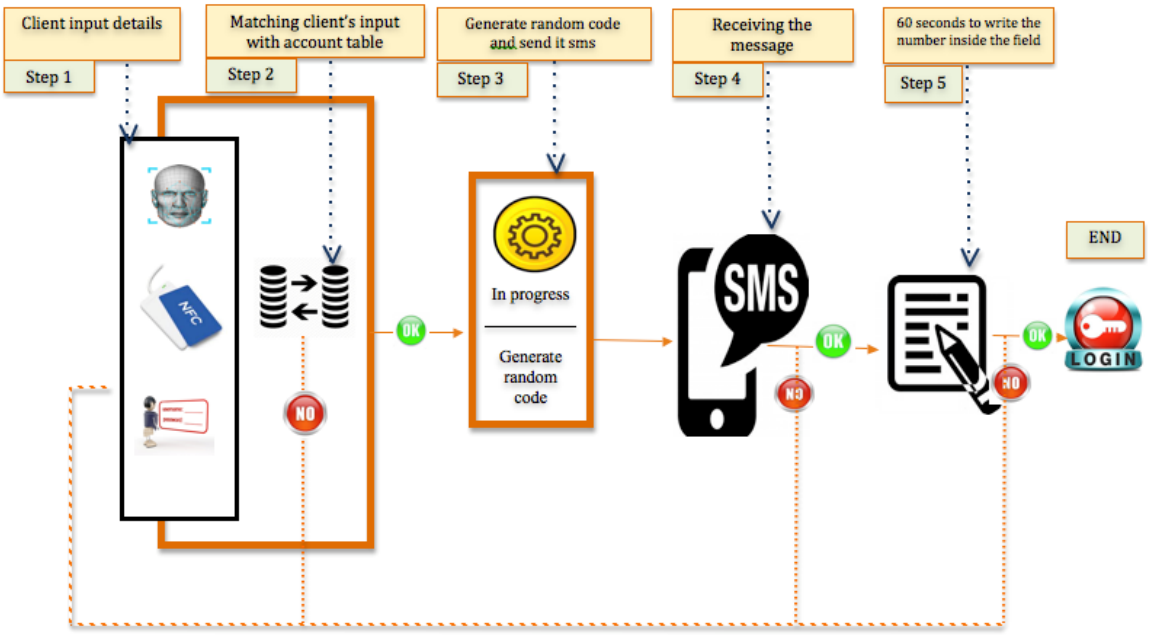
The third type of authentication mechanism that is majorly used in highly secured applications is biometrics. According to Campisi (2013), biometrics is authentication mechanism that involves in authenticating each user based on what the user is. Several unique characteristics of each user such as face features, finger prints, palm prints, iris are used to authenticate each user. Even though the biometric authentication mechanisms are very strong in providing security level, implication of this authentication mechanism is costly and also requires costly resources.

Roy et al (2016) developed an authentication protocol for e-health care systems .this authentication protocol is completely based on biometrics and also employee's cryptographic methods in order to secure the data present in e-health care database. The authentication protocol designed by Roy et al (2016) indicates the use of three types of information namely biometrics, password and the smart card for authentication. In other words this authentication protocol is designed to use all the three types of authentication methods to verify the identity of a user.

2.8 Proposed Multifactor Authentication System

Considering the importance of securing the patient private data stored in e-health care systems and based on the review of the existing authentication mechanism, this project proposes a multifactor authentication system for e-health care applications. This multifactor authentication system intends in authenticating an individual based on their knowledge, biometrics and also based on the thing that they possessed. This made the multifactor authentication adopt five steps to complete the authentication process before allowing an individual to enter into e-health care application. All the five steps that are involved in multifactor authentication are shown in the figure below.

العدد الواحد والثلاثون
تاريخ الإصدار: 2 – آيار – 2021 م
www.ajsp.net
ISSN: 2663-5798



NOTE: I Use AES256 Algorithm

Figure 1: Shows five steps that are involved in multifactor authentication system

Step 1: The first step of multifactor authentication involves in user providing all the details needed for identity verification. These details include the user name and password details of the user, facial recognition of the user and a unique number called NFC code. All these three key details about the user will be acquired in the first step of the multifactor authentication system.

Step 2: This step involves in matching the obtained details with those present in the database. In the process of matching each of the three details will be compared with those present in the database. In order to allow the user go to the next stage of authentication process, there must be match for all the three types of details (facial features, NFC code, user name and password). Mismatch of any one of these three details denies the user to enter into next step of authentication process.

Step 3: This step involves generating a five digit random code . This step is executed only when the identity of the user is successfully verified based on their NFC code, user name and password along with their facial features. This random code will be sent as text message to the mobile number that is given during registration stage.

Step 4: This step involves in verifying whether the random code is received as text message by the user. Any problem in receiving this text message will be sorted out at this stage. The use has another option, which is to receive an email, in case the mobile signals are lost or unavailable. Moreover, where in the case of unavailability in receiving a mobile text or email, the user has the option to use the security question.

Step 5: This step involves in asking the user to write the random number that is received in the text message on the prompted screen of authentication process. Proper match between the entered and generated random number makes the authentication successful and there by allows the user to access the application.

2.9 Summary

In this chapter critical review of existing works in the literature of e-health care security and authentication is presented. Specifically the existing authentication mechanism that were developed for e-health care systems are specified and the security issues, security requirements of e-health care applications are indicated.

Chapter 3: Requirements Specifications

3.1 Overview

This chapter covers the requirement analysis and requirement specification stages of the project. In spite of the current project involving in the development of software based application, requirement specification involves in the specification of functional and non-functional requirements. A detailed list of these functional and non-functional requirements of an authentication system for the e-health care architectures are identified is presented in this chapter.

3.2 Functional Requirements

A functional requirement specifies the high level statements that give details about the system functionality. In other words the functionality requirements provide the requirements regarding the way in which an authentication system implemented for e-health care system must possess. More specifically, taking the high security requirements of e-health care system, the functional requirements are identified for a strong authentication system. List of the functional requirements are tabulated below along with input, output and priority levels.

Req _Number	Description	Input	Output	Priority
Req_1	E-healthcare system must allow only authorized users to access the application	Users entering required credentials before login.	Entered credentials must be validated and based on the result; user has to be allowed access.	High
Req_2	The authentication system of E-healthcare must be using either two or multi-factor	Users of e-health care system must be authenticated using more than one password.	Any number of passwords that are entered by the user must be validated before allowing access.	High
Req_3	The authentication system of E-healthcare should allow new users to be registered	New users must access the registration page to register their details.	Registration details must be validated to confirm user registration.	High
Req_4	To ensure more security, the authentication system must use dynamic passwords rather than all static passwords	Authentication system should generate one time passwords dynamically	The user can be considered as authorized user only when the dynamically generated password is appropriate.	high
Req_5	The authentication system should adopt more than	User of e-health care system should input	All the entered authentication details must be validated before allowing access.	High

	one stage of user authentication	authentication details in more than one stage.		
Req_6	The authentication system must combine biometric, password and dynamic passwords for authenticating users	User enters three types of passwords during the login stage.	All the three types of passwords are authenticated before allowing the user to enter the application.	High
Req_7	The E-healthcare system must have a database to store all the password details	All the passwords used in different stages are collected and stored in database.	During validation these stored passwords are used for user authentication.	High
Req_8	In using biometrics, the e-healthcare authentication system must collect user biometrics accurately	User inputs the required biometric details.	These input details are collected properly and stored in the database for future validation.	High
Req_9	In using dynamic password for authentication, the system must send the dynamic password to mobile or email	During authentication, the user enters the dynamic password that is send to the mobile phone	Validation of the entered password is done before allowing user to enter the next stage	High
Req_10	In using multi-factor authentication, user must be given access only when all the factors are met	User enters all the required credentials in all the stages of authentication.	All the entered user credentials are validated and are ensured to be appropriate before allowing user to access the application.	High

3.3 Non-Functional Requirements

The non-functional requirement is another type of the system requirement that specifies the criterion through which system operation can be judged. These non-functional requirements differ from the functional requirements in the way that these requirements do not focus on the specific behaviour or specific functions of the system. According to Ameller et al (2013), some of the non-functional requirements are reliability, usability, security, maintainability, scalability and performance. These requirements act as restrictions or the constraints on the design of the system. In the context of developing an authentication system for e-healthcare system, following are the non-functional requirements that must be satisfied.

1. **User-friendliness**

In the case of web applications, user-friendliness specifies the concept of the usability, which specifies the easiness in using the application. The usability of the multi-factor authentication for e-healthcare system is assessed based on five goals such as memorability, learnability, satisfaction, errors and the efficiency level.

a. **Learnability**: The new users of multi-factor authentication should be easily accomplishing the activities when encountered first time and must be capable of learning the activities involved in this authentication process quickly.

b. **Efficiency**: Users of multi-factor authentication system of e-healthcare system must be able to perform the authentication activities quickly after being learnt.
c. **Memorability**: The steps involved in multi-factor authentication of e-healthcare system must be able to be performing of the login process correctly even visiting the application after a long time.
d. **Error handling**: The multi-factor authentication system must be able to handle and recover the errors effectively by taking the severity level into account.

2. Accessible

Accessibility indicates the extent by which a system can be used by several people. Based on the views of Hamlet et al (2014), the technical accessibility of the multi-factor authentication system is determined in terms of operable, perceivable and understandable.

Operable: Navigation commands used in the multi-factor authentication system and the commands on user-interface must be operable easily by the users.

Perceivable: The presentation of the information and components on the user interface of multi-factor authentication system must be easily perceived by the users.

Understandable: The components, steps and the information placed in the multi-factor authentication system must be able to be easily understood to all the application users.

3. Security

The third important non-functional requirement that must be satisfied by multi-factor authentication system is the security aspect. The authentication system must provide high levels of security by allowing only the authorised users to enter the application. In other words, the multi-factor authentication system must be able to satisfy the five security principles such as confidentiality, accountability, integrity and the availability.

3.4 Summary

In this requirements specifications chapter, the functional and non-functional requirements of the multi-factor authentication system for e-healthcare system are identified and specified. The functional requirements are specified in terms of the way in which the authentication system functions or behaves. The constraints on the functionality of this authentication system are specified as non-functional requirements in terms of user-friendliness, accessibility and security in this chapter.

Chapter 4: System Design

4.1 Overview

The main purpose of this chapter is to detail the design of the multi stage authentication system that is carried out for e-health care architectures. Taking the crucial role of system design in the software application development projects like the current one, in this chapter the architecture of the multi factor authentication system is provided along with the design diagrams. The design diagrams which are included in this chapter are activity diagram and other database diagrams such as entity relationship diagrams are presented.

4.2 System Architecture of multifactor authentication system

The system architecture of multi factor authentication system details the high level design diagram of the complete system. In this high level design diagram the various components involved in multifactor authentication system along with the way in which these components work are given. The detailed system architecture for the multifactor authentication system is given below.

As shown above the user of e-health care application either new or old will be prompted towards the login page. If the user is an existing user the user is required to follow three authentication methods as sown in the above figure. These three authentication methods are face recognition, generation of NFC code and static user password. Each user is allowed to undergo all the three stages of authentication process in which facial recognition is done first followed by entering a dynamically generated password and then entering a static username and password. Verifications of the passwords that are entered by the user in the three stages of the authentication are done using the details stored in the database. From the architecture of multifactor authentication that is shown above it is evident that a user will be allowed to access the application only when all the entered passwords are accurate. The database is also indicated in this architecture where all the required authentication details are stored. A valid and authenticated user is then allowed to access the e-health care application in which the user can access privilege screen, email screen, patient screen and search for patient screen.

4.3 Flow of the System

The design of multi-factor authentication system that is proposed for e-healthcare applications is shown in the below figure. This design shows the actual working procedure of multi-factor authentication system.

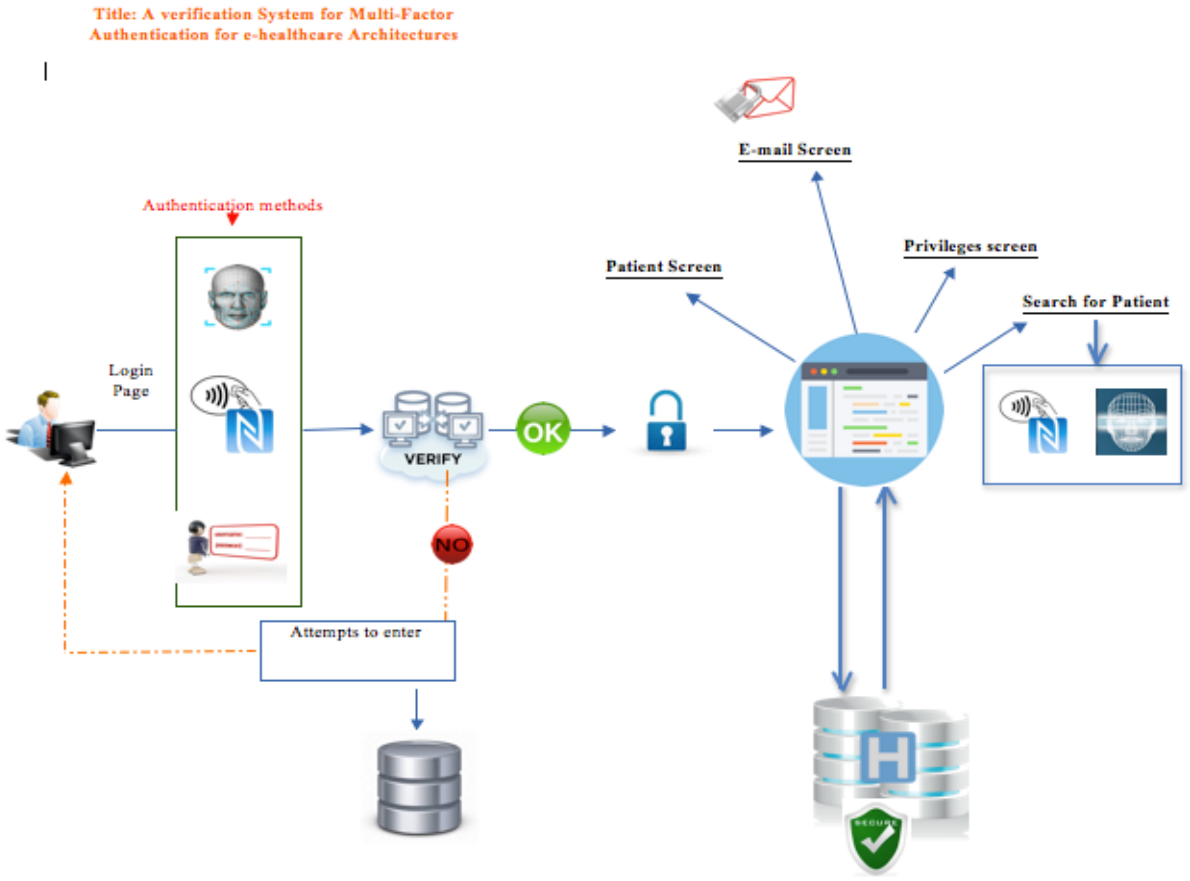


Figure 1 the actual working procedure of multi-factor authentication system

As shown in the above design, the login page prompts for authenticating the user using three methods namely facial recognition, NFC code, user name and password. All these entered details are verified and only then the user will be allowed to access the database. An authorized user can access the patient screen appointment screen, email screen, treatment free screen and also can search for the patient details. In this process, the authorised user can add or modify the patient details only after verifying his/her identify using all the three authentication methods.

4.4 ER Diagram for Privilege Screen

As the working of multi factor authentication system for e-health care architecture requires huge data, a separate database is designed for this system. The working of this database is shown in the form of entity relationship diagrams. The entity relationship diagram for privileged screen of e-health care application is shown below.

ISSN: 2663-5798

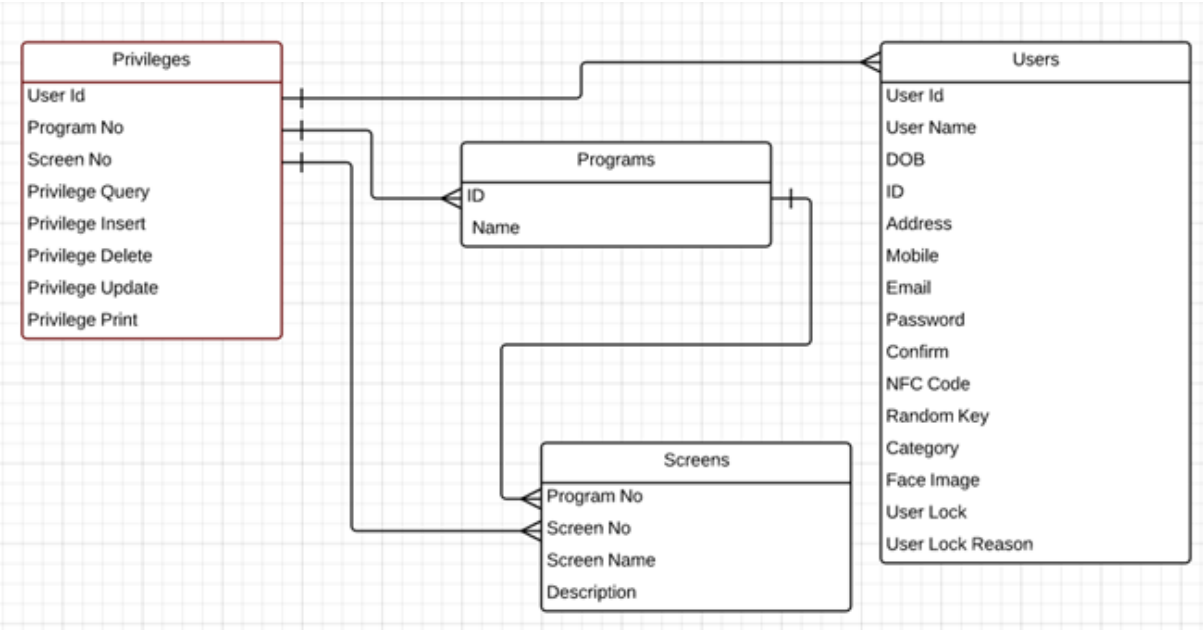


Figure 2 explains the relation between user's schedules and validities tables.

As shown above the ER diagram consists of four main tables namely privileges, users, screens and programs. The relationship that exists among all these four database tables is given in the above entity relational ship diagram. For example users and privilege and user table consist of one-to-many relationship as each privilege can be assigned to many users. In the same way privilege and screens table consists of one-to-many relationship as each privilege can be assigned for more than one screen. This ER diagram shows the way in which each user is assigned with a privilege and based on this privilege the user will be allowed to access the different screens present in e-health care system. For example patient will be provided with only query and insert privileges but will not be provided privileges for updating and deleting the data present in the database. In this way based on role of each user privileges are assigned and then the screens that can be accessed are specified.

4.5 ER diagram of Medical Screen

The entity relationship diagram for the medical screen is shown in the below figure. In this ER diagram the tables that are involved in the proper working of medical screen present in the e-health care system are given.

العدد الواحد والثلاثون
تاريخ الإصدار: 2 – آيار – 2021 م
www.ajsp.net
ISSN: 2663-5798

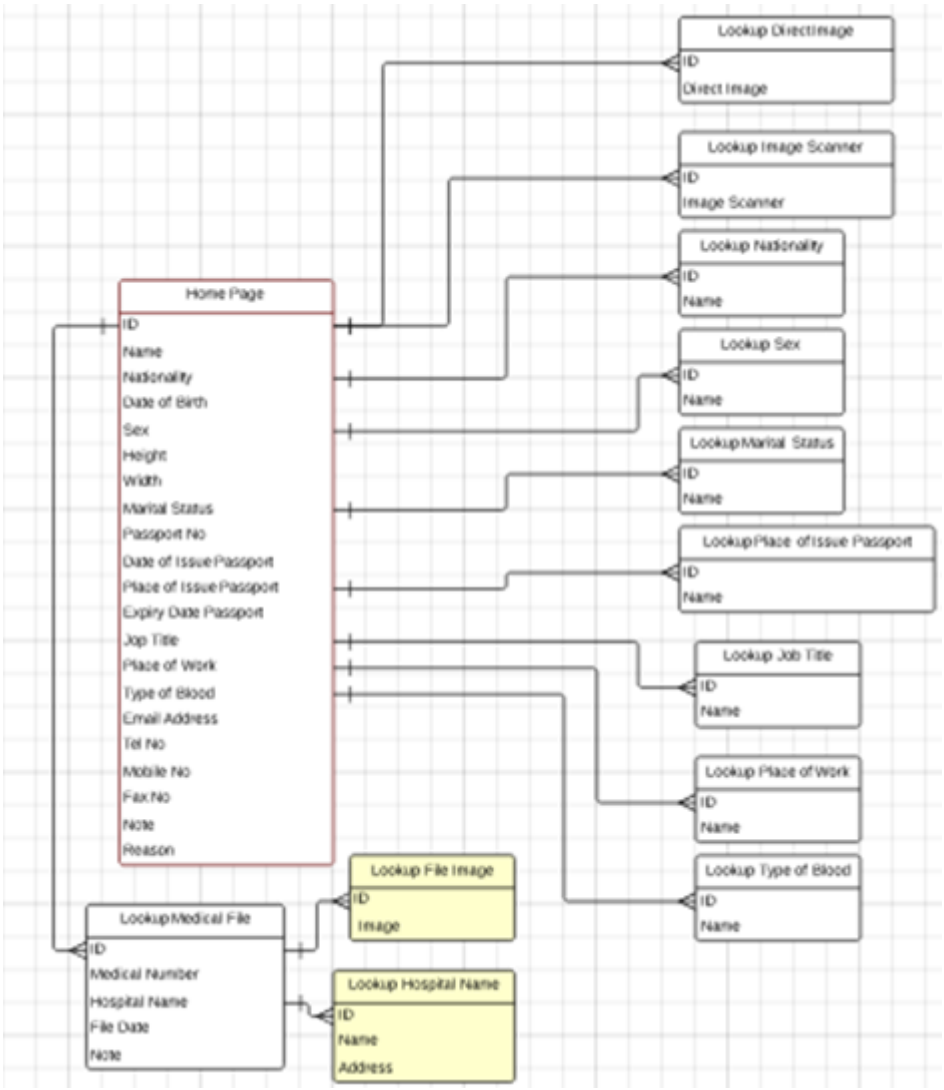


Figure 3 explains the related relation in the main schedule, fields and schedule names for medical file screen

In this ER diagram the relation existing between main schedule and the field names of medical screen is shown. The main table which is patient medical file is linked with the home page of the e-health care application based on the entity relations that are shown in the figure. In other words the relation between home page and the other lookup files related to postal name, medical files, job title and other personal details of the patients registered in this e-health care application are clearly shown in the above ER diagram.

ISSN: 2663-5798

4.6ER diagram of email screen

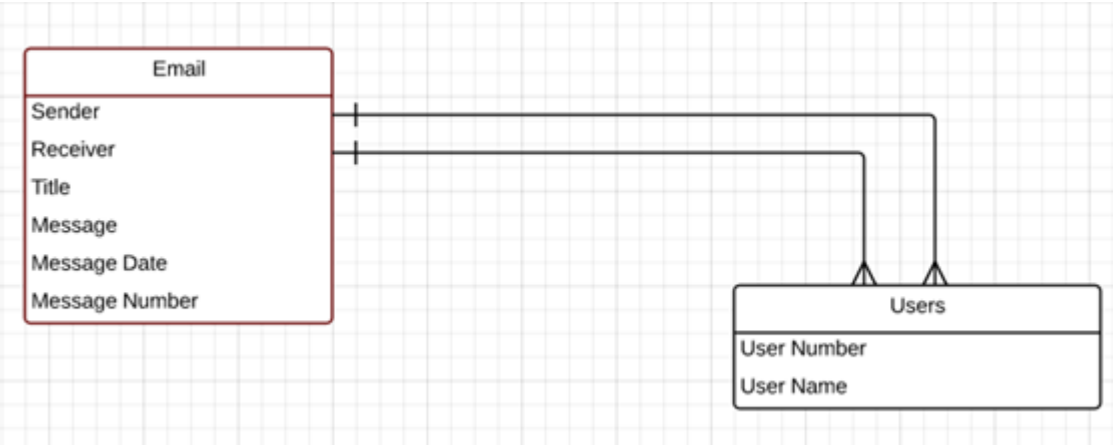


Figure 4 explains the special table relations with E-mail

The above entity diagram shows the tables that are involved for the proper working of email screen present in e-health care system along with the relationships existing among these tables. As shown above, there exist two classes in this ER diagram which are email and the users. There exists a one-to-many relationship between email table and the users table, which indicates that the contents of email can be related to more than one user of this e-health care application. This relation between email and the users table greatly help in proper working of the internal email system of e-health care application.

4.7Activity Diagram

Besides the ER diagrams, the design of multi factor authentication is also presented using UML diagrams such as activity diagram. The activity diagram of electronic prescription system details the list of all the elements that are present in an e-health care system.

ISSN: 2663-5798

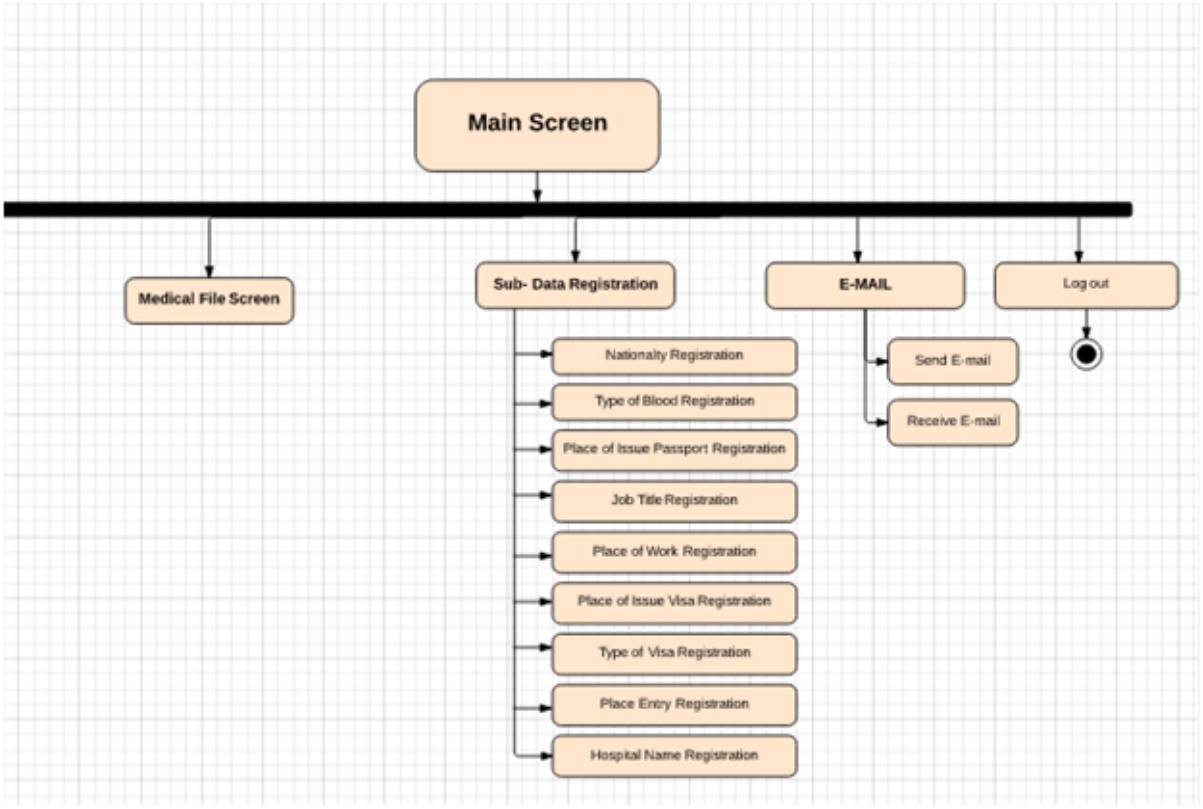


Figure 5 explains all the main list elements for the system

As indicated in the above activity diagram, the main screen of e-health care system consists of several sub screens such as medical file screen, sub data registration screen, email screen and the logout screen. Among all these sub screens, the email screen in turn consists of two options namely sending email and receiving email. The sub data registration screen consists of several options such as nationality registration, blood registration, passport registration, job title registration and so on. In this way for each patient the details of all these aspects are registered into this application in order to properly authenticate the valid users when accessing the application.

4.8 Database and Design Stage

We need to analysis, the related project database relations and scheme drawing at beginning of any project for facilitating determination of schedule names and data field to enable us specifying problems and weakness points that may issue from soundly and speedy database.

4.9 Summary

The design chapter of this project has given details about the design of multifactor authentication system and e-health care system. This design is presented in terms of providing architecture for multi-factor authentication system, entity relationship diagrams for the screens present in e-health care system and activity diagram.

ISSN: 2663-5798

Chapter 5: System Implementation

5.1 Overview

This chapter covers the implementation details of multifactor authentication system and also the e-health care system. The implementation details are provided in terms of the software packages that are used for developing multifactor authentication for e-health care system and the screen shots of developed application. All the provided screen shots are given with detailed explanation regarding the way in which implemented system works.

5.2 Implementation Details

In this project the development of multifactor authentication system for an e-learning system is done using the tools like a camera, ACR122 NFC device, Oracle Forms, Oracle 10g database and java programming language. Clear details of all these tools used for system implementation are provided in this section.

Java is one of the preeminent languages of Internet as it has completely revolutionized the way in which programming is carried out. Java platform that supports in the use of Java programming language consists of two elements namely Java Virtual Machine (JVM) and Java Application Program Interfaces (APIs). The main reason behind the selection of Java programming languages to develop multi-factor authentication system for e-healthcare system is the ability of Java in enhancing the security and portability feature as output of Java compiler does not consists of executable code but it is in the form of byte code. The byte code of Java is optimised collection of instructions that are being designed for execution by the run-time system of Java called as Java Virtual Machine (JVM). This property of Java programming code to be executed and interpreted by JVM makes Java platform independent as any operating system installed with JVM will be able to interpret and execute the java programming language code. According to Liang (2013), besides platform independency, Java also provides several merits such as portability, security, inheritance, polymorphism, Java swings and applets. All these merits of Java programming language, especially in designing highly secured applications have resulted in the selection of this programming language for the current implementation process.

5.3 Implemented system screenshots

In this section, the full explanation to all the screens present in the implemented multi-factor authentication based e-healthcare system is given. The main purpose of each screen and the different fields that are involved in each screen are detailed.

العدد الواحد والثلاثون
تاريخ الإصدار: 2 – آيار – 2021 م
www.ajsp.net
ISSN: 2663-5798

New User Registration

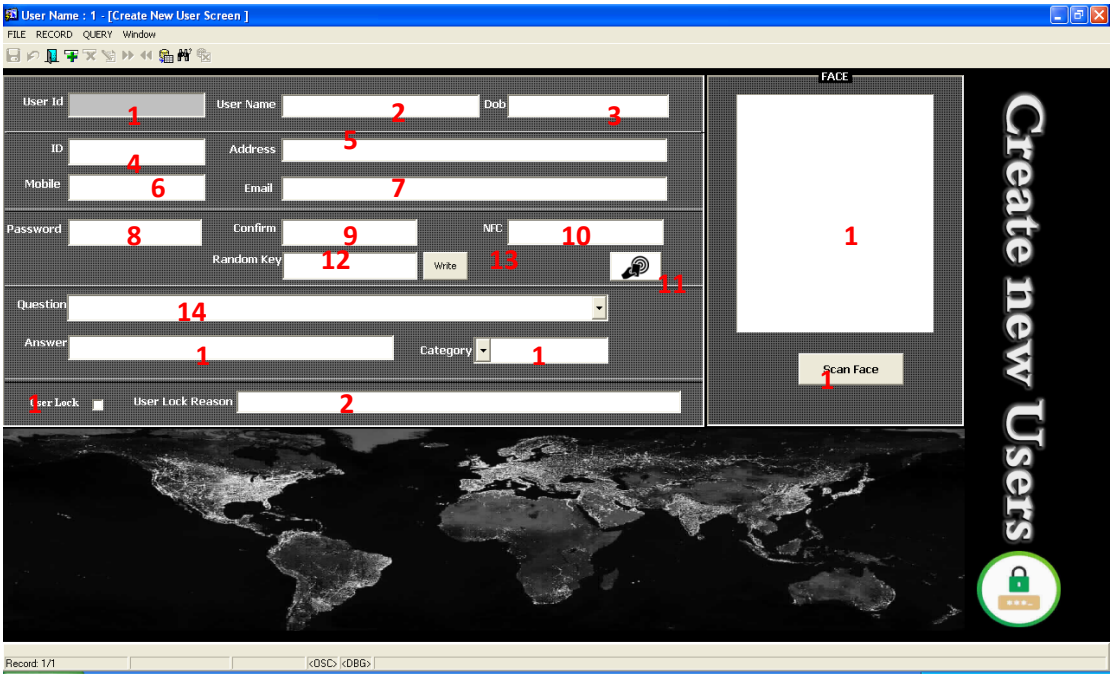


Figure 6 New User Creating Screen

Any new user of e-healthcare system undergoes the registration stage using the screen shown above. In this screen, the new user is required to enter a wide range of information such as user ID, user name, telephone number, email address, face recognition and so on. Each of the entered details is stored in the databases that are later used in the validation stage to authenticate each user. Clear details of each field that is included in the above registration stage is given below,

1- User ID: Every user has a related digit issued automatically by the system after success of data saving process; this digit doesn't be subject to repeating as it is considered a main key of the user.
2- User Name **:**This field is used for user name registration, it is very important in registration process in entry screen and it is not subject to repeat.
3- DOB: This field is used for registration of user date of birth.
4- ID: This field is used for the registration of user image, where the image is used for the identification of user face.
5- Address: This field is used for registration of work or residence address of the system user.
6- Mobile: This field is used for the registration of system user mobile phone, it is very important in verification process as the system sends verification code to the registered mobile phone in this field.
7- E-mail: This field is used for registration of the system user E-mail.
8- Password: This field is used for the registration of system user special password.

Password encryption process: In the implemented system, the user passwords are stored in the database in encrypted format. Advanced Encryption Standard (AES256) is done to encrypt the passwords before storing them in the database. A key size of 256 is used in this implementation for the encryption process, which is given in Figure 7.

9- Confirm this field is used for password repeating, there will be no transition to the next field unless congruency of password is established.

ISSN: 2663-5798

10- NFC: This field is used for registration of the bank card or smart card that has been read by card reading device. This NFC is un-repeated digit and it is specialized for reading either the bank card or smart card.
11- Read: This button recalls the existed digit inside the card and set it at field digit 1
12- Random Key: This field displays a random text which is issued by the system and it is written on the pasted or smart card beside NEC. This random key offers high protection to the system as the user cannot enter the system without obtaining this random key.
13- Write: This button produces a random digit which is issued by the system, it is located on field 12, and the random digit should be put on the posted or smart card.
14- Question: User chooses a security question, which they can answer, in case there is not mobile texts or emails communication. Once the question is answered corrected (as matched with the database) the user can login.
15- Answer: the user inputs their answer to the security question (as in point 14, above), in order to gain access to the system. The inputted text are to be encrypted using the encryption of AES256 type.
16- Category: In this field user category is specified, whether the user is administrator or user.
17- Face Image: When the user requires validating his/her identity using their face image then it will be displayed in the rectangle field that is named as 15. This is the stage where the face recognition system is used.
18- Scan Face: This button is used for connecting to the camera for collecting user image and then putting it on its position which is marked as 'digit 14' in the above scree.
19- User Lock: This option is used in case of system administrator desire to lock accessing the system. This option is automatically ticked when a user is not able to enter the valid details successfully in three attempts.
20- User Lock Reason**:** In this field user lock reason is written.

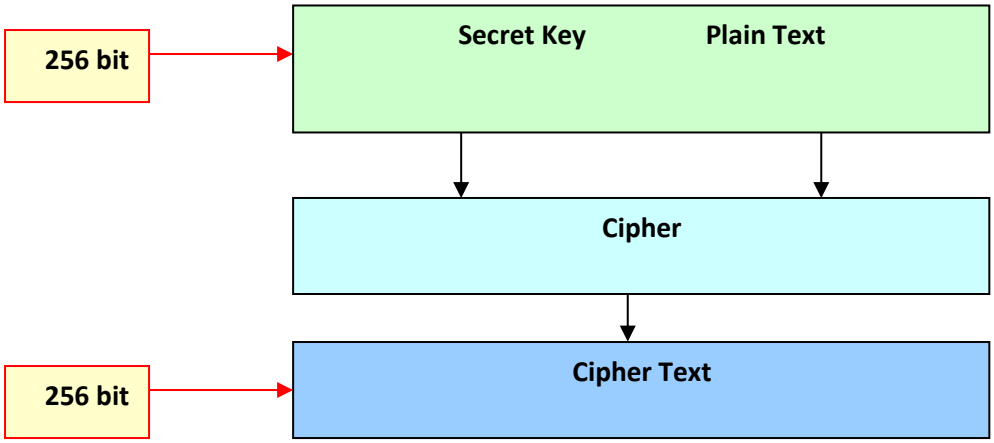


Figure 7 explains password encryption mechanism

As shown in the above figure, the plain text and secret key of 256 bits is taken as input for the encryption process. Using this secret key and **AES256** algorithm, the encryption is carried out for the user entered passwords and then stored in the database.

ISSN: 2663-5798

Process of user registration

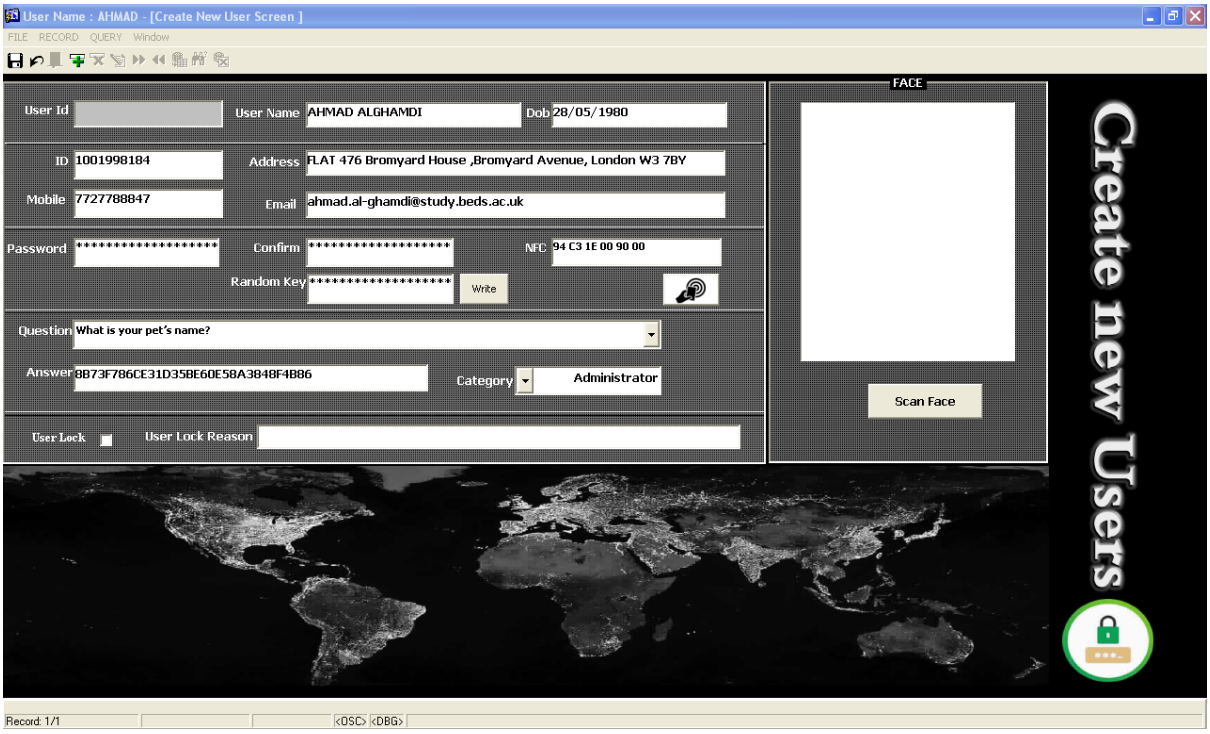
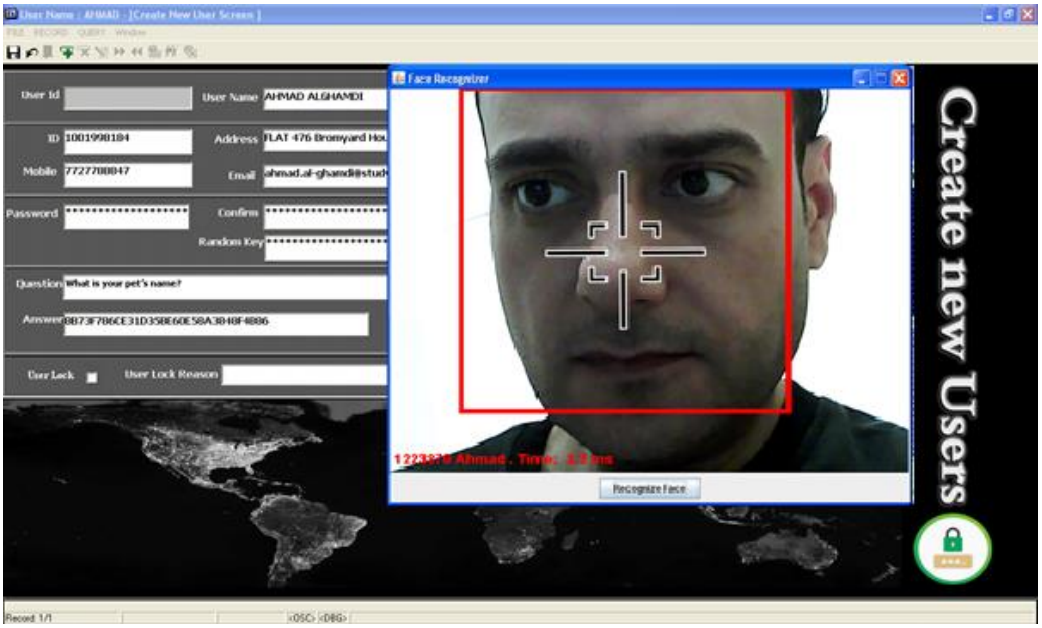


Figure 8 displays data registration process

All the fields in the registration page are entered by the new user based on the requirements. As shown above, the content in the password and content fields is not shown properly and the random key is displayed in encrypted format. This way of hiding both these details from displaying in plain text format avoids shoulder surfing attack.

Face recognition in User registration page



ISSN: 2663-5798

Figure 9 explains image taking process

The above screen shows taking of the user image by clicking on "image taking" button in the registration page. The red rectangle that appeared is used for specifying the image taking boundaries and it will be stored in database for identification of the user image.

Confirmation of user registration

Figure 10 displays ending of registration process

The above screen displays the end of new user registration process. The use of AES 256 algorithm has resulted in displaying the content in 'password', 'content' and 'random key' in encrypted format. The password 'password 123' is encrypted into 32 characters, which makes password complex and unpredictable. When the ending of data process saving is done, the user special digit is appeared in the system that cannot be modified.

العدد الواحد والثلاثون
تاريخ الإصدار: 2 – آيار – 2021 م
www.ajsp.net
ISSN: 2663-5798

Privileges Grant Screen

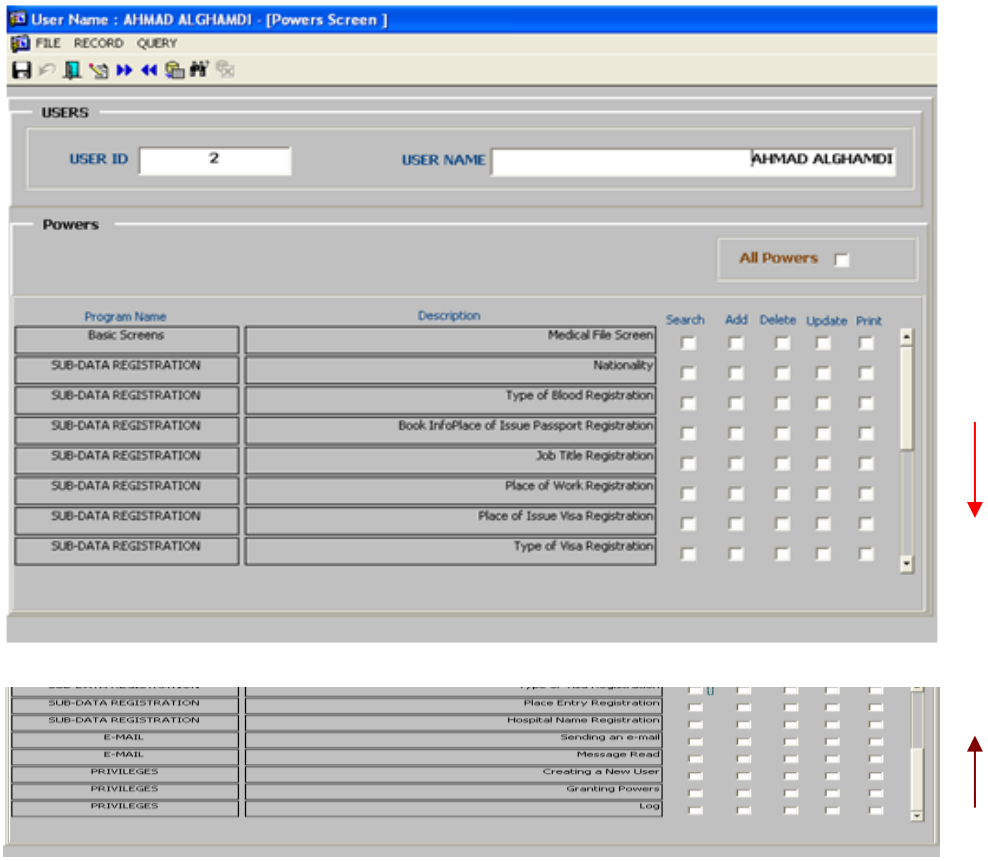


Figure 11 shows validities grant screen for users

The system allows new user to grant the privileges when the new user registration is completed successfully. This screen is involved in determining the user access permissions and in determining the validities such as "save – amendment – delete – search – print" as shown in above screen.

Privilege granted

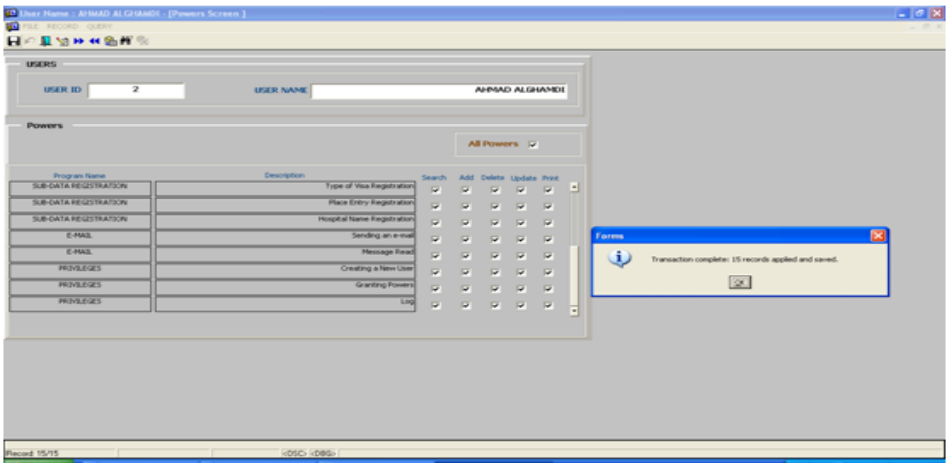


Figure 12 Validities Grant Process Explanation

The extra dialogue box displayed in the above screen shows the confirmation that the user "AHMAD ALGHAMDI" has been granted all validities of accessing to the system.

Login Screen

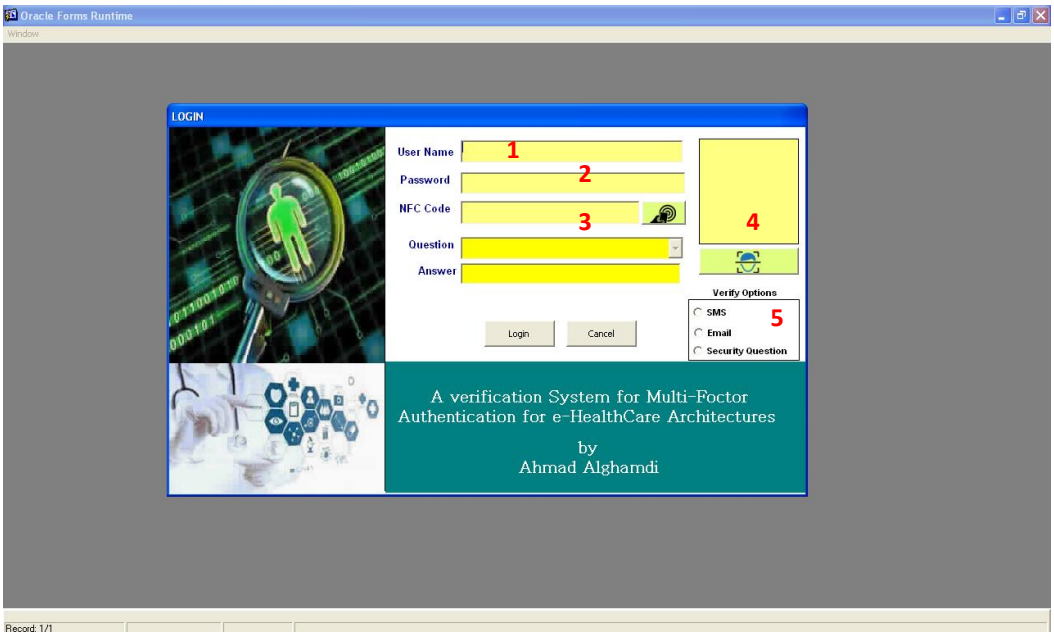


Figure 13 Login Screen

After the completion of user registration, login stage of multi-factor authentication system is entered. As indicated above, the login screen prompts for four key fields to be entered by the user. Any user will be granted validities to enter the next stage in the screen when all the details in the above screen are entered correctly.

1- **User Name**: User name will be entered in this box.
2- **Password**: Password will be entered in this box.
3- **NFC Code**: This code will be recalled through the button that is located beside the field after assurance of connecting the smart card reader device with the PC. Every user of this system has a special entry card which includes the card basic digit and random digit that are entered by the user in registration phase.
4- **Scan Face:** The button under the box marked '4' is used to connected with the camera. This camera will take the image and it puts the specified position and prepares it for conforming process of user identity.
5- **Verify options:** For this multi-factor authentication, verification system is also developed in this project as shown in the above screen. There exist three options for verification for verification such as:
    1- Verification by sending SMS message which contains verification code.
    2- Verification by E-mail which contains verification code.
    3- Verification by secret question.

Based on the availability of access to email or mobile, the user can chose either of the verification options that are presented in the above screen.

ISSN: 2663-5798

Steps in Facial recognition

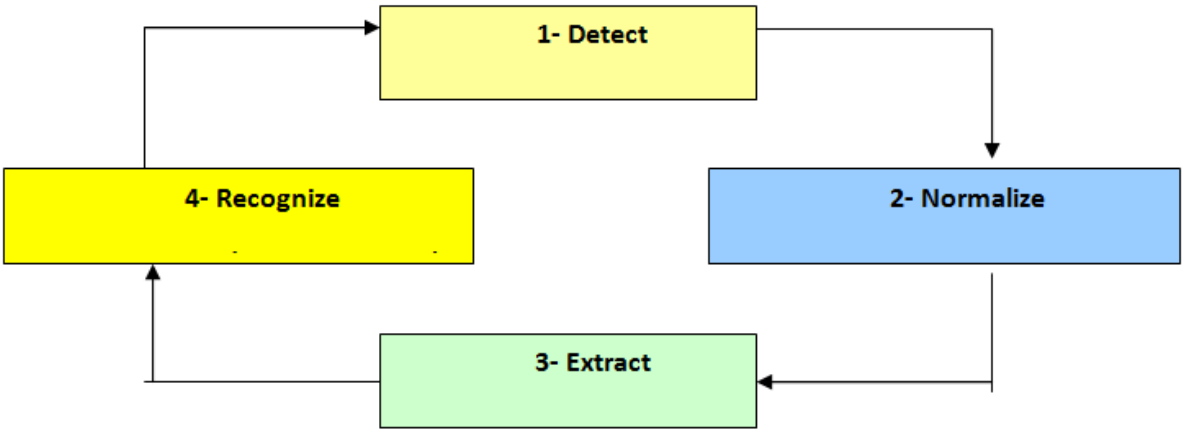


Figure 14 Steps in the facial recognition process

From the login screen of multi-factor authentication system it is evident that facial recognition is used as one of the techniques to authenticate the users. The steps that are included in the implementation of facial recognition system are detailed above as detect, normalize, extract and recognize. Initially after detecting the face, it will be normalised and then facial features are extracted from the face in order for the recognition process.

Login mode Explanation

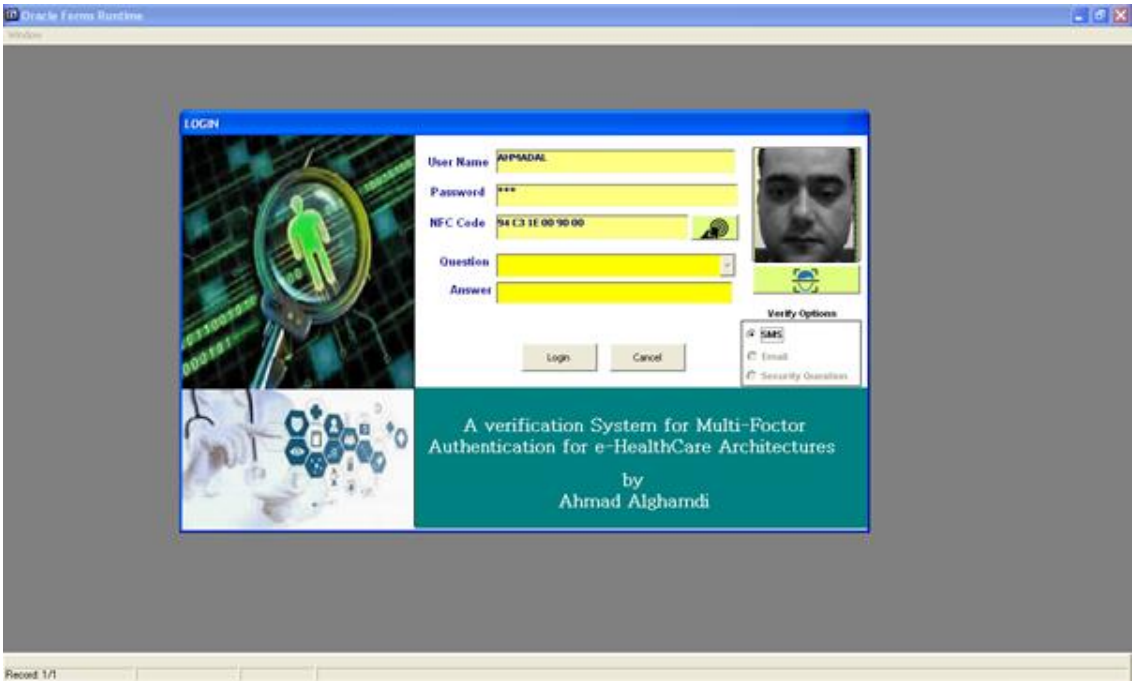


Figure 15 Information Preparation for system entry beginning

As shown in the above screen, all the required fields are entered by the user and 'Login' button is pressed. After pressing the 'login' button, the system validates the entered details before allowing the user to access the system. When all the details entered are correct, the system opens a box for entering confirmation code, which is been automatically sent by the system to registered mobile number. The user cannot enter any information unless this confirmation code is displayed within 60 seconds; countdown of second will begin as a confirmation time from the time code is being sent. In case of the message is delayed by the service provider or any other reason, you can repeat the countdown of 60 seconds again, it is an estimated time to send the message amongst this time.

Countdown started

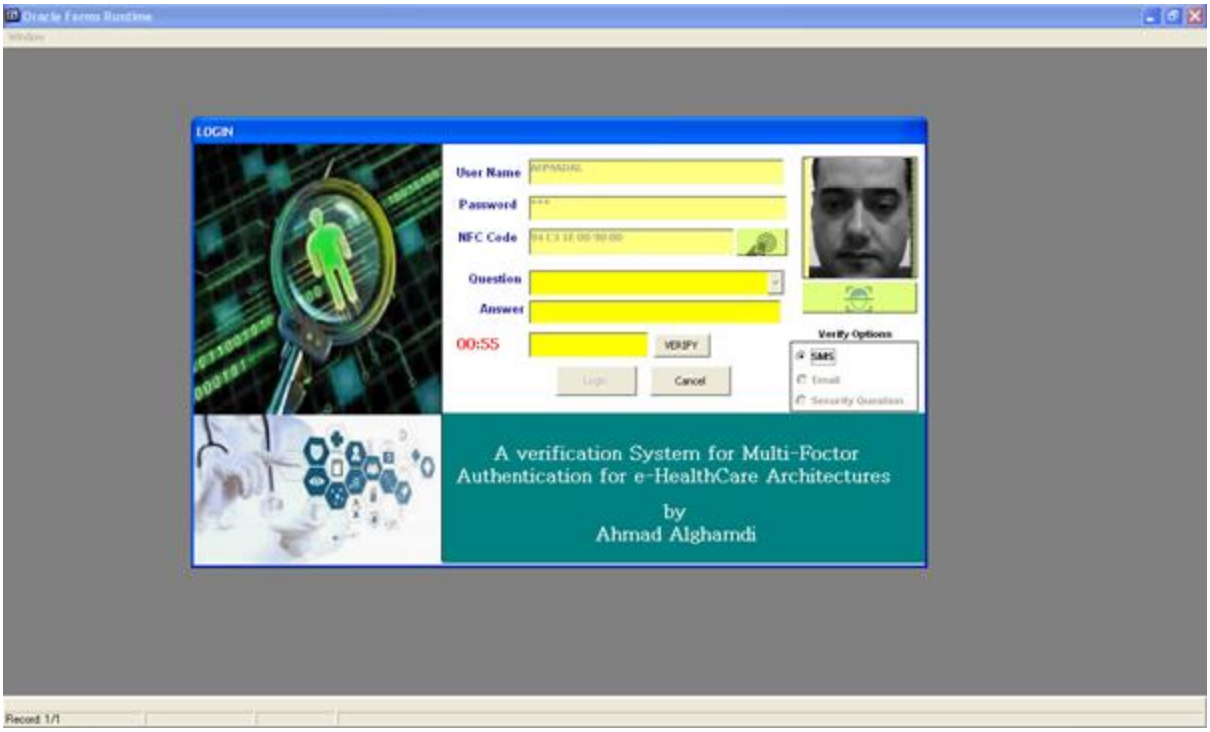


Figure 16 Countdown started

As shown in the above screen, all the fields have become inactive and the timer has started to enter the code that is sent to the mobile device.

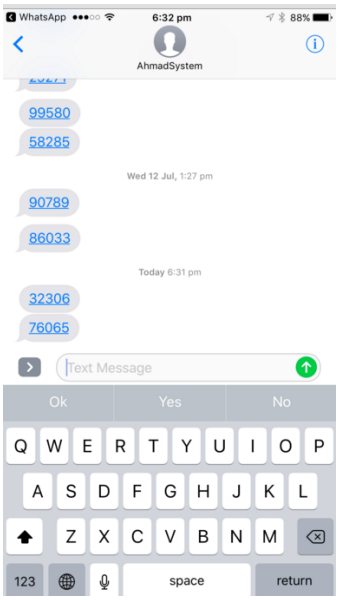


Figure 17 shows the mobile message that sent by the system.

The above screen shows the messages received by the registered mobile number in the multi-factor authentication system. As shown above, each time a different 5 digit number is sent from "AhmadSystem".

Entering Random number

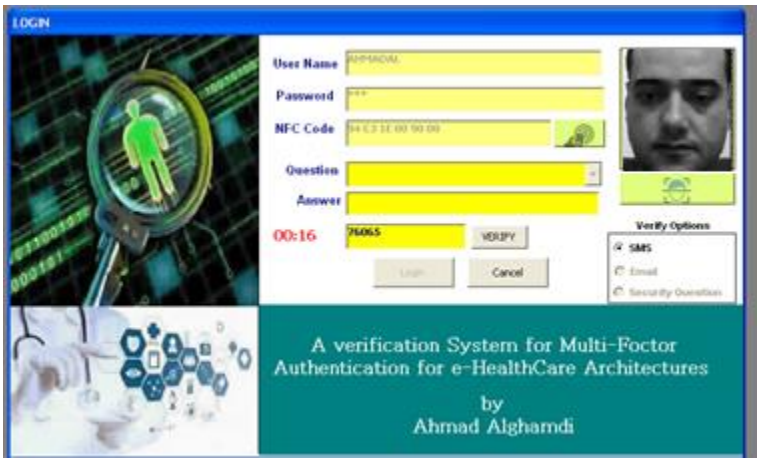


Figure 18 shows the entering process of the sender code to the user

The above screen shows the entering process of the random code sent by the system to the registered mobile number. This is the final confirmation process and after that the user enters the main screen, taking into account that all attempts to enter either successful or failed are recorded in a database with IP device digit as well as the date, time and image.

ISSN: 2663-5798

Registration Logs

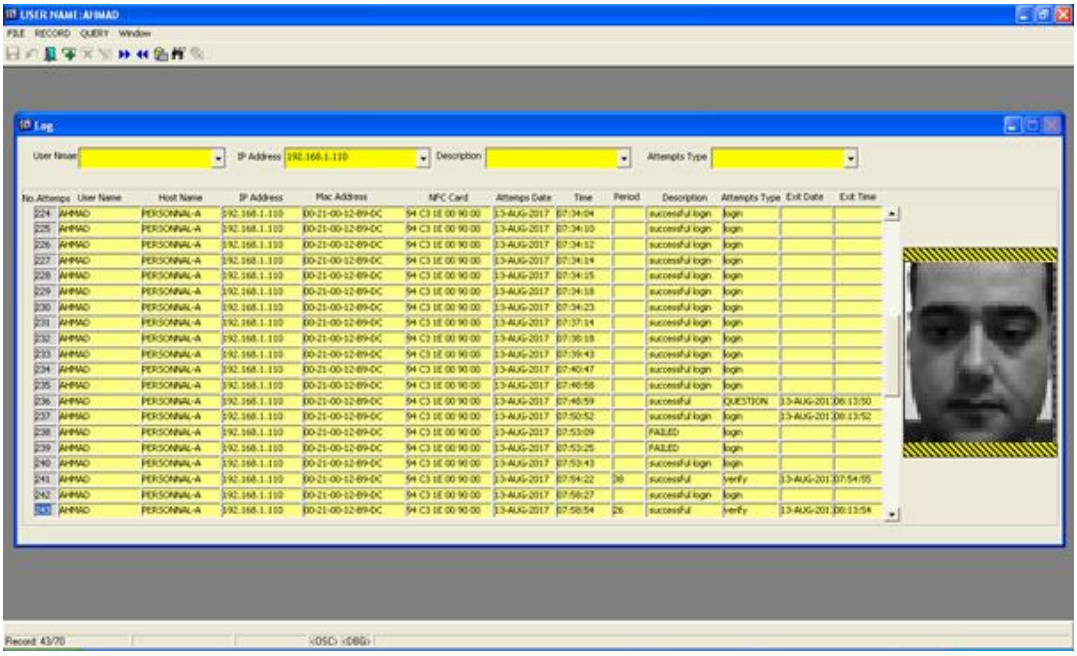


Figure 19 Screen Registration of All Attempts to enter the system

The above screen shows the log in which all the registration attempts made the users to enter the system whether they are successful or failed are displayed. The details of the login attempts that are stored in the log are related username, device, address of the device, smart card digit, MAC Address, date of attempts, Period, type and description of the attempt, entry time to the system, exit time from the system, the used image and the number of attempts a valid user tried to enter the system. In case of exceeding the attempts to login more than 3 times on valid user name, the account of the user is suspend for a security action until the user return to the system administrator.

العدد الواحد والثلاثون
تاريخ الإصدار: 2 – آيار – 2021 م
www.ajsp.net
ISSN: 2663-5798

Main Screen

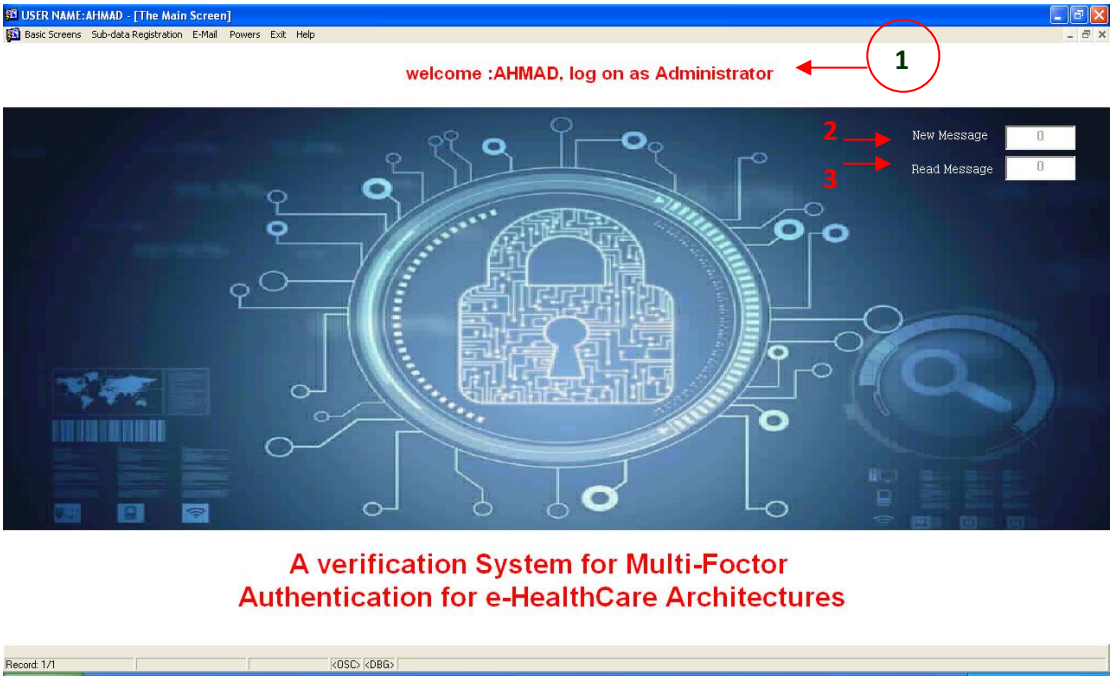


Figure 20 main screen of e-healthcare system

The system main screen of e-healthcare system is shown above. From the appearance of welcoming screen, it is found that the user name and validity level are indicated as shown above. "New Messages" specifies new coming E-mail messages that have been sent by any other user of the system and "Read Messages" specifies the message that has been read by the user.

Opening medical file screen

Figure 21 Main Screens and Option from Menu to the Patient Medical File

From the 'basic screens' option present in the menu bar, the user will be able to view the other important file screens. The 'Medical File Screen' option can be viewed by the user by selecting it as shown above.

Medical file screen

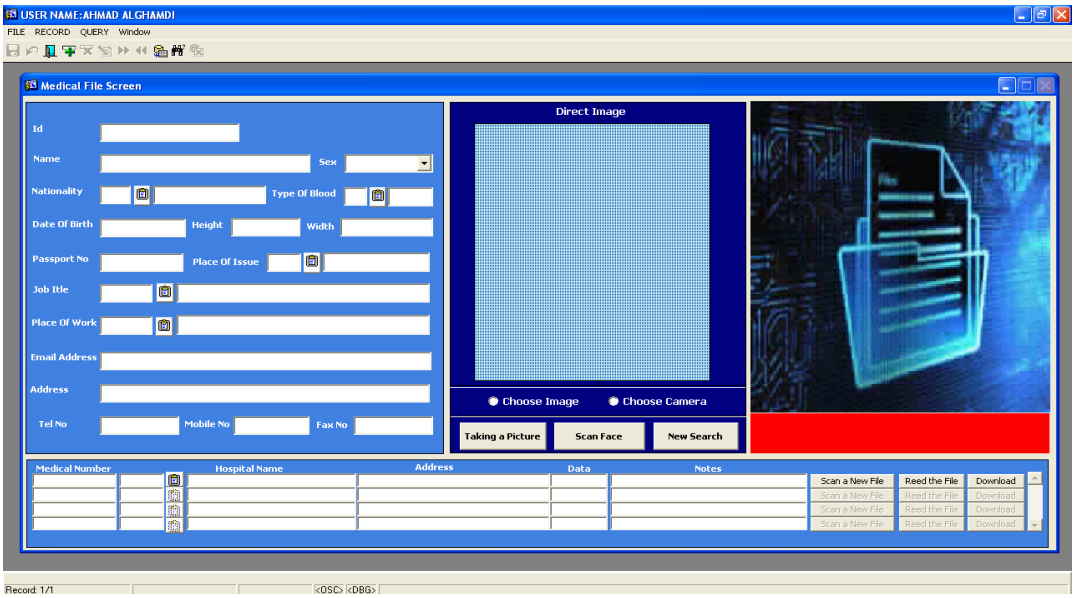


Figure 22 Patients Medical File Screen

The medical file screen shown above is completely about patient medical file, whereas it contains some information about the patient such as name, age, blood type, weight, length Id No., Passport No., occupation, work place, house address, E-mail, and telephones digits, patient image. This screen is used for full registration of the patient, registration of the medical digit that are acquaint to the patient medical electronic file within limits of determined system user validity. This is done for the sake of ensuring confidentiality of the patient's private information.

Patient data registration

Figure 23 shows data registration process and patient data displaying

The above screen explains the patient data registration process in which all the required details of the patients are entered. This screen is designed to have "scanner" option through "scanning patient file icon" shown in red colour tab. In this screen, there is also a feature of downloading the file in case of desire to send electronic file of the patient to another hospital, this service enable the other hospital to follow up patient file from the admission to the hospital to the moment of sending his file.

Patient electronic file

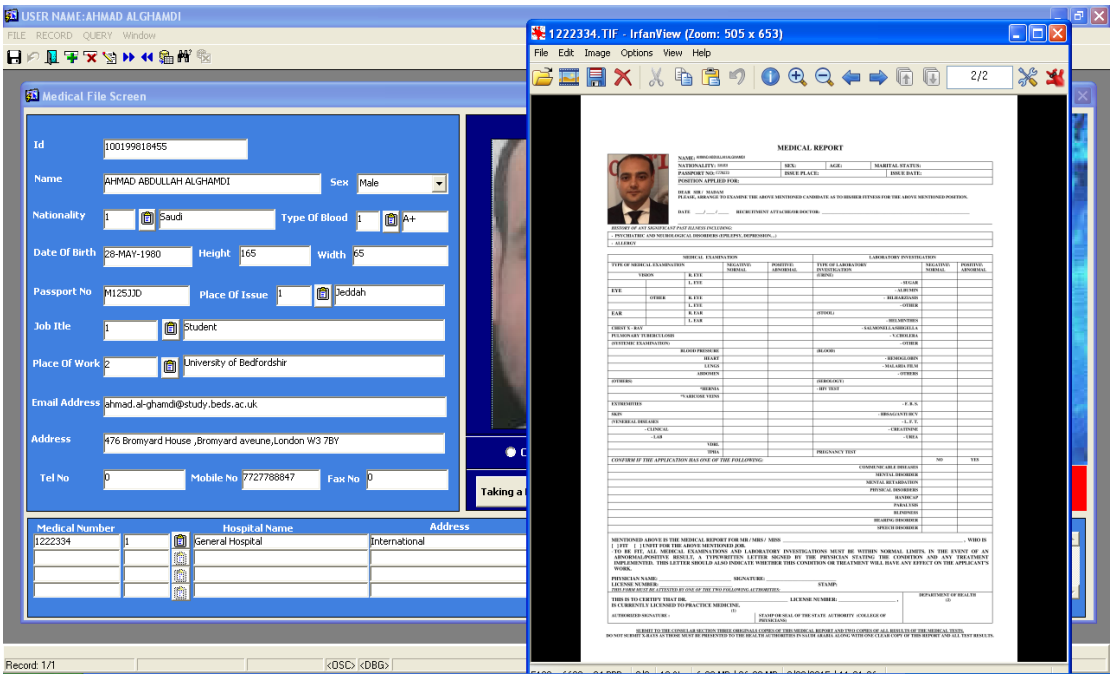


Figure 24 electronic file of the patient

The electronic file of the patient that can be downloaded from this e-healthcare system is shown separately in the above screen.

ISSN: 2663-5798

Figure 25 digital data registration list (LOOKUP)

In this e-healthcare system, some digital data can be registered through the 'Sub-data Registration' process as shown above. This information includes nationality, blood registration, place of work, place of issue, type of visa and others as shown above.

Entering Nationality

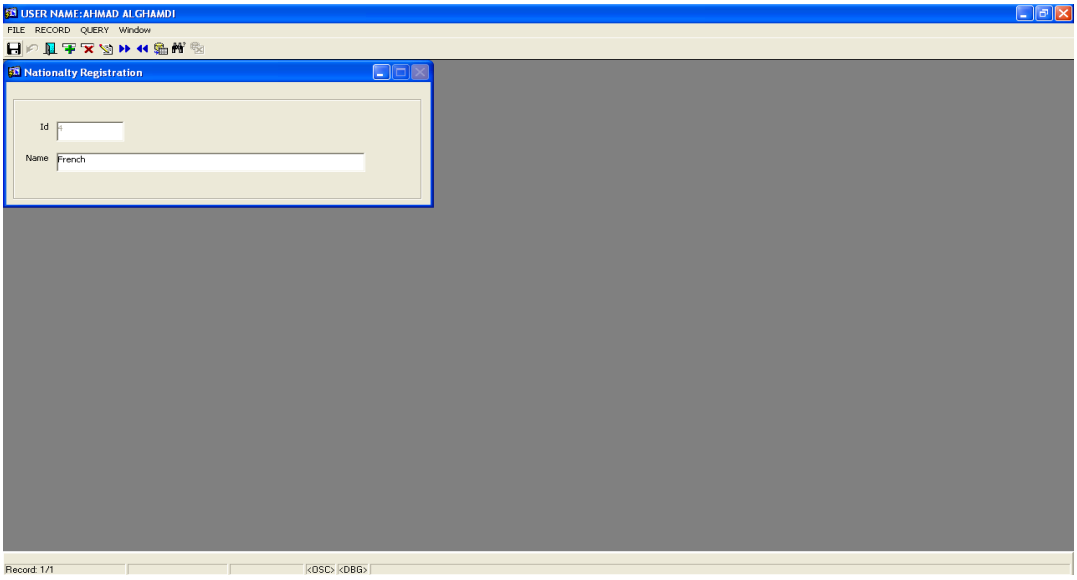


Figure 26 New Nationality Registrations

Under the 'sub-data' registration, the nationality is set-up in a digit that is issued automatically by the system as shown above.

Nationality during new patient registration process

Figure 27 Choosing of Nationality from the List

When the user desires to register new patient data in the registration screen, only the nationality digit is needed without the need to write as shown in the above screen. In this way, the registration time is summarized and assurance of entering data accurately, it is also benefit in statistics and research process.

Email Screen

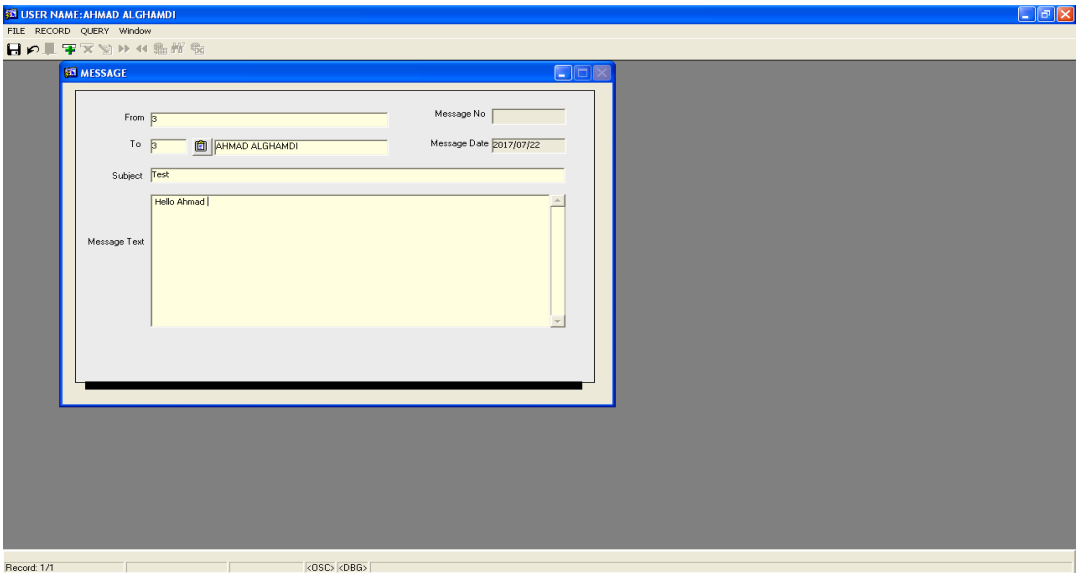


Figure 28 E-mail Sending Screen

ISSN: 2663-5798

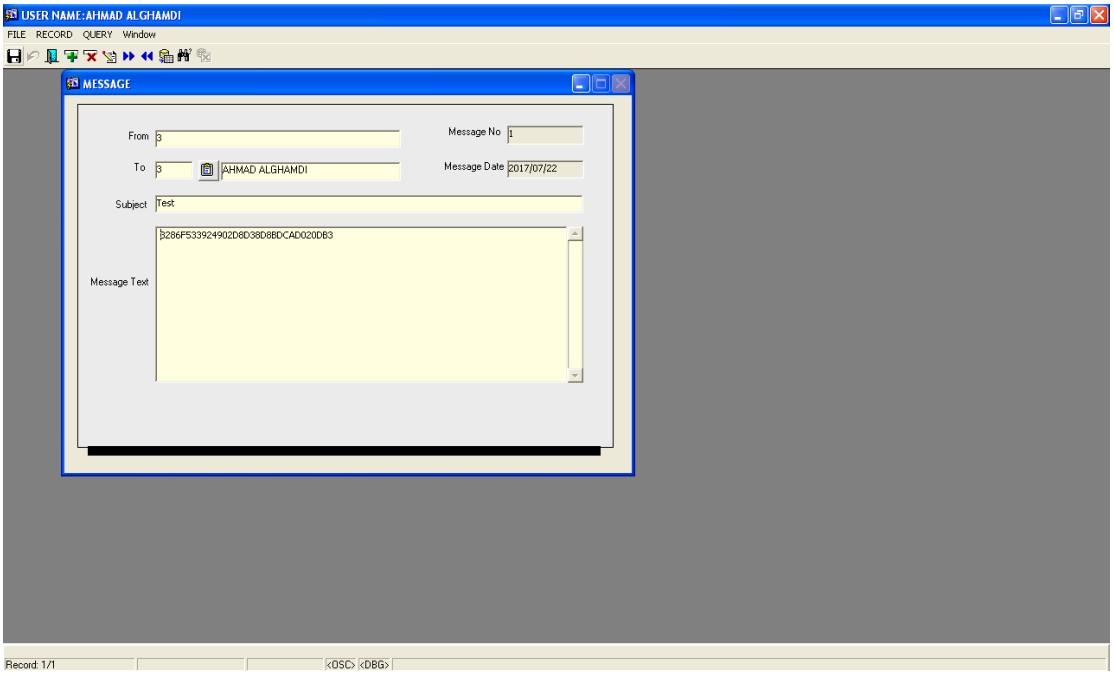


Figure 29 Explains Encryption Process

The E-mail sending screen shown above is internal for all system users. In this e-mailing option, the user name, recipient and the actual message content are specified. The text specified in the 'message text' is encoded by AES256 encryption method as shown in the above screen.

Email Received

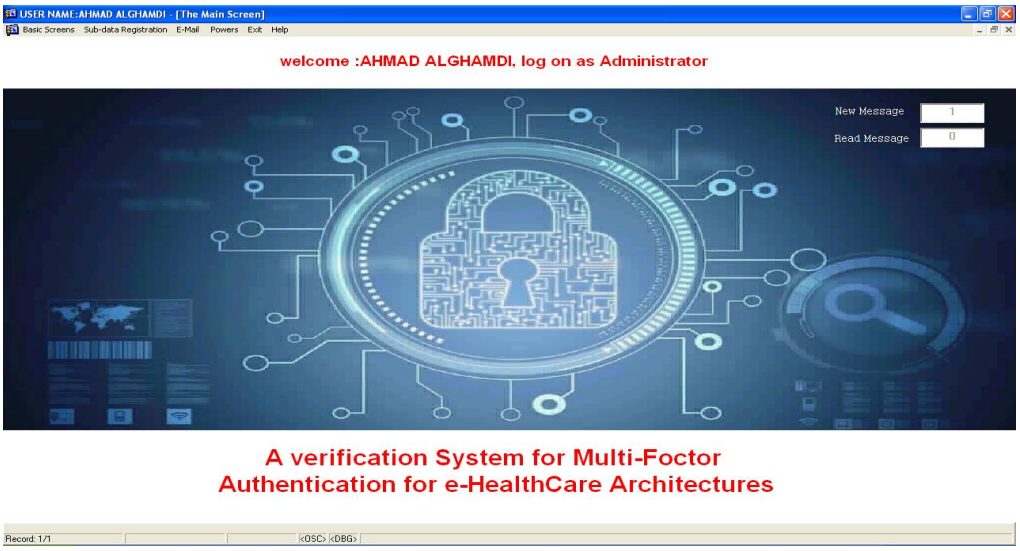


Figure 30 to show a process of receiving the message to the receiver

The above screen shows the process of receiving the message from the user in the referred box in red colour. This specifies that new messages are received but not read by the receiver.

Status in message reception box

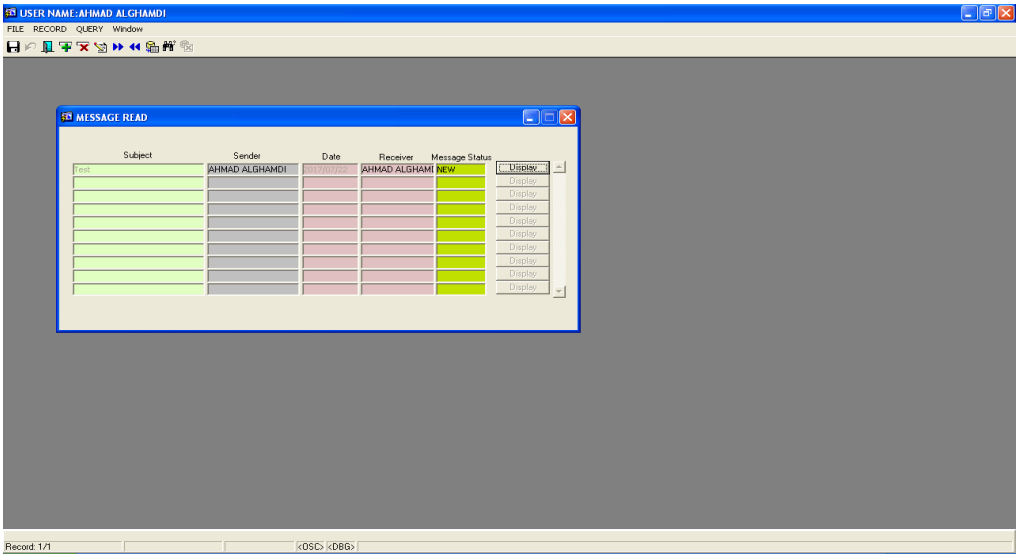


Figure 31 defines message reception box and its status

The message reception box shown above indicates the transferred message to the receiver. In this box, the sender name, date of sending, message subject and message status are displayed.

Message Read

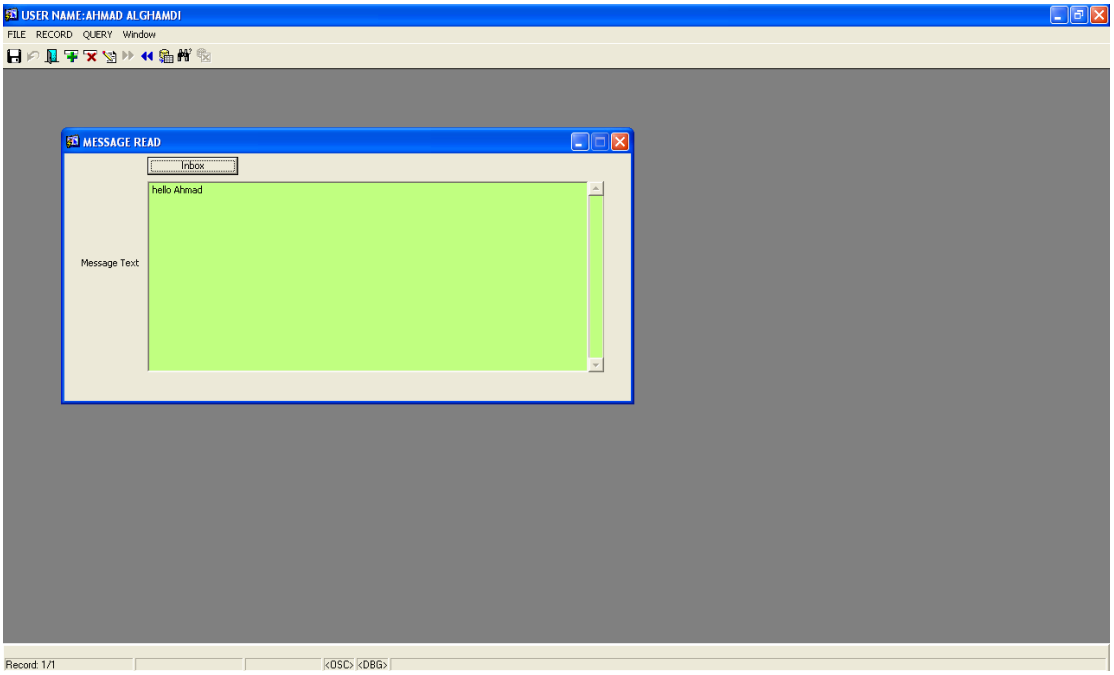


Figure 32 Message Text Reading Screen

The above screen shows the way in which the receiver has read the message that is being received.

ISSN: 2663-5798

Status update in message reception box

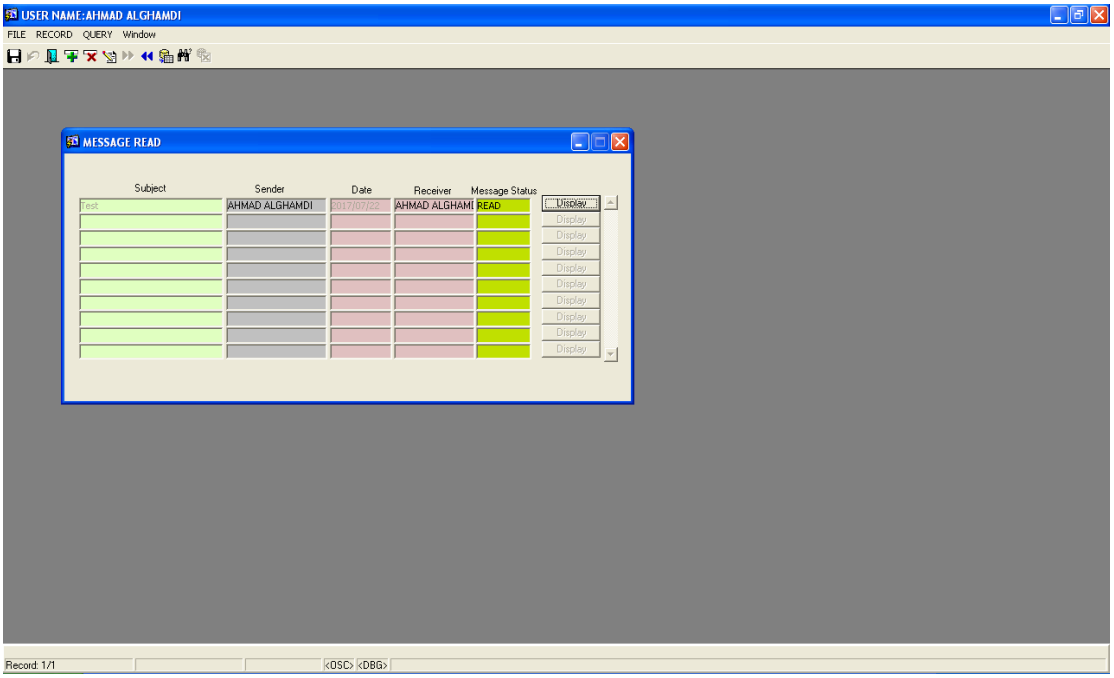


Figure 33 in messages box, it defines the message status after it has been reading than it was readable.

When the message that is received is being read by the receiver, the status of the message is immediately update in the message reception box under 'message status' column as shown above.

Message status on the screen

Figure 34 defines message status in the main screen

The above screen shows the message status on the main screen for the user without need to enter messages box to know the new messages status or readable messages.

Summary

This chapter gives the implementation details of the multi-factor authentication system for e-healthcare system along with the detailed description of the system screenshots. When the system is exited, the time and date of exit are registered in the log which is further useful for the user tracking.

Chapter 6: System Testing

6.1 Overview

This chapter covers the details of system testing that is carried on the implemented multi-factor authentication system for the e-healthcare architectures. In the process of presenting this system testing process, the adopted test plan and the test cases to carry out the testing process are detailed in this chapter.

6.2 Testing

Testing is one of the crucial steps involved in a project that involves in the identification of any errors present in the implemented system. According to Ammann and Offutt (2016), this process of testing involved in identifying any mistakes in implementation helps the testing process in improving the quality of the system. This testing of the system can be carried out either through black box, white box or grey box testing. According to Lewis (2016), black box testing also known as functional testing involves in the process of testing the functionality of the system, white box testing also known as glass box testing involves in the process of testing the internal working of the software. Grey box testing involves in combining both the white box and back box testing stages.

Taking the features of all the different types of testing, this research involves in the adoption of grey box testing method. This adoption of grey box testing involves in testing both the internal working of the software and also the external functionality of the system. Use of test cases is done in order to test the external functionality of the system, whereas the internal software system of the multi-factor authentication system is tested using manual testing of the code logic.

6.3 Test Cases

This section of the chapter gives clear details of the test cases that are used for carrying out the black box testing of the implemented multi-factor authentication system for e-healthcare application.

Test case 1: Login screen validation	
Description	This test case is aimed at verifying the validation controls that are implemented in the login page of the e-healthcare system
Input	Input involves in giving all the details such as username, password, facial recognition and NFC accurately.
Expected Output	As all the input fields are valid, the system must allow the user to enter the application

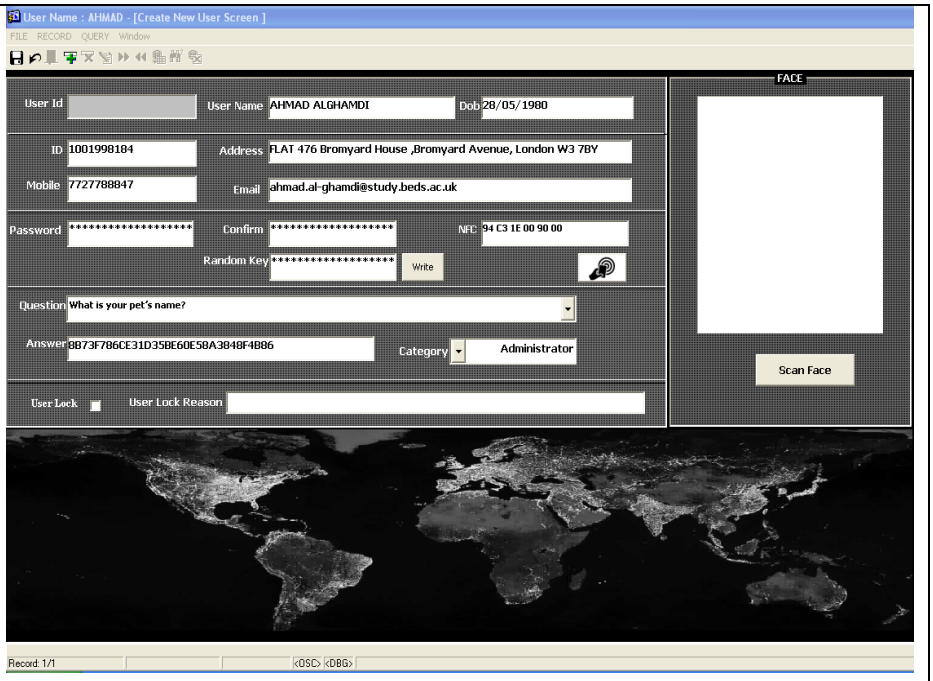
ISSN: 2663-5798

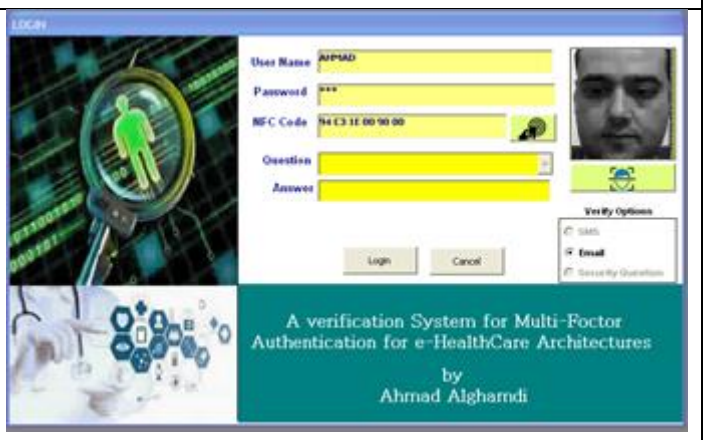
Obtained output	
Result	As the expected and the obtained output are same, the result of this test case is pass.

Test case 2: Registration screen validation	
Description	The aim of this test case is to verify the validation controls that are implemented in the registration page of this system.
Input	The input involves in the user giving the content in the fields “password” and “content” differently.
Expected output	As the actual and confirm password are different, the user must be prompted with an error message.
Obtained output	**Put a screen that displays error when content in “password” field and “content” field are different**
Result	The result of this test case is pass as the expected and obtained output are the same.

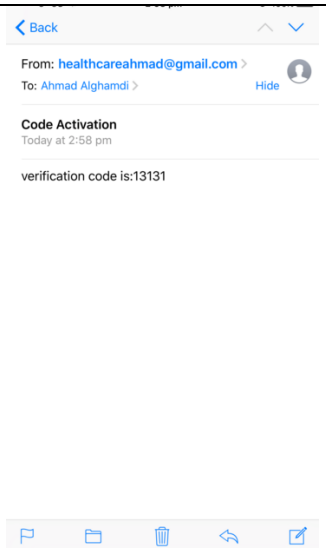
Test case 3: Encryption in password page	
Description	This test case is mainly aimed at testing the encrypting mechanism that is being implemented as part of the registration screen of the system.
Input	Input involves in user entering the password, answer to the question and the random number.
Expected output	All the information that is given as input in the above mentioned fields must be encrypted

ISSN: 2663-5798

Obtained Output	
Result	As the expected and obtained outputs are the same, the result is pass.

Test Case 4: E-mail verification	
Description	This test case is aimed at testing whether the verification code is properly send to the registered e-mail address
Input	Input is providing valid email address in registration stage and selecting the radio button 'email' in the login page.
Expected output	The expected output involves in user receiving the 5 digit code through email.
Obtained output	 STEP 1(Verification via E-mail which contains verification code)

ISSN: 2663-5798

	 Step 2 (system sent a verification code to the user)
Result	As expected and obtained outputs are the same, result of this test case is pass.

6.4 Summary

This chapter has detailed the output of system testing which is carried out using test cases and dedicated test plan on the implemented system. From the test case results, it is found that all the test cases are passing and the implemented system is found to be error-free.

Chapter 7: Conclusion, Recommendations and Future Work

7.1 Conclusion

Huge developments in the technology resulted in the extensive use of internet in majority of the applications. Currently, internet has become part and partial of every one's life due to its usage for several activities by the individuals. Among the various applications that were revolutionised by the use of internet, health care is also one of the crucial ones, which has resulted in the development of e-health care architectures. Besides the e-health care systems providing several advantages to its users, they also face various security issues due to unauthorized user access. Taking the severity of the security issues and the importance of providing high level of security for e-health care architectures, this research intended in developing a strong authentication mechanism for a typical e-health care system. Based in the review of existing authentication mechanisms, a multi-factor authentication scheme is developed in this project the e-health care system. The critical review of the existing methods helped in identifying that multi-factor authentication schemes are very less implemented for e-healthcare systems. This critical review on the e-healthcare security helped in achieving the first objective of this research. The multifactor authentication system developed in this project is intended in verifying user identity based on three main aspects namely password, NFC code and facial features. This multifactor authentication mechanism differs from existing methods by combining all these type of authentication method and also the user of dynamic NFC code that is generated randomly by the system. The allocation of only 60 seconds activation time for this NFC code used as part of multifactor authentication makes the proposed method more effective and also unique. This shows that the current project has achieved the objective of implementing NFC based smart card machine in order to verify the user.

Rapid application methodology helped in carrying out the different stages of the project in a simultaneous manner through which the project was able to completed within the given time period. Design of this project was carried out using unified modelling language

diagrams and the database details are presented in the form of entity relationship diagrams, thereby showing the achievement of the objective on designing the e-healthcare system. Taking these design features into account implementation of multifactor authentication system for e-health care application is done using java programming language, android studio and oracle 10g database. In the implemented system a typical user is initially registered and then authenticated based on password, NFC code and the facial recognition. In order to enhance the security level, AES 256 encryption mechanism is also implemented in this project. This encryption method is used to encrypt the user passwords, random numbers and also the verification questions that are assigned by the users. This shows the achievement of the current project objective on the implementation of AES 256 algorithm for encryption. Testing of the developed application showed that all the test cases are passed indicating the presence of no errors in the developed application. Analysis and the evolution of implemented multifactor authentication revealed the uniqueness and the high security level of proposed scheme in terms of data authentication and security. In this way the current project objective on testing and evaluation of the implemented system.

7.2 Recommendations

Taking the findings and the contributions of the current research into account, following are the recommendations that are made,

1. Highly private and confidential applications like e-healthcare systems must be offered with two-factor or multi-factor authentication system in order to restrict unauthorised user access into the system.
2. Taking the growing number of security attacks on static passwords, it is recommended that applications with higher security requirements must adopt dynamic passwords like NFC codes.
3. Besides using multi-factor authentication, it is recommended that e-health care systems must use cryptographic methods to encrypt the sensitive data while storing and data transmission.

7.3 Limitations

Time is the major limitation of this project as it is very hard to cover the complete implementation and documentation parts within the available short time period of three months. In other words, development of a complete e-healthcare system with multi-factor authentication system along with the preparation of two reports (interim report and final report) was very challenging in the available time of 3 months.

7.4 Future Work

Considering the need of providing high level of security for the e-healthcare architectures, this project is involved in the implementation of multi-factor authentication system. However, technological developments have resulted in the development of several security devices used to enhance the security level of an application. Therefore, the future work of this research is involved in the application of PinSentry device for the purpose of user authentication. As use of this PinSentry can avoid using the current three options to authenticate a user, identification of the requirements of this device implementation and implementing it acts as an interesting part of the future work.

References

- Alzahrani, A., Alqhtani, A., Elmiligi, H., Gebali, F. and Yasein, M.S., 2013, August. NFC security analysis and vulnerabilities in healthcare applications. In Communications, Computers and Signal Processing (PACRIM), 2013 IEEE Pacific Rim Conference on (pp. 302-305). IEEE.
- Ameller, D., Ayala, C., Cabot, J. and Franch, X., 2013. Non-functional requirements in architectural decision making. IEEE software, 30(2), pp.61-67.
- Ammann, P. and Offutt, J., 2016. Introduction to software testing. Cambridge University Press.

- Bae, M., Kang, H., Kang, J. S., &Yeom, Y. (2017). Mutual Authentication Mechanism using Pre-Shared Key and BB84 Quantum Key Distribution for Quantum Cryptography Communication. Advanced Science and Technology Letters, Vol.143, pp.156-159
- Bhattasali, T., Saeed, K., Chaki, N., &Chaki, R. (2014). Bio-authentication for layered remote health monitor framework. Journal of Medical Informatics & Technologies, 23.
- Boric-Lubecke, O., Gao, X., Yavari, E., Baboli, M., Singh, A. and Lubecke, V.M., 2014, June. E-healthcare: Remote monitoring, privacy, and security. In Microwave Symposium (IMS), 2014 IEEE MTT-S International (pp. 1-3). IEEE.
- Brumen, B., Ivančič, R., &Rozman, I. (2016, September).A comparison of password management policies. In Management of Engineering and Technology (PICMET), 2016 Portland International Conference on (pp. 1922-1927). IEEE.
- Burger, M., Consumerinfo. Com, Inc., 2017. Adjustment of knowledge-based authentication. U.S. Patent 9,633,322.
- Campisi, P., 2013. Security and Privacy in Biometrics (Vol. 24). London: Springer.
- Chaudhry, S. A., Farash, M. S., Naqvi, H., Kumari, S., & Khan, M. K. (2015). An enhanced privacy preserving remote user authentication scheme with provable security. Security and Communication Networks, 8(18), 3782-3795.
- Ford, R. and Graft, W., 2014. User Susceptibility to Internet Attacks.
- Frontoni, E., Baldi, M., Zingaretti, P., Landro, V., &Misericordia, P. (2014, October). Security issues for data sharing and service interoperability in eHealth systems: the Nu. Sa. Test bed. In Security Technology (iCCST), 2014 international Carnahan Conference on (pp. 1-6).IEEE.
- Galbally, J., Marcel, S., &Fierrez, J. (2014). Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. IEEE transactions on image processing, 23(2), 710-724.
- Garrety, K., McLoughlin, I., Wilson, R., Zelle, G. and Martin, M., 2014. National electronic health records and the digital disruption of moral orders. Social Science & Medicine, 101, pp.70-77.
- Hamlet, J.R. and Pierson, L.G., Sandia Corporation, 2014. Multi-factor authentication. U.S. Patent 8,868,923.
- He, D., &Zeadally, S. (2015). Authentication protocol for an ambient assisted living system. IEEE Communications Magazine, 53(1), 71-77.
- He, D., Kumar, N., Chen, J., Lee, C. C., Chilamkurti, N., & Yeo, S. S. (2015). Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. Multimedia Systems, 21(1), 49-60.
- Huang, X.W., Hsieh, C.Y., Wu, C.H. and Cheng, Y.C., 2015, September. A token-based user authentication mechanism for data exchange in RESTful API. In Network-Based Information Systems (NBiS), 2015 18th International Conference on (pp. 601-606). IEEE.
- Idoga, P. E., Agoyi, M., Coker-Farrell, E. Y., &Ekeoma, O. L. (2016, October). Review of security issues in e-Healthcare and solutions. In HONET-ICT, 2016(pp. 118-121). IEEE.
- Karimian, N., Wortman, P. A., &Tehranipoor, F. (2016, October).Evolving authentication design considerations for the internet of biometric things (IoBT). In Hardware/Software Codesign and System Synthesis (CODES+ ISSS), 2016 International Conference on (pp. 1-10). IEEE.
- Kim, D., Lee, J., Yoon, H. S., & Cha, E. Y. (2014).A non-cooperative user authentication system in robot environments. IEEE Transactions on Consumer electronics, 53(2).
- LastPass (2017).The best way to manage passwords. [Online] Available at: https://www.lastpass.com/how-it-works, Accessed on: 19/7/2017.
- Lawrence, C., Fulton, E., Evans, G., & Firth, D. (2014).Employing Two Factor Authentication Mechanisms: A Case Study. Information Systems Education Journal, 12(5), 16-22.
- Lewis, W.E., 2016. Software testing and continuous quality improvement. CRC press.

- Liang, Y.D., 2013. Introduction to Java programming: brief version. Pearson.
- Ma, Y. and Han, S., 2009. Self-face advantage is modulated by social threat–Boss effect on self-face recognition. Journal of Experimental Social Psychology, 45(4), pp.1048-1051.
- Odelu, V., Das, A.K. and Goswami, A., 2015. A secure biometrics-based multi-server authentication protocol using smart cards. IEEE Transactions on Information Forensics and Security, 10(9), pp.1953-1966.
- Pussewalage, H.S.G. and Oleshchuk, V.A., 2016. Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions. International Journal of Information Management, 36(6), pp.1161-1173.
- Pussewalage, H.S.G. and Oleshchuk, V.A., 2016. Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions. International Journal of Information Management, 36(6), pp.1161-1173.
- Shahabadkar, R., Reddy, S. S. S., Manjunath, C., Channabasava, U., &Shahabadkar, K. R. (2017, April). Secure Framework of Authentication Mechanism Over Cloud Environment. In Computer Science On-line Conference (pp. 284-291).Springer, Cham.
- Wang, A., Chang, W., Mohaisen, A. and Chen, S., 2014, November. POSTER: How Distributed Are Today's DDoS Attacks?. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (pp. 1511-1513). ACM.
- Zhang, R., Chen, D., Shang, X., Zhu, X., & Liu, K. (2017).A Knowledge-Constrained Access Control Model for Protecting Patient Privacy in Hospital Information Systems. IEEE Journal of Biomedical and Health Informatics.
- Zhao, R., Li, X., Xu, G., Feng, Z. and Hao, J., 2016, November. E-SSL: An SSL Security-Enhanced Method for Bypassing MITM Attacks in Mobile Internet. In International Workshop on Structured Object-Oriented Formal Language and Method (pp. 101-120). Springer, Cham.