International Journal of
Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2020.33940

Volume 6, Issue 12
December - 2020

Development of Access Control Mechanism Based on Fingerprint Biometrics and Mobile Phone Identity for Industrial Internet of Things Critical Infrastructure Protection

Joseph Kalunga*[1], Simon Tembo[2], Jackson Phiri[3]

Ph.D Scholar[1], Professor [2, 3]

[1,2] Department of Electrical and Electronic Engineering, School of Engineering, University of Zambia

[3]Computer Science Department, School of Natural Sciences, University of Zambia

Lusaka, Zambia

ABSTRACT

This paper details the development of an access control mechanism based on fingerprint biometrics and mobile phone International Mobile Equipment Identity (IMEI) modalities for the industrial internet of thing (Industrial IoT) Critical Infrastructure (CI) protection. The idea behind this study is to harden physical security through human identification and authentication processes to Smart CI places such as buildings, military bases, hospitals, airports and other important infrastructure. Fingerprint and mobile phone IMEI are very recognized and accepted identities hence used in police criminal investigation and legal community. Other uses of mobile phone identities include e-medicine, mobile banking, mobile money and remote machine operation. The main objective of this study is to develop a prototype application for authentication and identification of legitimate Industrial IoT human entities/objects based on the mentioned two identities as opposed to traditional knowledge (password, phrase or personal identification number (PIN) etc.,) and possession (token, smart card, identity card etc.,) based Access Control instruments. To achieve this, the study based on eXtreme programming methodology was conducted using visual studio 2010 on DotNet framework 4.0 with C# object oriented programming language. The backend database employed was MySQL open-source Relational database management system (RDMBS). The research produced a number of key results include the development of fingerprint biometric and mobile phone IMEI human identity security layers (modules) and many others. The developed prototype application performance was evaluated by enrolled some fingerprints, IMEI and captured related individual personal information. The result indicated 99.999% accuracy levels. In conclusion, the study shows that the integration of fingerprint and mobile phone IMEI identities in access control roles can improve the security of the Industrial IoT institution and alleviate problems associated with traditional identity authentication methods.

Key Words: *Physical Security hardening Access Control*, *Biometrics, Mobile phone identity, Industrial IoT Security, Critical infrastructure protection, Authentication &identification.*

1. INTRODUCTION

Access Control is one of the emanate security issues that may affect the escalation of current initiative and trend “industrie4.0” or “Industrial Internet of things (Industrial IoT)” in modern Critical Infrastructure (CI). People throughout the world are increasingly becoming mobile and the use of mobile phone services to support human living conditions, work related activities and crime perpetuation and illusion have also become community rampant activities. For this reasons, Control of people accessing industrial IoT CI institutions, resources or installations have also become of paramount importance to security requirement of any institution or organization such as smart buildings, military bases, hospitals, airports and other important smart infrastructure. Traditionally, access control mechanisms relied on users to remember a secret text (password) or what they carry (token, card) or combination of both to prove their identities. However, traditional access control mechanisms are not intelligent enough and prone to security vulnerabilities mentioned in [1]. Therefore, an access control mechanism based on biometrics and mobile phone identity may solve some of the problems resulting from using traditional access control methods for human identification and authentication especially in high technological CIs. Additionally, a Mobile phone and biometrics systems today have become two powerful access control and crime-fighting tools because they have both contained vital information suitable for criminal investigations. Biometrics systems offers physiological and behavioral data while mobile phone may provide call history, contacts, text messages, web browser history, a global positioning systems (GPS) and any other location information that police and law enforcement agencies may find valuable[2]. For this reason, Evidence from mobile phones and biometric access control systems can help investigators piece together motives, events and provide new leads[3]. Furthermore, mobile phone and human are designated at the Centre of modern institution and industrial productivity[4]. Adoption of the Industrial IoT concepts in CI can actually revolutionize how CI industries operate, but there is a challenge of having a robust Access Control strategy in place to boost digital transformation efforts while maintaining mobility and legitimate use of mobile devices. These advancements in industry have opened up the paradox of security problems mostly from Internet of thing (IoT) component resulting from the merging of operation technology (OT) and Information Technology (IT) components[5]. For this reason, CIs based on Industrial IoT are vulnerable to a lot of security problems due to human behavior, usage of mobile devices and remote operation technologies and are, therefore, vulnerable to both physical and logical attacks. However, the most serious threat among all could emanate from physical intrusion of unauthorized personnel. Physical Intrusion is a serious threat because it may lender even logical security mechanism ineffective. Physical Intrusion may result in an attacker having a full physical and logical control of the restricted place, installation or assets. Nevertheless, there is no easy, fool proof technical fix, to Industrial IoT critical Infrastructure Security concerns. But the use of biometrics and mobile phone International Mobile Equipment Identity (IMEI) identity characteristics in physical security Access Control hardening role can be modeled to improve security of CI places, installations, buildings, rooms and smart cities.

In view of the above, the main objective of this study is to develop a prototype Access Control Mechanism that is able to authenticate and identify legitimate Industrial IoT human entities/objects based on the biometrics and mobile phone identity traits. The other objective is to show that a real-life generic connection, interaction, communication of sensors, people and mobile phone in Industrial IoT environment could be coined intelligently to harden physical security instead of weakening it. To achieve this, a physical security hardening prototype access control application was developed on Dot Net framework.

The general organization of this paper is as follows: In section 2, Contribution. Section 3 Biometrics and IMEI identity modalities. In section 4 detailed study Materials and Methods. Section 5, reviewed the related works. Section 6 covers Analysis and Modeling aspects. In section 7 highlighted some Results and Discussion. Finally, section 8, conclusion and future works.

2. CONTRIBUTION

This study contributes the following:

- The development Model of physical security hardening access control mechanism based on fingerprint biometrics and Mobile Phone IMEI or SIM number.
- Literature on fingerprint biometrics & mobile phone identity, access controls and Industrial IoT security.
- Architectural design for human identification and Authentication process specifically in industrial IoT CI protection.
- Contributed some areas of study which require further works.

3. BIOMETRICS AND IMEI

Biometrics is an automated method of authenticating a person identity based on biological or behavioral characteristics[6]. Biometrics technologies measure and analyze living human body characteristics for human authentication and identification purposes. Among the different human authentication methods, biometrics is often presented as a promising solution[7]. In view of the above, biometrics based authentication has received extensive attention in research community and industry. This achievement is further attributed to growing security needs and reliability of the biometrics security systems[8]. Considering that, biometrics systems offer higher degree of security and less probability of being spoofed and has proved to be an efficient and an accurate answer to human identity authentication problem[9]. Biometrics authentication models have superseded the effectiveness of the traditional access control security techniques like passwords, national identity card, PIN and many others methods. However, there are various biometrics traits employed in human recognition and authentication systems today. Among these biometrics traits fingerprint and face biometrics have dominated other modalities especially in Access Control and surveillance systems [10]. Nevertheless, due to data privacy concerns, face biometrics recognition system is becoming unpopular especially after land mark court ruling in UK against police force extensive usage and deployment of face biometrics recognition system in community surveillance[10]. Furthermore, government agencies elsewhere including U.S., Canada and many countries around the world are considering or revisiting the legal frameworks concerning the usage and deployment of face biometrics recognition systems in the communities[11]. Additionally, most countries lacks legal framework governing the deployment and usage of face recognition and surveillance systems[11]. With the huge community discontent surrounding face biometrics, acceptability, permanence and distinctiveness of fingerprint biometrics traits in legal and law enforcement community worldwide, access control mechanism based on fingerprint and smart mobile phone identity characteristics could provide an effective tool for human identification and authentication process in Industrial IoT CI protection. However, an increasing number of new fingerprint biometric sensors, applications and a diverse user population in industrie4.0 may result biometric interoperability issue. Additionally, sensors inaccuracy may also provide a security risk that could result in false identification and false rejection fingerprint biometrics problems especially in resource constrained environment[12]. In recent years, Mobile phone and fingerprints identities have become a regular part of human identification and criminal investigation because they are unique; use cheap technology, acceptable in legal community and provide accurate human identity information. These are some important security requirements for a robust access control mechanism to harden physical security in CI protection.

4. MATERIAL AND METHODS

The study employed eXtreme programming (XP) software development methodology. XP is one of the agile software development methodologies. It is suitable for IIoT application development because of its lightweight, release based, efficient, low-risk, flexible, predictable and engineering nature. XP provides value and principles for self-organizing and always guild team behavior. Since IIoT System requirements are normally huge, complex, and vague[13], it requires a methodology that supports program change at less cost, short development cycle, embraces user participation and produce high quality software by taking software engineering practices to extreme. XP is such a methodology and was created by Kent beck in 1996[14]. XP is centered on adaptive planning, self-organizing and short delivery time which tradition software development methodology such as waterfall model cannot archive in modern competitive and dynamic business world. Extreme Programming methodology are based on sound values include communication, simplicity, feedback and respect. Extreme programming methodology life cycle has five phases namely analysis, planning, designing, implementation and the delivering phase. But among these stages, designing, coding and testing are most important activities for software developers and programmers. Figure 1.1 shows XP system development methodology.

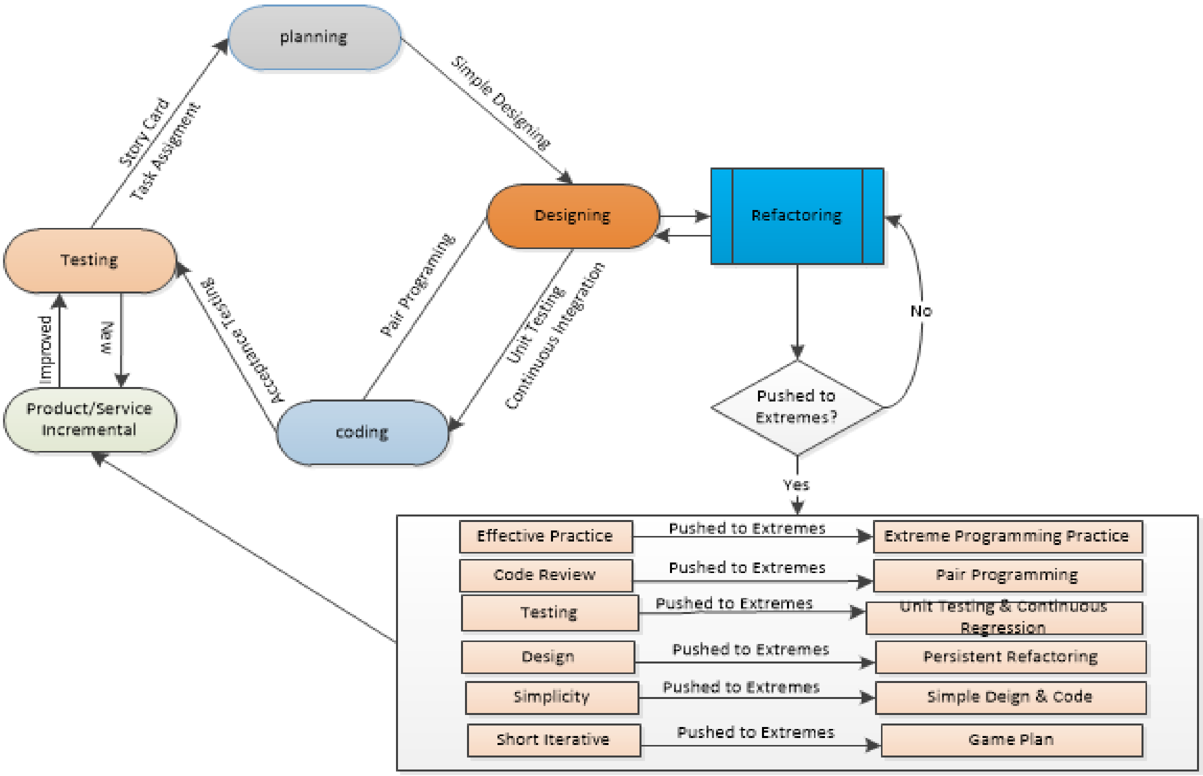


Figure1.1: Extreme Programming System Development Methodology

Additionally, the study instruments were divided into computer hardware and software. The engineering specifications of these tools were as prescribed in table1.1

DOI: 10.31695/IJASRE.2020.33940

Table1.1. Hardware and Software Specification

Hardware Name	Specification
Laptop	- Hard disk 100GB Minimum - Processor 2.6 MHz Minimum. Preferable core i3 and above - RAM 4.0 GB - Graphics frequency 3.30 MHz - 64-bit Operating System
Fingerprint Scanner	- Image resolution 500 pixels per inch. - Image area 9.75mm X 0.41mm/ 192 X 8 pixel - ISO / IEC 7816 T=0 and T=1 - Up to 8MHz smart cards, and a 412 Kbit/s communication speed
Digital Camera	- 18.0 Megapixels - 18-55mm lenses - Speed 3frs - Full-high definition
Software Requirements	- Visual studio 2010 - ZKFinger SDK - Nuetech Bio SDK

5. RELATED WORKS

In[15], the researcher proposed a face biometric access control mechanisms for CI control room protection. The prototype access control system uses continuous authentication and face recognition. The proposed system provided good feature such as user friendliness, and ensures availability and traceability. However, the said prototype access control system lacked mechanism to identify and authenticate other mobile industry IoT entities rather than human. Additionally, Face recognition is still a challenge for recognizing face in motion images, twin's, pose variations, having different accessories like beard, glasses, hair color, hair partition, make-up, different facial expressions under different illumination condition, light intensity, noise, occlusion and thermal image for face matching and error generation[16].

In [17] baina el at proposed a logical PolyOrBAC Access Control Mechanism for interdependent critical information infrastructure (CII) protection. The proposed access control was developed for CII collaborative entities dedicated for power generation, transport, distribution and financial services. Baina et al recognizes that any critical infrastructure (CI) in the network can fail with various degrees of severity due to physical and logical security vulnerabilities. Since many interdependencies exist between CIs, failures can have dramatic consequences on the entire infrastructure hence a new collaborative access control framework called PolyOrBAC. The framework offers each organization participating in a CII the ability to collaborate with other organizations while maintaining control of its resources and internal security policy. However, PolyOrBAC access control framework is very complex and developed to provide logical access control among CIIs collaborative entities. Furthermore, it cannot be implemented to harden physical security which is a sole responsibility for each member in CI institution.

In [18], the researcher proposed cyber-physical access control (CPAC) solution, the proposed cyber-physical access control framework enables fine-grained enforcement of context- aware policies in a real-time control system environment. CPAC takes a comprehensive view of both the computing and physical elements comprising the control system, and simultaneously incorporates both continuous physical dynamics i.e mathematical models and discrete computing i.e administrator specified policies into its security monitoring and control calculations. Considering that, the traditional discretionary and mandatory access control mechanisms are often based on manually-generated policy rule sets that do not consider the underlying physics of the grid, and its complexity precludes attempts at formal analysis. CPAC is also very complex and logical security which can work only well in power grid CI type. This type of access control is contextual based, hence may not be suitable in other type of critical infrastructure such as military bases, nuclear plant, petroleum plant and other smart buildings critical installations.

DOI: 10.31695/IJASRE.2020.33940

In[1], the access control mechanism was developed and integrated in to military police duties to protect military Critical Infrastructure such as military bases, command post, installation and military buildings. The researcher employed the combination of fingerprint biometrics modal and traditional national registration card (NRC) to authenticate, identify, control and monitor military Critical Infrastructure. The proposed access control can work well in hardening physical security of the military installations based on traditional ICT settings. However, the proposed mechanism is inefficient in terms of controlling access to infrastructure based on Industrial IoT (industry 4.0) element because in that environment an attack cannot only activated from human entities but also mobile IoT devices armed with surveillance and remote access communication features. There is need to integrate logical and physical security for authenticating and identifying alien mobile IoT objects accessing CI. These mobile device properties may provide valuable information for forensic investigation in an aftermath of an attack. Unlike the forensic investigation of previous attacks on CI which never provided the conclusive autopsy of what actually happened and the actual sources of attack[5].

6. ANALYSIS AND MODELLING

System development process has life cycle and may be constructed from various phase as explained in section 4. At the initial stage of the application development, requirements are extraction from users and stakeholders. The process of extracting requirements from users and stakeholders is called requirement elicitation. Requirement elicitation process is one of the most important application development phases[19]. It involves expressing, analyzing and documenting Users' requirements together with their dependencies. However, implementation and development of all users and stakeholders requirement is extremely difficult in industrial IoT environment due to huge scope of security considerations and limited resources such as budget constraint, short project delivery schedule and lack of qualified man power. Before requirement modeling and documentation, elicited requirements were subjected to further analysis involving weightage in terms of importance and institution critical needs. In our case, the development of the proposed physical security access control mechanism was prioritized. But before system development stage, fingerprint biometrics and mobile device identification and authentication were analyzed and modeled. The abstract requirements of the proposed mechanism were visualize and modeled in to the situation.

6.1. Situation Modeling

Situation analysis and modeling could provide a firm ground for Industrial IoT security design and development. The Situation analysis is however a mental process that involves the creations of story cards which is also referred to as the rich picture. Rich picture was created by Peter Check land for describing IT problem situations[20]. The rich picture can also be drawn to represent the problem situation, scenario, issues, initiative or any other occurrence of concern[1]. In other words a rich picture is drown to explore, acknowledge and define a situation and expresses it through diagrams to create a preliminary mental model. In our case, the physical security Access Control mental model was created. The mental model included some Structures, Processes, environment, people, and emotions, fears, issues expressed by people and conflicts and so on. The rich picture may also referred to as a story card in XP software development methodology. Figure 2.1 shows the rich picture of developed Industrial IoT physical security Access Control Mechanism.

DOI: 10.31695/IJASRE.2020.33940

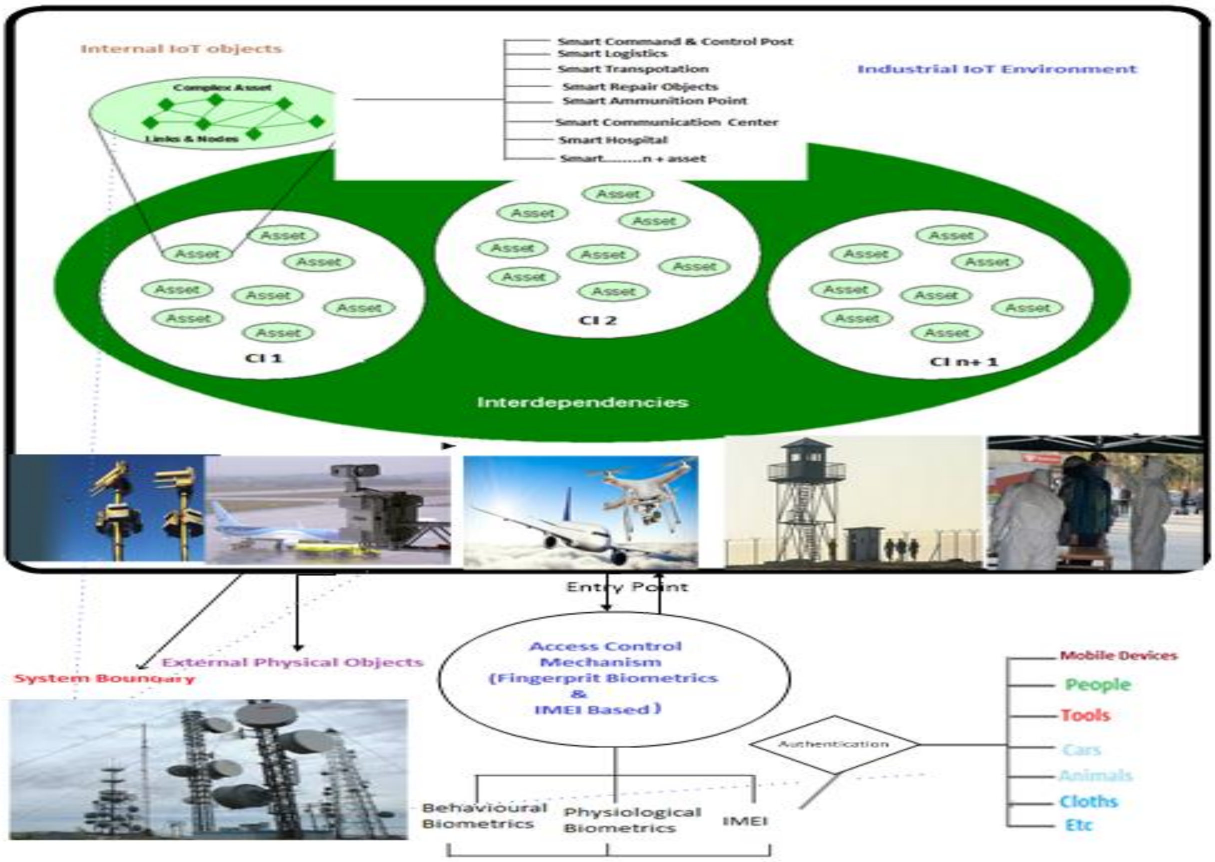


Figure2.1: Rich Picture of the developed Access Control Mechanism

As expressed in figure 2.1, Industrial IoT environment may include internal and external CI objects and assets. These objects and assets may be grouped together according to core service / function or geographical location as indicated in the story card. Access control security is then enforced according to specific organization implementation policy and may include connected and interdependent CI themselves, assets and objects. The interdependence implies that the failure of one CI installation may have cascading effect to other dependent CIs. The rich picture also expressed that, in Industrial IoT environment machines, equipment, mobile device, people, cars, animals, cloths or thing have abilities to connect, access and communicate to each other through sensor and actuator networks [21].

6.2. Human and Mobile Phone Identity Modalities

As the use of mobile computing and communications technologies, like smartphones, continues to increase across government and development agencies, supporting biometrics with these mobile devices may be an appropriate future strategy to cut device and implementation costs[22]. In this context a mobile device is simply a portable computing device [3]. Mobile devices are not an exception to Industrial IoT CI protection because mobile phones have proved themselves essential in supporting human living and work activities. For this reason, mobile phone identity modalities are slowly being accepted in community; government and banking world. Mobile phone has unique features such as Subscriber Identity Module (SIM) and IMEI that makes it a suitable modality for access control security implementation. According to the research conducted by Juniper [23] human mobile phone identifier services could become a primary source of identification and authentication in future. This could provide a drastic shift in human identity modalities which are currently dominated by biometrics and other traditional techniques. Biometrics identification modalities may be categorized in to behavioral or physiological[6]. Physiological human characteristics refers to the measurement of human body parts which may include but not limited to fingerprint, hand geometry, face, iris, and retina and foot configuration[24]. Physiological biometrics computes either physiological or biological human features. Examples of these biological features include ridges and valleys (in fingerprint biometrics), the shape of the hand, shape of the finger, vein pattern, the eye (iris and retina), and the shape of the face[25].These biological features are subjected to further morphological analysis in order to detect and identify uniqueness in the template or patterns.

For biological analysis, DNA, blood, saliva, or urine may be employed especially by police or medical expert examination particularly in criminal offences that require forensics investigations. Human biometric features vary from one person to another and hence are suitable for security implementation especially in Access Control (human identification and authentication) role.

DOI: 10.31695/IJASRE.2020.33940

The fingerprint biometric systems based on physiological or biological characteristics have relative high accuracy as compared to the one based on behavioral characteristics[26]. However, physiological biometrics has its own downside include getting affected by chemicals especially for those people working in the chemical industries[27]. Furthermore, physiological biometric is affected by diabetic disease[28]. The eyes of diabetes patient get affected resulting in differences in matching features. Another problem is that physiological biometrics introduces public data privacy concerns because human body characteristics are permanent and irreplaceable[1]. The same could be said to human behavior.

Behavioral biometrics refers to the type of biometrics that uniquely identifying and measure patterns in human activities[29]. It estimates human ways, habits, style or pattern of doing something such as signing documents (signature), typing habits (keystroke), voice (speech pattern), mouse movement, body orientations when walking (gait), lips movement, handwriting and many others human behaviors. In other words, behavioral biometrics identify people by how they do what they do, rather than what they are (e.g. fingerprint, DNA and face) and what they know (e.g. token and password). For example, the signature recognition is based on the dynamics of making the signature, rather than a direct comparison of the signature template stored in the relational database. Behavior biometric is cheaper in implemented because it can utilize an existing hardware and only require a third party application for analysis[30]. Examples of these biometrics traits include: voice and keystroke that can be captured without any employment of specialized hardware. Additionally, Behavior biometrics template is simple to analyze as compared to physiological biometrics. Behavior biometrics traits can be captured and enrolled non-obstructively (without knowledge of the donor). However, its biometrics traits may be affected by an illness caused through diseases such as cancer, Parkinson, arthritis and stroke [31]. Behavior biometrics may also suffer from old age disorder due to reduction in human body activities and thus violets biometrics characteristics of permanence[32]. In view of the above, behavior biometrics systems are less established and only those based on muscle control such as keystroke, gait or signature are well analyzed. As the result, most behavior biometrics traits may not be unique enough to provide accurate human identification and authentication[33]. Behavior biometrics is also not fully accepted in the community today and hence cannot be employed as a sole identifier in commercial security application. This leaves us with fingerprint biometrics system option which is accepted in criminal justice and legal community[1]. However, in smart CI protection, access control based on biometrics trait alone may not be resilient enough as other ambiguity communication devices may communicate stealthily with other important assets, infrastructure, equipment or installation its. Figure3.1 shows some common human and mobile device identity characteristics:

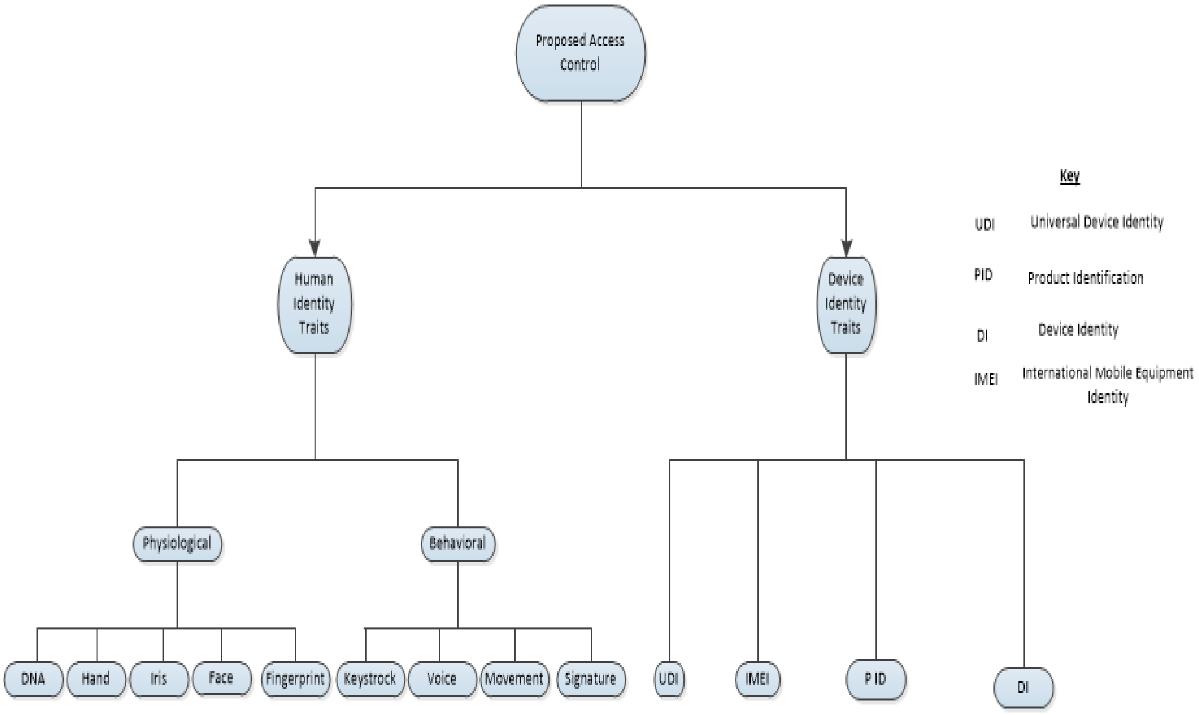


Figure3.1: Human and Mobile device Access Control Identities

DOI: 10.31695/IJASRE.2020.33940

6.3. Context Modeling

To illustrate the operational context of the developed prototype access control mechanism, the context diagram was employed. The context model shows how the proposed access control mechanism fit into the security context of the people and the CI organization they serve. Context models can also referred to as enterprise architecture models, high-level design models or conceptual models[34]. In simple terms, context model shows the other systems in the environment and not how the system internal components behaves, developed or used in the CI environment. Figure 4.1 shows the context diagram:

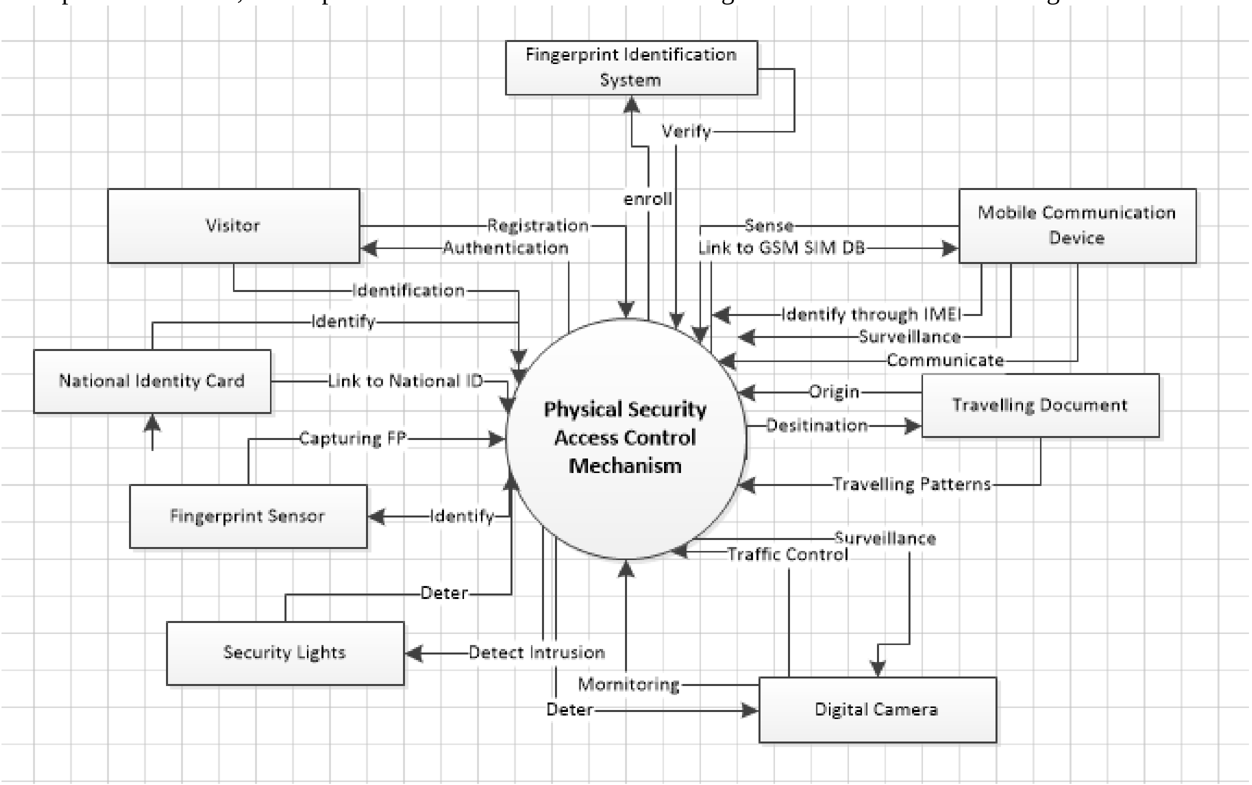


Figure4.1: Context Diagram

Fig 4.1 illustrates various access control mechanism for hardening physical security. The study acknowledges that untrusted IoT entities (human and mobile device) present serious security vulnerabilities to smart CI and acknowledges that human could be the weakest security link to CI protection. The developed application provides a focal point for hardening physical security in CI protection in addition or in combination with other highlighted security mechanisms. Traditionally, National identity documents (NRC & travelling documents), CCTV (digital camera), security lights and biometrics system are other standalone interventions that could be employed in hardening physical security. However, due to manual intervention (national identity document), tediousness', labor intensive and high heterogeneity of devices and network protocol (logical security) which is the part of IoT ecosystems, there are several limitations in these mechanisms especially interoperates between themselves and the surrounding services, infrastructure or environment. In this information age, the combination of biological, behavioral and communication aspect in providing access control to important resources, services or infrastructure may provide a missing link to human centric CI protection.

6.4. Behavior Modeling

To model the entire systems behaviors, activity diagram was employed. An activity is any operation aspect of the system which focuses on conditioning the flow and sequence in which various processes happen. Activity diagram offer high level description of our access control mechanisms. Additionally, Issues' concerning what triggered a particular occurrence may also be detailed clearly [35]. In summary, an activity diagram portrays the task flow from start to finishing point, showing various decision paths that may exist while certain activities are being executed. However, activity diagram does not model the system and user interaction which is another important aspect in modern software projects development. Fig 5.1 shows activity diagram for the developed prototype Access Control Mechanism:.

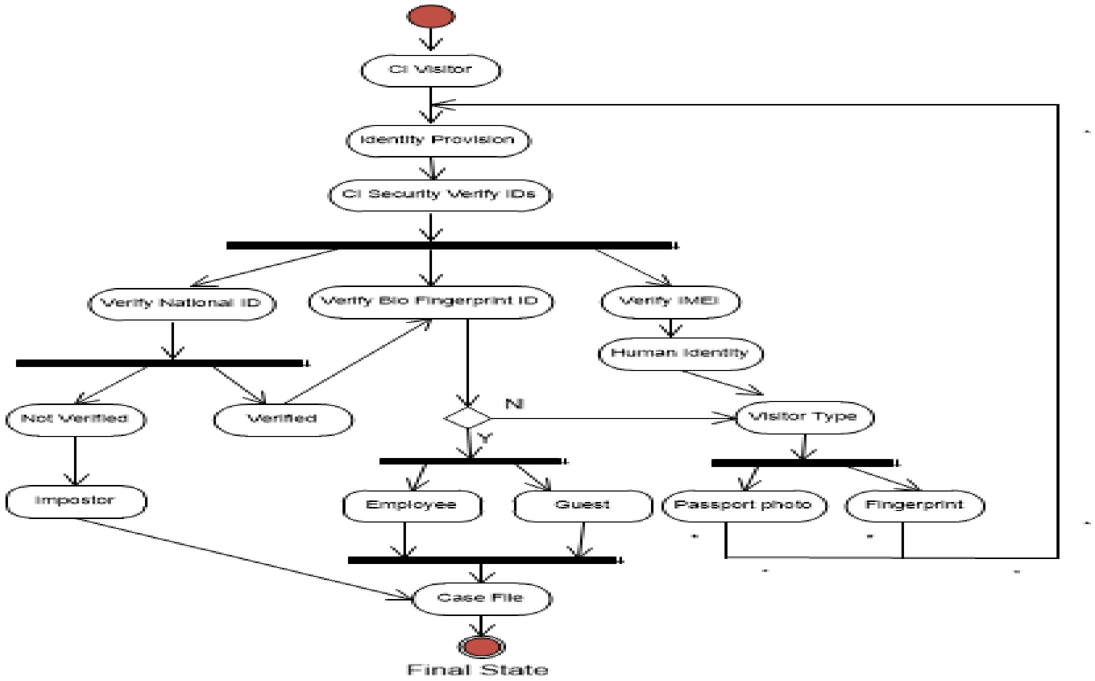


Figure5.1: Activity diagram

6.5. Use case Modeling

In order to model the system and user interaction, Use case diagram was employed. Use case diagram is one of the most important aspects in software requirement modeling because it captures system dynamic behavior. The dynamic behavior means behavior of the system and users themselves when the access control prototype application is running. Activity diagram models static behavior as opposed to dynamic behavior in the use case model. That being stated, use case diagram helped us to model the dynamic aspects of our proposed access control prototype mechanism. But before that, internal and external collaborators referred to as actors were identified. Identified actors include CI Security (sentries), criminal investigating officer (CIO), data entry office (vetting office), visitor and many others highlighted in figure 6.1. Some important use cases in this study are detailed in table 2.1 below:

Table2.1. use case description

Use Case	Actor	Pre - condition	Post-condition
Verify visitor	CI Security, fingerprint sensor, SDK	Criminal vetted	Identification & authentication
Authentication	CI Security, Fingerprint sensor	Criminal vetted	Identification
Security Vetting	CIO & DDE	Identified	Identification & Authentication
Criminal Investigation	CI & visitor	Committed offence	Identification
Donate fingerprints & IMEI	Visitor	Criminal vetted	Identification & authentication
Fingerprint analysis	CIO & CFI	Identity & digital investigation issues	Building criminal offences
Capture visitor particulars & amendments	DEO, visitor & fingerprint sensor	First visit	Identity detail mining
Library	SDK & Sensor	Developer studio & developer	Developed access control mechanism

DOI: 10.31695/IJASRE.2020.33940

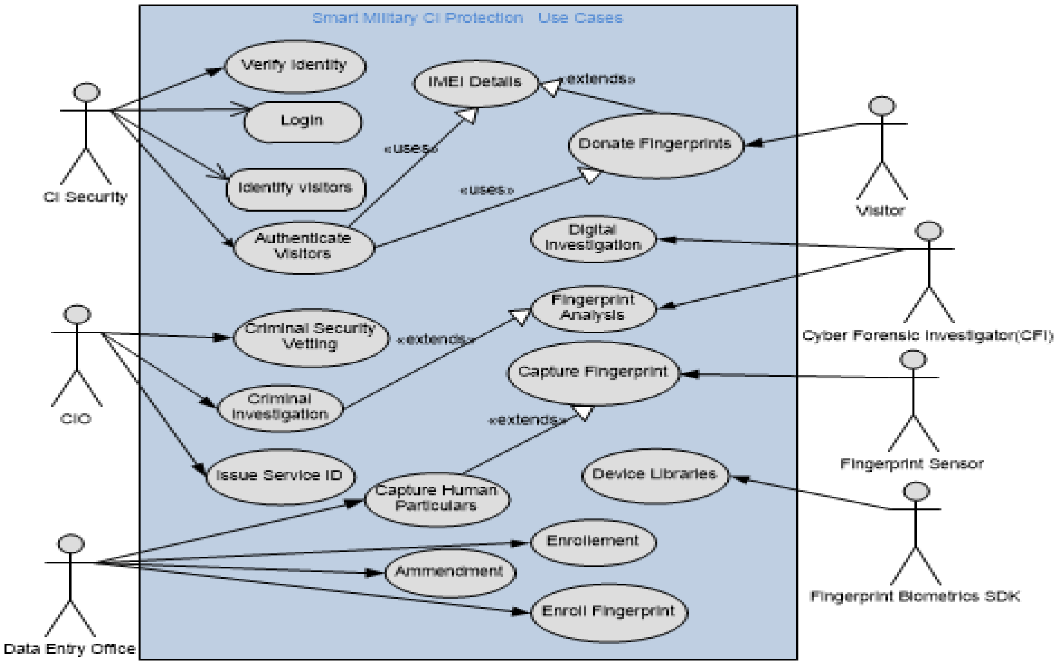


Figure6.1: Use Case Diagram

6.6.Architecture

The architectural design of the developed prototype access control application has four important components namely fingerprint sensor, mobile device, business logic and relational database. The three components are logically hosted at the edge server of Industrial IoT CI building or installation. These components were sub-divided further into specialized sub components such as device drivers, middleware and application plug-in interfaces (API) and dynamic data link libraries (DDL). Device drivers define operating parameters of fingerprint scanner and digital camera and enable the two devices to communicate with the operating system. Without drivers, the computer would not be able to send, receive or format data. Each device connected to the computer system has its own driver that manages its operations. Middleware application acted as an adapter between two applications. The generic Architectural design of the developed access control is as indicated Fig.7.1:

DOI: 10.31695/IJASRE.2020.33940

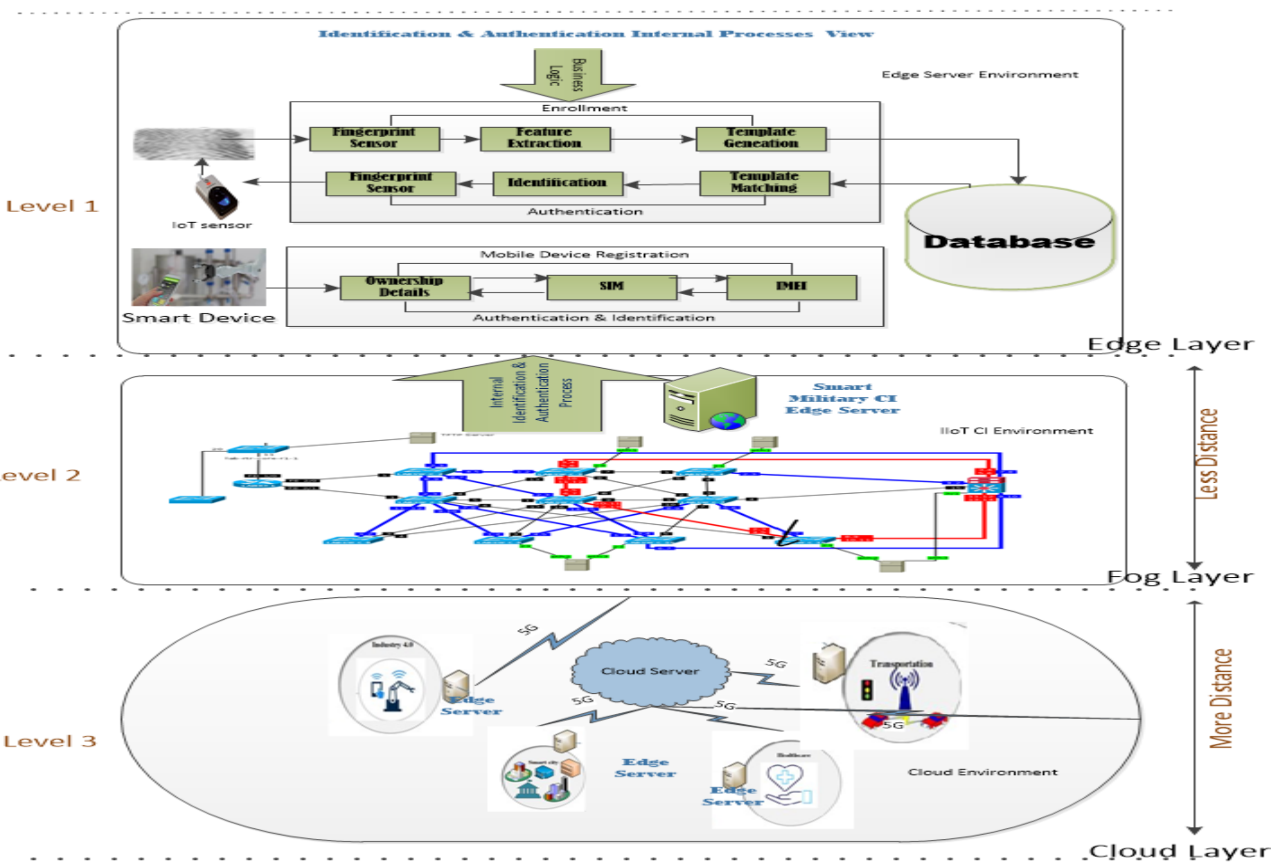


Figure7.1: Generic Architectural Design

6.6.1. Fingerprint Sensor and Mobile Device

Fingerprint scanner and mobile phone devices were employed to capture human and device identity characteristics. In this access control mechanism, DigitalPerson U4500 fingerprint reader was used. DigitaPerson U4500 fingerprint sensor is the USB device built on the latest optical fingerprint reader technology. It has a compacted and attractive design to conserve desk space in an enterprise. Furthermore, digital personal has professional modern appearance suitable for point-to-point environment and has ability to read fingerprint from any angle makes it suitable for application where users share computing devices. On the other hand, mobile device IMEI were captured manually and electronically by dialing *#06# on the targeted device itself [4,12].

6.6.2. Business Logic

Business logic includes processes for fingerprint biometrics enrollment and authentication and mobile device registering and authentication. Technically, business logic is sometimes refer to as domain logic and involves all aspects of system design and development that encodes the real-world business rules in to a computer program or software. It involved all phases required to determine how data is created, stored, and changed. Business logic also prescribes how IoT objects interact with one another, and enforces the routes and the methods by which business of various IoT object are accessed and updated.

6.6.3. Fingerprint Biometric and IMEI Processes

The fingerprints captured for biometric use are subjected to further processing involving irreversible fingerprint template. It is this generated template that is identified against the live fingerprint impression on the fingerprint sensor and consequently grants specific access to particular resource. The other module of this access control include capturing and storage of fingerprints images employed for security vetting and mining of human and phone identity details for the purpose of digital forensic investigation as a preparatory measure required to mitigate human and mobile phone centric attacks. However, fingerprint captured for security vetting process does not require any processing but are stored directly as images in the relational database together with relevant personal details. While fingerprint image captured for biometric system are processed to skeleton image levels in order to extract relevant biometrics features. In similar ways, mobile phone identity characteristics are manually captured from the mobile phone and saved directly in to the database. Minutiae base fingerprint image processing algorithm using crossing number(CN) concept has seven stages include fingerprint capturing, normalization, segmentation, enhancement, thinning and minutiae extraction, storage and identification as shown in the data flow diagram figure 8.1:

DOI: 10.31695/IJASRE.2020.33940

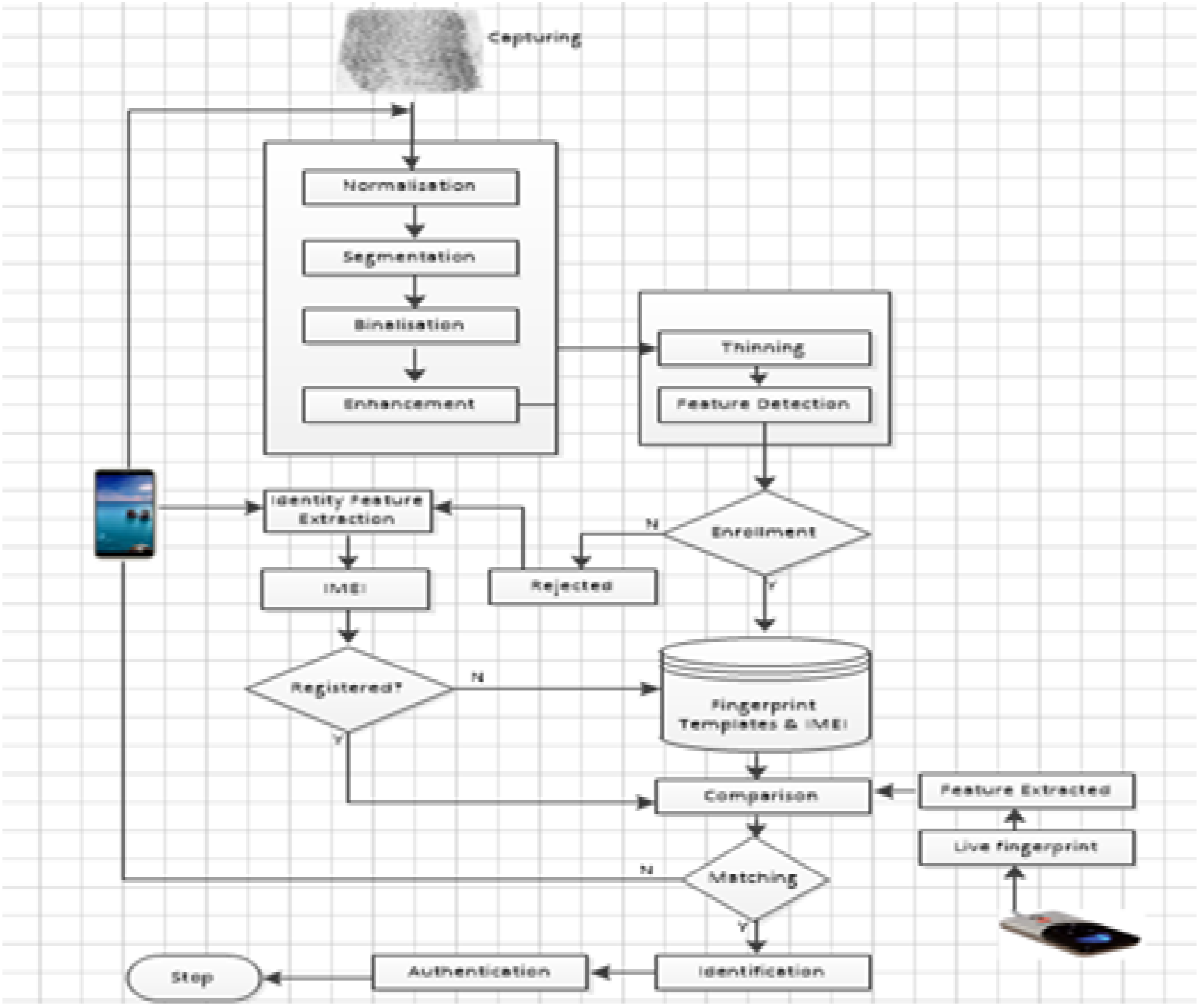


Figure7.1: Data flow diagram

a. Capturing. Fingerprint capturing is the process of input fingerprint image from the optical fingerprint scanner into the computer system. The image captured by the fingerprint sensor is called a grey image. Fingerprint image capturing algorithm is as indicated in the block figure 8.1:

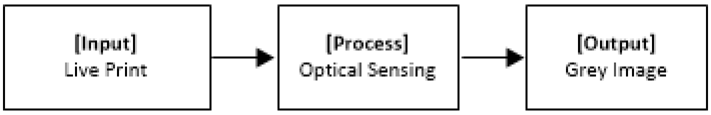


Figure8.1: Data flow diagram

b. Normalization. Normalization operation acts on the gray fingerprint image to standardize image pixel intensity values. Normalization in image processing is sometimes called contrast stretching or histogram stretching. Normalization transforms gray image of n-dimension I: {X ∈ R^n }→{Min,….Max} with intensity values range (min, max) into a new image I_N :{ X ∈ R^n }→{Min,….Max} with intensity value in range (newmin…newmax). Therefore, normalization of the gray scale captured fingerprint image is performed according to the following formulae:

$$I_N = (1 - \min)\frac{New\ Max - NewMin}{Max\ -\ Min} + NewMin$$

Where: I_N = New Image, min is minimum intensity pixel value and Max is maximum intensity value. Normalization is defined by grayscale variance and mean pixel value analysis as expressed in [6] as :

DOI: 10.31695/IJASRE.2020.33940

$$N(i,j) = f(x) = \begin{cases} M_0 + \sqrt{\frac{v_0(I(i,j)-M)^2}{v_0}} & if\ I(i,j) > M \\ M_0 - \sqrt{\frac{v_0(I(i,j)-M)^2}{v_0}} & otherwise, \end{cases} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Where:

M and V are estimated mean and variance of I(I,j) respectively and M_0 and v_0 are undesired mean and variance value respectively.

c. Segmentation. The normalization process is followed by the separation of the foreground fingerprint image features from the background corresponding to the region outside the border of the fingerprint area which does not contain sufficient identity data information. Segmentation process is required to facilitate a reliable extraction of minutiae. In a fingerprint image processing, the background regions generally exhibit a very low grayscale value and the foreground has very high variance. To normalize the situation, thresholding image segmentation method is introduced. The Segmentation algorithm divide fingerprint image into blocks and grayscale variance is calculated on each block. If the variance of block is less than the global threshold, then the block is assigned to the background image region, otherwise it is assigned to be part of the foreground. The grey-level variance for a block of size WxW is calculated by:

$$\sum v(k) = \frac{1}{w^2} \sum_{j=0}^{w-1} \sum_{j=0}^{w-1} (I(j,i) - M(k))^2 \ldots\ldots\ldots\ldots\ldots\ldots (2)$$

Where:

V (k) is the variance for block k, I (i, j) is the gray level value at pixel (i, j), and M (k) is the Mean gray-level value for the block k.

d. Enhancement. The pattern of ridges and valleys with well-defined frequency and orientation in a fingerprint image provide useful information which helps in removing undesired noise. Gabor filter was appropriately applied because it has both frequency-selective and orientation-selective properties and have optimal joint resolution in both spatial and frequency domains[25]. Therefore, it was appropriate to use Gabor filters as band pass filters to remove the noise and preserve true ridge and valley structures.

e. Binalisation. Image binarization is the process of taking a grayscale image and converting it in to black-and-white, essentially reducing the information contained within the binary image. Binarisation is a type of segmentation and is performed by improving the contrast between the ridges and valleys in a fingerprint image and consequently facilitates the extraction of Minutiae. Consider, an image I (x, y) represent the intensity value of enhanced grayscale image at pixel position (x, y). Let Tp be the global threshold value. In case of fingerprint images Tp represents the imbalance in intensity between the back-ground pixels and ridge pixels. BW(x, y) represent the binary image acquired as expressed in equation 3 below:

$$\mathrm{BW}(\mathrm{x},\mathrm{y}) = \sum_{0\ otherwise}^{1\ if\ I(x,y) \geq TP} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

f. Thinning. Thinning process is a Morphological operation that is used to remove selected foreground pixels from binary images. Thinning operation preserves the topology (extent and connectivity) of the original region while throwing away most of the original foreground pixels. In other words, thinning algorithm usually consist of the iterative removal of the contour until the skeleton is formed. In this study, Stentiford thinning algorithm on window size 3x3 template is employed [37].The application of different algorithm leads to different skeleton sharp. The thinning of an image I by a structuring element J is given as:

$$Thin(i,j) = I - hit\ and\ miss\ (i,j) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (4)$$

g. Feature Extraction. There are two main unique features in a fingerprint image: endings and bifurcations. These features are properly identified from the morphologically thinned fingerprint image. An ending is the end point of a ridge line, while a bifurcation is the junction point of two lines. Ridge ending and bifurcation is what is referred to as minutiae. For matching purposes, minutiae are usually denoted by their type, their location, and the direction of the adjacent ridge. Due to noisy original images and artifacts produced in the Image-Preprocessing stage, spurious minutiae will always be present and normally removed by using empirically determined thresholds. Fingerprint ridge ending and bifurcation are detected with separate algorithm. Using Crossing Number Concept (CN) by Rutovitz. The CN concept is widely used for extracting minutiae in digital fingerprint image and Rutovitz definition of crossing number P is:

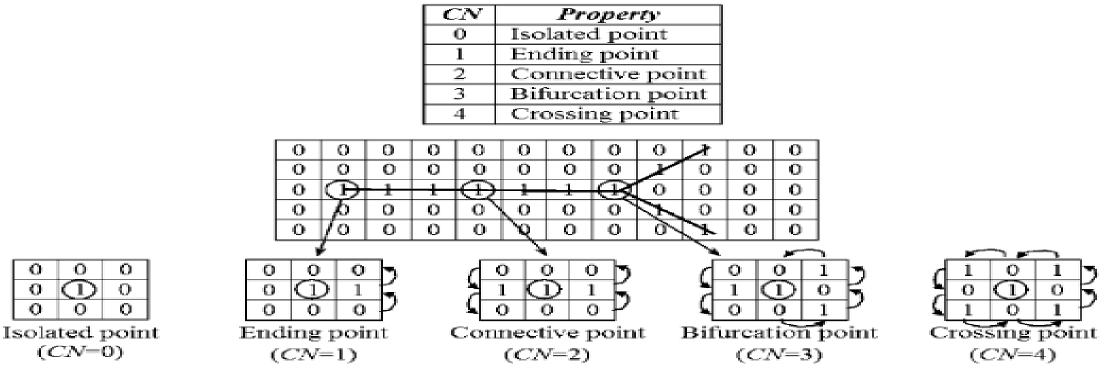
P4	P3	P2

DOI: 10.31695/IJASRE.2020.33940

P5	P	P1
P6	P7	P8

$$CN = \frac{1}{2}\sum_{j=1}^{8} |p_1 \ - p_{1+1}| \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ (5)$$

Where P_1 is the binary pixel value in the neighborhood of P with P_i = (0 or 1) and $P_1 = P_9$. The Skeleton image of fingerprint is scanned and all the minutiae are detected using the properties of CN as illustrated in Figure. 9.1:



CN	*Property*
0	Isolated point
1	Ending point
2	Connective point
3	Bifurcation point
4	Crossing point

Source:[38]

Figure9.1: Crossing Number concept

h. Minutiae Matching. Consider T and I to be the representation of the fingerprint template in the database and sensor input, respectively. Each minutia is considered as a triplet m = {x, y, θ} that indicates the x, y minutia location co- ordinates and the minutia angle θ: T = {m_1, m_2, m_3 ….. m_m}, m_i= {x_i, y_i, $θ_i$} , i=1,2…m $_I$ = {m'_1, m'_2, m'_3 ….. m'_n}, m'_j= {x'_j, y'_j, $θ'_j$ } , j=1,2…n where m and n denote the number of minutiae in T and I, respectively. A minutia m′j in I and a minutia mi in T are considered "matching", if the spatial distance (sd) between them is smaller than a given tolerance r0 and the direction difference (dd) between them is smaller than an angular tolerance θ0[25].

i. Mobile Phone feature Extraction. If fingerprint biometric traits were falsely accepted or rejected, further test are conducted using IMEI or SIM number against identity details stored in the relational database. Otherwise, IMEI and SIM numbers synchronizes with more trusted databases such as GSM or National SIM registration database. By so doing, the correct human identity is retrieved or verified.

6.6.4. Database Analysis and Design

Relational database is used to store human fingerprint bio-identity and mobile phone identification data at the edge server. Information kept in the relational database may include store data, dynamic application settings, parameters and system variables of the proposed access control mechanism. Database design aspect may also include structural design of key entities (objects), attributes, data types, stored procedures, events, queries and the relationships that exist among various database objects. Entity Relationship diagram (ERD) was used to model database requirements. The main components of ERD are entities (things) and their relationships. An entity in [6] is defined as any person, place, thing, or event of interest to an institution or organization about which data are captured, stored, or processed. Figure10.1. shows an ERD of the prototype access Control:

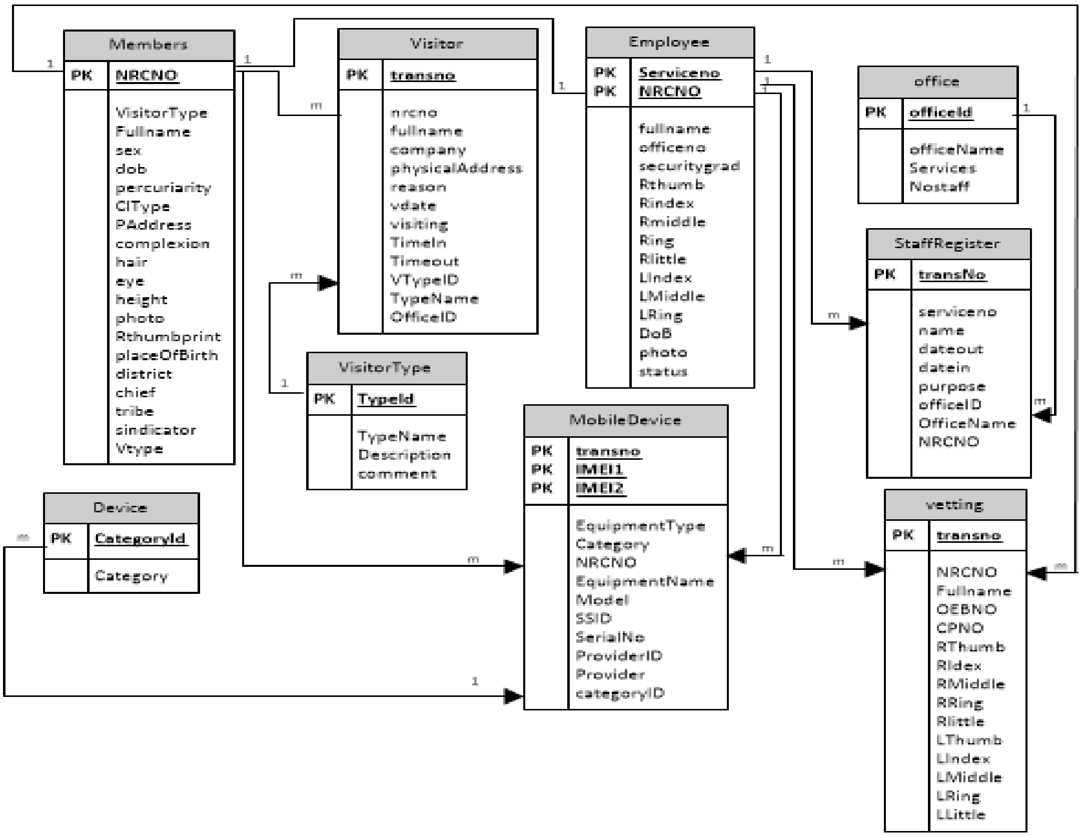


Figure10.1 Entity Relationship Diagram (ERD)

8. RESULTS AND DISCUSSION

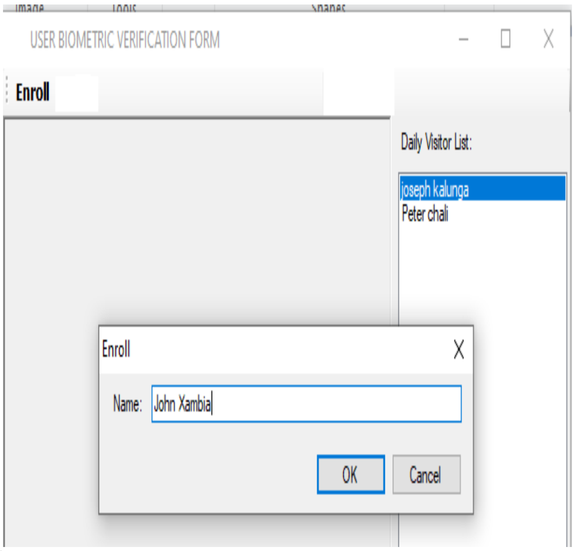
The prototype Industrial IoT Physical Security hardening Access Control mechanism requirements were elicitated, analyzed, modeled, developed, coded and tested. Application testing phase is final stage in adopted xP software development methodology.

8.1. Testing

The test conducted on developed prototype access control mechanism was modular testing. Modular testing was conducted on two modules namely fingerprint and mobile phone identification and authentication module. The main objective of unit testing was to ensure that a section of an application meets its design and intended behavior. The other reason for performing unit testing is to remove software bugs in the developed software module. The snapshots of results were as indicated and explained in screenshot 1 to 9 below:

DOI: 10.31695/IJASRE.2020.33940

1 Visitor Fingerprint Enrollment process

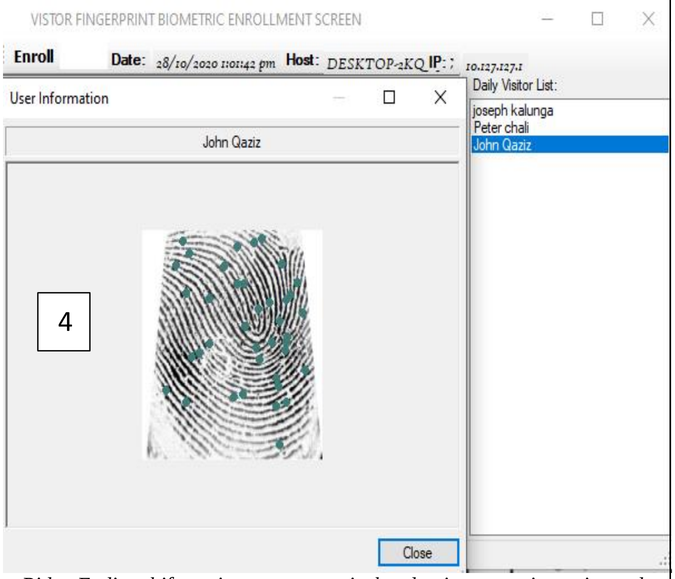


Daily Visitor List: joseph kalunga, Peter chali

Name: John Xambia

Live fingerprint is captured and save in the donor name and appeared in daily visitor list or register.

2 Enrolled Template Identity Features



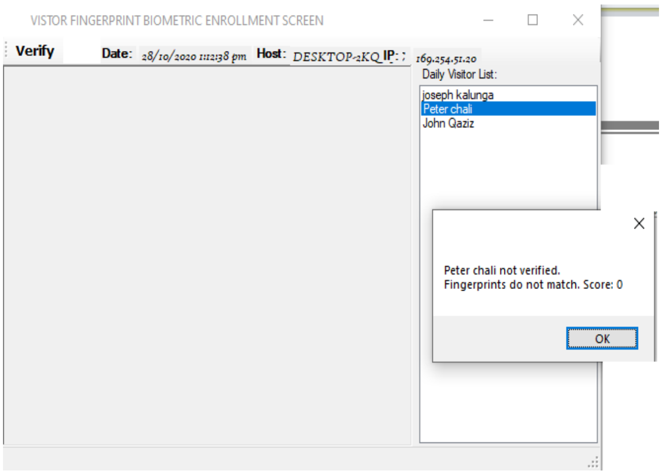
Date: 28/10/2020 1:01:42 pm Host: DESKTOP-2KQ IP: : 10.127.127.1

Daily Visitor List: joseph kalunga, Peter chali, John Qaziz

John Qaziz

Ridge Ending, bifurcation, crossover, isolated points, crossing point and many other fingerprint identity features were highlighted

3 Verification Process (failed Identity Activity)



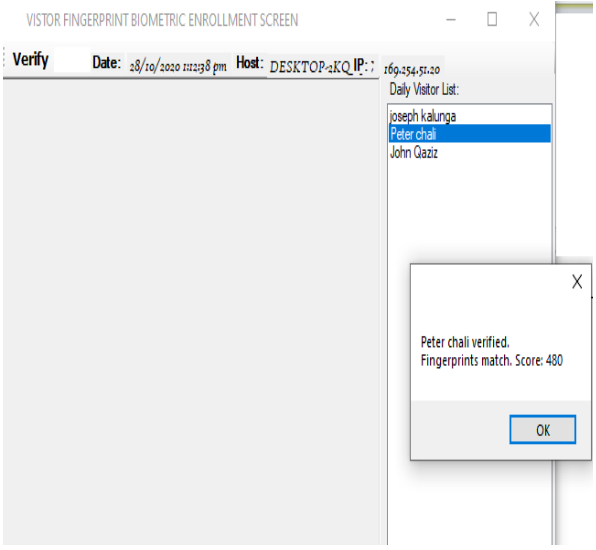
Date: 28/10/2020 1:12:38 pm Host: DESKTOP-2KQ IP: : 169.254.51.20

Daily Visitor List: joseph kalunga, Peter chali, John Qaziz

Peter chali not verified.
Fingerprints do not match. Score: 0

Zero fingerprint matching features detected. Identity process escalated to verification process 5& 6 using donor substative Mobile Phone identies (IMEI1,IMEI2, SIM number or NRC No)

4 Verification Process (Pass Identity Activity)



Date: 28/10/2020 1:12:38 pm Host: DESKTOP-2KQ IP: : 169.254.51.20

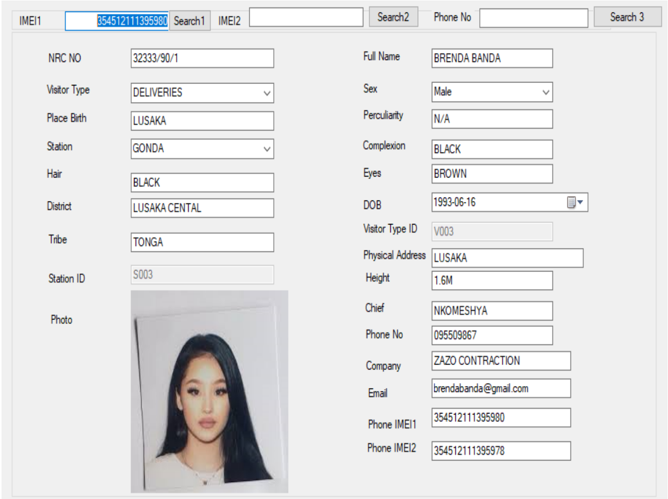
Daily Visitor List: joseph kalunga, Peter chali, John Qaziz

Peter chali verified.
Fingerprints match. Score: 480

480 fingerprint matching features detected. Still Identity process escalated to verification process 5 & 6 using donor substative Mobile Phone identities (IMEI1,IMEI2 or SIM number) to detect false biometric enrollment attacks concerning personal details

DOI: 10.31695/IJASRE.2020.33940

5 Verification Process (passed)



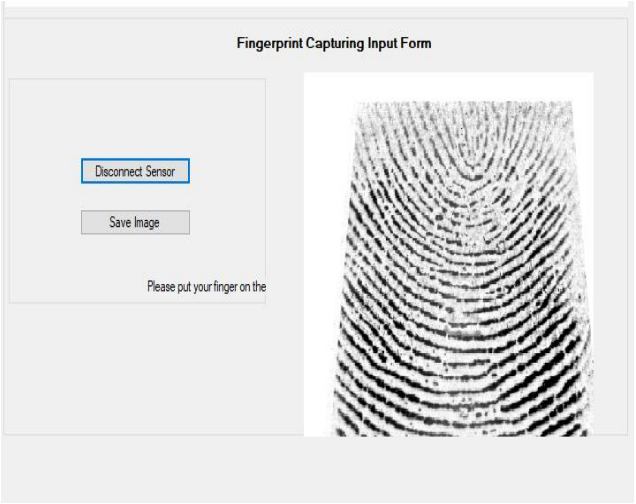
IMEI1 354512111395980 | IMEI2 | Phone No

NRC NO 32333/90/1
Visitor Type DELIVERIES
Place Birth LUSAKA
Station GONDA
Hair BLACK
District LUSAKA CENTAL
Tribe TONGA
Station ID S003

Full Name BRENDA BANDA
Sex Male
Perculiarity N/A
Complexion BLACK
Eyes BROWN
DOB 1993-06-16
Visitor Type ID V003
Physical Address LUSAKA
Height 1.6M
Chief NKOMESHYA
Phone No 095509867
Company ZAZO CONTRACTION
Email brendabanda@gmail.com
Phone IMEI1 354512111395980
Phone IMEI2 354512111395978

Identity verified employing mobile phone identity characteristics (IMEI1, IME12, and SIM Number) otherwise no record retrieved.

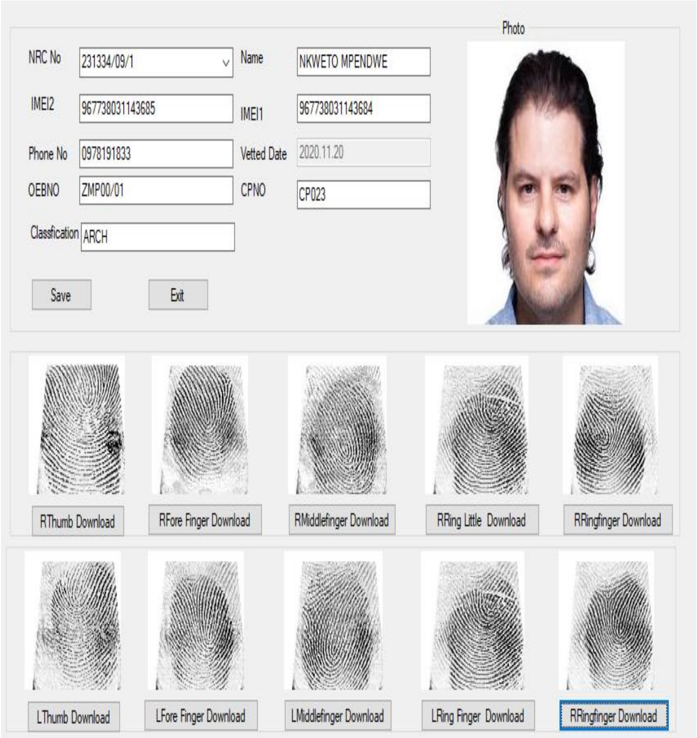
6 Fingerprint Capturing process



Please put your finger on the

Output is Grey image(lot of noise) suitable for security vetting and illiterate business authentication or signature

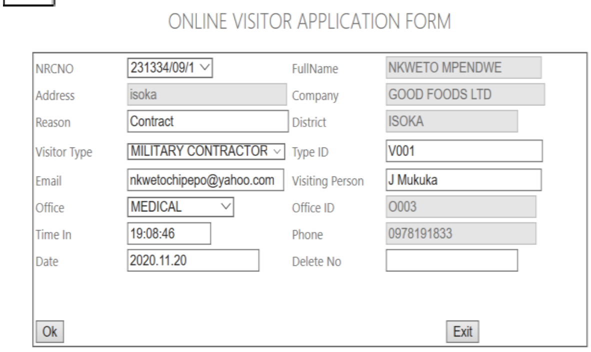
7 Verification Process (passed)



NRC No 231334/09/1
Name NKWETO MPENDWE
IMEI2 967738031143685
IMEI1 967738031143684
Phone No 0978191833
Vetted Date 2020.11.20
OEBNO ZMP00/01
CPNO CP023
Classfication ARCH

Identity confirmation using NRC Number and fingerprint captured during vetting process. Before, that visitor preliminary request is conducted online in stage 8. Otherwise, mobile phone device is checked for stolen status in activity 9

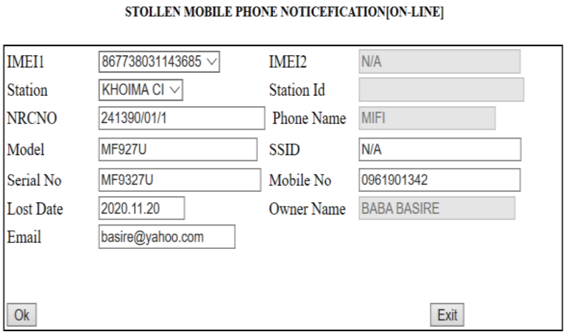
8



ONLINE VISITOR APPLICATION FORM

NRCNO	231334/09/1	FullName	NKWETO MPENDWE
Address	isoka	Company	GOOD FOODS LTD
Reason	Contract	District	ISOKA
Visitor Type	MILITARY CONTRACTOR	Type ID	V001
Email	nkwetochipepo@yahoo.com	Visiting Person	J Mukuka
Office	MEDICAL	Office ID	O003
Time In	19:08:46	Phone	0978191833
Date	2020.11.20	Delete No	

9



STOLLEN MOBILE PHONE NOTICEFICATION[ON-LINE]

IMEI1	867738031143685	IMEI2	N/A
Station	KHOIMA CI	Station Id	
NRCNO	241390/01/1	Phone Name	MIFI
Model	MF927U	SSID	N/A
Serial No	MF9327U	Mobile No	0961901342
Lost Date	2020.11.20	Owner Name	BABA BASIRE
Email	basire@yahoo.com		

Users are encouraged to report stolen phone online using form 9. Once the stolen phone appears on CI network an alert signal is activated for stolen electronic device. When that happens, the case is marked for further investigation.

Screenshot 1 to 9 shows summary findings of various tests on application functionality as per specified requirements. The result indicated that an access control application was developed comprising human identification and authentication using two security layers namely fingerprint biometric and mobile phone identity (IMEM). The first layer involved fingerprint biometric identification and authentication which achieved about 99.9 percent accuracy level. The second layer involved personal mobile phone identity authentication. In absence of topographical errors, personal mobile phone IMIE identity recognition is more accurate and faster than the biometric layer. However, the concept of operation is that, the two security layers support each other with a view to improve security resilience in CI protection. Thereby, maintaining service availability and integrity principles which are more important than confidentiality in Industrial IoT CI security. IMIE identity recognition, however, has disadvantage

DOI: 10.31695/IJASRE.2020.33940

of being transferable. Nevertheless, it can give investigator more tangible information and leads during criminal investigation and examination processes.

8.2. Deployment

The developed Access control application could be deployed at the edge server. Edge server is the powerful computer installed at the “edge” of a given network where data processing is required to happen. Edge servers are physically close to systems that creating the data[39]. In our context, physical access points to Industrial IoT CI environment is where the edge server is deployed. This paradigm is suitable for high security level application deployment because its emphasis is on fast response time and quick decision making. It is also important to note that security principles of availability and integrity are more important in CI protection than confidentiality[13]. Another reason of using edge server paradigm is to offset cloud computing cost. Considering that in Industrial IoT, there are more nodes and data collectors (sensor/actuators) pushing data up into the cloud than ever. Pushing unfiltered data to cloud involves sending and storing huge volumes of data to the cloud even those data, we will not use. Therefore, deploying physical access control hardening application at the edge server may reduce cost in terms of both transfer fees as well as cloud storage fees.

9.0 . CONCLUSIONS CONTRIBUTION AND FUTURE WORKS

In this work, we have developed an access control mechanism for industrial IoT CI protection based on fingerprint biometrics and mobile phone IMEI. To achieve this, we employed cheaper fingerprint sensors, mobile phone, open source fingerprint System Development Kit (SDK), visual studio 2010 on C# platform and MySQL database. The literature was reviewed on related products and services involving CI protection. To model this application rich picture, Use case diagram, activity diagram, DFDs, ERD and context diagram were employed. The Use case diagram defined users, roles, processes and their relationships. Context diagrams showed how the developed access control mechanism fitted into the context of the people and the CI institution security as the whole. While activity diagram illustrated business case and DFD detailed the logical flow of information in the system. For example, data flow diagram helped us to understand how digital image processing is done. It involved various stages of fingerprint template creation and mobile phone identities extraction. Furthermore, the study also revealed that definitions, architecture and application of industrial IoT CI protection were broad, contextual based and has no predefined standard and architecture. It is dependent on problem context. On results, the developed application has abilities to verify human true identity based on fingerprints, mobile phone IMEI and SIM number. Furthermore, the developed system has abilities to store information suitable for conduct forensics and digital investigations on CI places and installation.

9.1. Future Works

The following are the research recommendations:

a. Further research is needed in developing Physical security hardening mechanism to control natural causes such as extreme high/low temperatures, fire, water poisonous gases armful to existence of Industrial IoT elements (human, devices, installations or infrastructure).
b. Further research is needed to fight IoT Sensor devices heterogeneous problem.
c. Further research in Data privacy Issues affecting practical Industrial IoT application.
d. Future works towards addressing biometrics Hacking Concerns. It is fairly easy for sophisticated hackers to get a hold of a person’s biometric markers. On internet, there malicious individuals that have created fake fingerprints through high-resolution images. Even highly secured apple’s TouchID was successfully hacked with less effort [42]. Hence, there is need for further works to solve hacking concerns.
e. Further works are needed to find modalities of maintaining integrity of compromised fingerprint biometric template since biometric template when compromised cannot be changed or altered like password.

DOI: 10.31695/IJASRE.2020.33940

f. Further research is need in development of contactless fingerprint sensors to avoid spread of contact virus such as deadly corona virus. Modern fingerprint sensors are contact based and hence, fingerprint sensor is among the technologies whose existence is threatened by corona virus era.

REFERENCES

[1] J. Kalunga, "INTEGRATING FINGERPRINT BIOMETRICS SYSTEM INTO THE MILITARY POLICE DATABASE," University of Zambia, 2015.

[2] E. Ferrara, "Detecting criminal organizations in mobile phone networks," no. November 2017, 2014,

[3] South University, "Fighting Crime with Mobile Technology," *CRIMINAL JUSTICE*, 2016. [Online]. Available: https://www.southuniversity.edu/news-and-blogs/2016/08/fighting-crime-with-mobile-technology-137309#:~:text=Crimes Using Cell Phones,every day on mobile devices. [Accessed: 06-Nov-2020].

[4] G. Lampropoulos, K. Siakas, and T. Anastasiadis, "Internet of Things (IoT) in Industry: Contemporary Application Domains, Innovative Technologies and Intelligent Manufacturing," *Int. J. Adv. Sci. Res. Eng.*, vol. 4, no. 10, pp. 109–118, 2018.

[5] U. P. D. Ani, H. M. He, and A. Tiwari, "Review of cybersecurity issues in industrial critical infrastructure : manufacturing in perspective," *J. Cyber Secur. Technol.*, vol. 1, no. 1, pp. 32–74, 2017, doi: 10.1080/23742917.2016.1252211.

[6] J. Kalunga and S. Tembo, "Development of Fingerprint Biometrics Verification and Vetting Management System," *Am. J. Bioinforma. Res.*, vol. 6, no. 3, pp. 99–112, 2016.

[7] R. Belguechi, E. Cherrier, V. Alimi, P. Lacharme, and C. Rosenberger, "An Overview on Privacy Preserving Biometrics," *Recent Appl. Biometrics*, no. July, 2011, doi: 10.5772/19338.

[8] V. Patel, "Airport Passenger Processing Technology : A Biometric Airport Journey AIRPORT PASSENGER PROCESSING TECHNOLOGY : A BIOMETRIC AIRPORT JOURNEY by A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Cybersecuri," 2018.

[9] R. V Yampolskiy, *Taxonomy of Behavioural Biometrics*, no. January. 2009.

[10] Umberto Bacchi, "Landmark UK court ruling finds police use of facial recognition unlawful," *Reuter*, 2020. [Online]. Available: https://www.reuters.com/article/us-britain-tech-privacy-idUSKCN2572B8. [Accessed: 23-Nov-2020].

[11] C. Burt, "Legal issues around facial biometrics use examined in U.S., Canada, and UK," *Feb 3, 2020*, 2020. [Online]. Available: https://www.biometricupdate.com/202002/legal-issues-around-facial-biometrics-use-examined-in-u-s-canada-and-uk. [Accessed: 23-Sep-2020].

[12] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "Security and accuracy of fingerprint-based biometrics: A review," *Symmetry (Basel).*, vol. 11, no. 2, 2019..

[13] J. Kalunga, S. Tembo, and J. Phiri, "Industrial Internet of Things Common Concepts , Prospects and Software Requirements," vol. 9, no. 1, pp. 1–11, 2020.

[14] T. Dudziak, "eXtreme Programming An Overview," 2000.

[15] K. Dragerengen, "Access Control in Critical Infrastructure Control Rooms using Continuous Authentication and Face Recognition," no. June, 2018.

[16] S. Singh and S. V. A. V. Prasad, "Techniques and challenges of face recognition: A critical review," *Procedia Comput. Sci.*, vol. 143, pp. 536–543, 2018, doi: 10.1016/j.procs.2018.10.427.

[17] A. Baina, A. Abou, E. Kalam, and Y. Deswarte, "Chapter 14 COLLABORATIVE ACCESS CONTROL FOR CRITICAL INFRASTRUCTURES," vol. 290, pp. 189–201.

[18] S. Etigowni, D. J. Tian, and K. Butler, "CPAC : Securing Critical Infrastructure with Cyber-Physical Access Control," pp. 139–152.

[19] L. Bormane, J. Gržibovska, S. Bērziša, and J. Grabis, "Impact of Requirements Elicitation Processes on Success of Information System Development Projects," *Inf. Technol. Manag. Sci.*, vol. 19, no. 1, pp. 57–64, 2017.

[20] S. Bell and S. Morse, "Rich pictures: A means to explore the 'sustainable mind'?," *Sustain. Dev.*, vol. 21, no. 1, pp. 30–47, 2013.

[21] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial internet of things (IIoT): An analysis framework," vol. 101, no. April, pp. 1–12, 2018.

[22] D. M. L. Storisteanu, T. L. Norman, A. Grigore, and A. B. Labrique, "Can biometrics beat the developing world's challenges?," *Biometric Technol. Today*, vol. 2016, no. 11, pp. 5–9, 2016.

[23] G. Association, "MOBILE IDENTITY ENABLING THE," *IDENTITY*, no. IDENTITY, 2020.

[24] M. S. Obaidat, I. Traore, and I. Woungang, *Biometric-Based Physical and Cybersecurity Systems*, no. October. 2018.

[25] A. S. Chaudhari, G. K. Patnaik, and S. S. Patil, "Implementation of Minutiae Based Fingerprint Identification System Using Crossing Number Concept," *Inform. Econ.*, vol. 18, no. 1/2014, pp. 17–26, 2014.

DOI: 10.31695/IJASRE.2020.33940

[26] I. M. Alsaadi, “Physiological Biometric Authentication Systems Advantages Disadvantages And Future Development A Review,” *Int. J. Sci. Technol. Res.*, vol. 4, no. 8, pp. 285–289, 2015.

[27] C. S. Koong, T. I. Yang, and C. C. Tseng, “A User Authentication Scheme Using Physiological and Behavioral Biometrics for Multitouch Devices,” *Sci. World J.*, vol. 2014, 2014.

[28] A. A. Mehta and A. A. Mehta, “Study of Fingerprint Patterns in Type Ii Diabetes Mellitus,” *Int. J. Anat. Res.*, vol. 3, no. 2, pp. 1046–1048, 2015.

[29] J. a. Unar, W. C. Seng, and A. Abbasi, “A review of biometric technology along with trends and prospects,” *Pattern Recognit.*, vol. 47, no. 8, pp. 2673–2688, 2014.

[30] B. Biometrics, A. Alzubaidi, and J. Kalita, “Authentication of Smartphone Users Using,” pp. 1–32, 2015.

[31] A. Lanitis, “A survey of the effects of aging on biometric identity verification A Survey of the Effects of Aging on Biometric Identity Verification,” no. January 2010, 2014.

[32] N. Sarfraz, “Adermatoglyphia: Barriers to Biometric Identification and the Need for a Standardized Alternative,” *Cureus*, vol. 11, no. 2, 2019.

[33] N. Nguyen, “Chokepoint: Regulating US student mobility through biometrics,” *Polit. Geogr.*, vol. 46, pp. 1–10, 2015.

[34] Chris Britton & Roberts. S Seiner, “Data Management and Context Modeling,” : *DATAVERSITY Education, LLC*, 01-Jan-2007.

[35] GeeksForGeens, “Unified Modeling Language (UML) | Activity Diagrams,” *GeeksForGeens*, 2018. [Online]. Available: https://www.geeksforgeeks.org/unified-modeling-language-uml-activity-diagrams/. [Accessed: 10-Sep-2020].

[36] M. I. Aririguzo, F. P. Nekede, and F. P. Nekede, “Mobile phone registration for a developing econom y: gains and constraints,” vol. 3, no. 3, pp. 44–52, 2016.

[37] P. Subashini and S. Jansi, “Optimal Thinning Algorithm for detection of FCD in MRI Images,” vol. 2, no. 9, pp. 1–7, 2011.

[38] F. Zhao and X. Tang, “Preprocessing and postprocessing for skeleton-based fingerprint minutiae extraction,” no. April, 2007, doi: 10.1016/j.patcog.2006.09.008.

[39] GSMA, “Opportunities and Use Cases for Edge Computing in the IoT,” 2018. [Online]. Available: https://www.gsma.com/iot/wp-content/uploads/2018/11/IoT-Edge-Opportunities-c.pdf. [Accessed: 22-Nov-2020].

DOI: 10.31695/IJASRE.2020.33940