A TRUST MODEL FOR CONTEXT-AWARE E-HEALTH SERVICES

BRENDA MARTHA AYUKU CHITERI

MASTER OF SCIENCE

(Computer Systems)

JOMO KENYATTA UNIVERSITY

OF

AGRICULTURE AND TECHNOLOGY

2023

A Trust Model for Context-Aware E-Health Services

Brenda Martha Ayuku Chiteri

A Thesis Submitted in Partial Fulfilment of the Requirements for the Degree of Master of Science in Computer Systems of the Jomo Kenyatta University of Agriculture and Technology

2023

DECLARATION

This thesis is my original work and has not been presented for a degree in any other university

Signature……………………………………………Date……………………………..

Brenda Martha Ayuku Chiteri

This thesis has been submitted for examination with our approval as the university supervisors.

Signature……………………………………………Date……………………………..

Dr. George Okeyo, PhD

Carnegie Mellon University Africa

Signature……………………………………………Date……………………………..

Dr. Geoffrey Wekesa Chemwa, PhD

JKUAT, Kenya

Signature……………………………………………Date……………………………..

Dr. Agnes Mindila, PhD

JKUAT, Kenya

ACKNOWLEDGEMENT

I would like to acknowledge and thank my supervisors Dr. Okeyo, Dr. Chemwa and Dr. Mindila. They have walked with me throughout this journey, providing guidance and support. In addition, I would like to express gratitude to my family, friends, and classmates for their support.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

ABSTRACT

With the rapid advancement of technology, context-aware services, ubiquitous technology, and pervasiveness, systems have revolutionized the healthcare sector, offering substantial benefits. Context-aware e-health services have emerged as a promising solution to enhance patient healthcare by continuously monitoring their health status and providing timely assistance during medical emergencies. However, the seamless monitoring of patients' context and health information gives rise to concerns regarding privacy and trust, particularly in terms of ensuring the reliability, integrity, and authenticity of authorized users accessing sensitive patient information. The primary objective of this thesis is to address these concerns and establish a secure trust model for handling patients' contextual and health information, while simultaneously fostering trust among patients, medical personnel, and administrators. The proposed trust model serves as a robust approach to evaluating trust in the context of e-health services. By considering key trust factors such as privacy, reliability, credibility, and transparency the model enables users to make informed decisions when choosing medical personnel. It also employs a well-defined computation formula to cultivate trust within the context-aware e-health ecosystem. The computation results of the proposed model outperform other Trust-Based Personalized Service models, the model obtained a precision of 1.0. Furthermore, the integration of blockchain technology further enhances the security and integrity of the system, ensuring that sensitive patient information remains tamper-proof and protected from unauthorized access. This trust model significantly contributes to the advancement of trust models in the context-aware e-health domain, facilitating improved user experiences and promoting the wider adoption of context-aware e-health services.

Keywords: Trust, context-aware services, e-health, privacy, context.

CHAPTER ONE

INTRODUCTION

1.1 Background Information

The World Health Organisation (WHO) defines health services as the services dealing with the diagnosis and treatment of disease or the promotion, maintenance, and restoration of health. They include personal and non-personal health services (Integrated Health Services , 2023). These services are the most visible functions of any health system, both to users and to the public (Tedros Adhanom Ghebreyesus, 2019). To improve healthcare services the health sector has adopted the use of technology to help in the treatment, diagnosis, and monitoring of patients. This has led to the widespread adoption of e-health (Ayuku, Okeyo, Mindila, & Chemwa, 2021).

E-health has increased efficiency through better retention and retrieval of records, better management of chronic diseases, shared health professional staffing, reduced travel times, and fewer or shorter hospital stays. The government of Kenya has been at the forefront of promoting e-health in the country, with the aim of improving the quality, accessibility, and affordability of healthcare services (Onyancha & et.al, 2020). Some of the initiatives that the government has implemented include the establishment of the National Health Information System (NHIS) and the deployment of mobile clinics to provide healthcare services in remote areas. The NHIS is an integrated health information system that provides a platform for healthcare providers to manage patient records, track disease outbreaks, and monitor health indicators in real-time. The system is connected to various health facilities across the country, making it easier for health workers to access patient records and share information (Bernadette, Anthony, Ngaira, & Pepela, 2019).

Mobile clinics, on the other hand, have been used to provide healthcare services to populations living in remote areas that lack access to health facilities. These clinics are equipped with telemedicine tools that enable health workers to consult with specialists in real-time, thereby improving the quality of care. Other private sector players such as Safaricom, the largest mobile network operator in Kenya, have also played a significant role in promoting e-health in the country. Safaricom has partnered with various healthcare providers to develop mHealth solutions such as M-TIBA, a mobile health wallet that enables users to pay for healthcare services using their mobile phones (Kwereba & Shah, 2022). Apart from payments the mobile health (mHealth) services have been developed in Kenya to improve healthcare access and delivery in remote and underserved areas. These services include mobile-based health information systems, appointment reminders, and telemedicine consultations. The use of context-aware mHealth services has been shown to improve patient engagement, increase access to care, and reduce healthcare costs.

The emergence of e-health and m-health services have enabled the development of context-aware health services. Context-awareness is a key concept in e-health that refers to the ability of digital health technologies to adapt to the specific context or situation of the user (Wan, Chieng, & Ho, 2018). Context-awareness in e-health involves capturing, interpreting, and utilizing the context information of the user to facilitate and improve the effectiveness and efficiency of health care delivery (Gubert, da Costa, & Righi, 2020). Context information can include a range of factors such as the patient's location, health status, medical history, preferences, and the healthcare provider's expertise and resources. Leveraging context information, context-aware e-health applications can provide tailored and personalized healthcare services that meet the unique needs of each patient.

For instance, a context-aware m-health application could use the patient's location data to recommend nearby healthcare facilities or pharmacies. A context aware e-health system could present relevant patient data to the healthcare provider based on the patient's medical history and current symptoms. One example of a context-aware e-health system is the m-Diabetes program in India. The program uses a context-aware mobile health application to support diabetes self-management among individuals in India, where diabetes is a growing health concern. The application leverages various context information, such as the user's location, activity level, and diet, to provide personalized health recommendations and support. For example, the application sends reminders to users to take their medication or engage in physical activity based on their location and activity level. It also provides nutritional advice based on the user's dietary preferences and restrictions. The m-Diabetes program has shown promising results in improving diabetes self-management among participants, including increased medication adherence and improved glycaemic control. The success of the program highlights the potential of context-aware e-health technologies to improve healthcare outcomes and address global health challenges (Kim, Lee, & Lee, 2018).

Another example of a context-aware healthcare system is the "Ambient Assisted Living" (AAL) system. AAL is a technology-enabled system designed to assist elderly individuals in performing daily activities and managing their health conditions. The system uses various sensors and other technologies to collect data on the user's context, such as their location, activity level, and vital signs. The system then uses this information to provide personalized recommendations and support, such as reminders to take medication or alerts for emergency situations. The "Personal Health Assistant" (PHA) system is another example. PHA is a mobile health application designed to provide personalized health recommendations and support to individuals with chronic conditions. The system uses context information, such as the user's location, activity level, and social context, to provide tailored recommendations on medication adherence, physical activity, and diet (Siddiqui, S. S., & Sheikh, 2020).

These examples highlight the potential of context-aware healthcare systems to improve healthcare outcomes and address the growing challenges of an aging population and increasing chronic disease prevalence. The use of context-aware e-health technologies maximum as the potential to improve healthcare access and delivery, enhance patient outcomes, and reduce healthcare costs. However, it also raises important ethical, trust, security, and privacy concerns, particularly around the collection and use of sensitive health information (Ayuku, Okeyo, Mindila, & Chemwa, 2021).

These concerns are particularly significant in the context of health services, where sensitive personal information is involved. As context-aware systems are designed to collect, process, and use large amounts of personal data, it is important to ensure that this data is protected and used appropriately.

One of the main concerns about context-aware health services is the potential for misuse of personal data. There is a risk that personal data may be used for purposes other than those for which it was collected, or that it may be shared with unauthorized parties. This could lead to breaches of privacy and confidentiality, as well as reputational damage for both individuals and organizations.

Another concern is the potential for bias in the design and implementation of context-aware health services. If these systems are not designed with fairness and inclusivity in mind, they may perpetuate existing health inequalities or even exacerbate them. This could result in unequal access to health services, unequal health outcomes, and discrimination against certain groups.

Furthermore, trust is an essential component of successful health services, and context-awareness may raise trust issues. Patients need to trust that their data is being used ethically and that their privacy is being respected. They also need to trust that the advice and recommendations they receive from context-aware systems are accurate, unbiased, and in their best interests.

1.2 Problem statement

As context-aware e-health services become more prevalent, the need for trust models that can effectively manage user privacy and security concerns becomes increasingly important. Existing trust models do not adequately address the unique challenges of context-aware e-health services. Therefore, there is a need for a trust model that can effectively address the privacy and security concerns of context-aware e-health services. These concerns include data integrity, end user privacy and confidentiality. When a patient’s information is accessed by unauthorised personnel it can be deleted, distorted, or used for criminal activities like identity theft, blackmail, user tracking etc. Due to these reasons, it is important for patients to trust the systems they are interacting with. They should have the power to decide the context information they want to provide and have the capability to verify the integrity of the context information. The trust model in this thesis proposes ways of addressing the privacy and security issues to enhance trust (Ayuku, Okeyo, Mindila, & Chemwa, 2021).

1.3 Research Objectives

Our main objective is to formulate a trust model that protects the patients’ privacy and establish a high level of trust for users using the context-aware e-health services (Ayuku, Okeyo, Mindila, & Chemwa, 2021).

1.3.1 Specific Objectives

1. To identify and analyses trust concerns related to the privacy, security, and reliability of context-aware e-health services, specifically focusing on the access and handling of patients' contextual and health information.
2. To conduct a comprehensive review and analysis of existing trust models with an emphasis on their applicability to context-aware systems. Evaluate their strengths and limitations to establish a solid foundation for the development of the proposed trust model.
3. To formulate a trust model by integrating insights and elements derived from existing trust models and incorporating the use of blockchain technology to enhance security and integrity.
4. To evaluate and measure the effectiveness and efficiency of the trust model in 3 by conducting experiments and simulations to assess its ability to maintain and enhance trust in context-aware e-health services, considering factors such as trustworthiness, privacy preservation, data security, and system reliability.

1.3.2 Research Questions

1. What are the key trust concerns related to the privacy, security, and reliability of context-aware e-health services, particularly in terms of accessing and handling patients' contextual and health information?
2. What are the strengths and limitations of existing trust models in the context of context-aware systems? How applicable are these models to address the trust concerns in context-aware e-health services?
3. How can insights and elements from existing trust models be integrated to formulate a comprehensive trust model specifically tailored for context-aware e-health services? How can the incorporation of blockchain technology enhance the security and integrity of the trust model?
4. To what extent does the developed trust model effectively and efficiently maintain and enhance trust in context-aware e-health services? How does it address trustworthiness, privacy preservation, data security, and system reliability?

1.4 Scope of the study

This research project aims to explore and establish trust within the context-aware eHealth services. The primary focus is on analysing the contextual factors that play a crucial role in context-aware services, including the users of the service (patients and medical personnel), the location of service users, the type of service requested, the time aspect, and the reasons for monitoring patients. The research methodology involves conducting a comprehensive literature review, developing a robust trust model specifically tailored for context-aware services in the healthcare sector, implementing the model, and rigorously evaluating its effectiveness. The scope is specifically limited to formulating a trust model for context-aware services within the healthcare industry, ensuring a focused and in-depth analysis of trust dynamics in this domain.

1.5 Dissertation significance and contributions

The research work aims to address the main objective of formulating a trust model that ensures the privacy of patients and establishes a high level of trust among users of context-aware e-health services. By developing and implementing this trust model, the research contributes to safeguarding patient privacy and promoting trust in the context-aware e-health ecosystem. This is crucial for encouraging the adoption and utilization of e-health services, as users can have confidence in the security and reliability of their personal health information. The proposed framework provides a robust approach to evaluating trust, considering key factors such as privacy, reliability, credibility, and transparency. Through the integration of blockchain technology, the research further enhances the security and integrity of the system, protecting sensitive patient data from unauthorized access and tampering. Overall, this research work significantly advances the field of trust models in the context-aware e-health domain, promoting improved user experiences and facilitating the wider adoption of context-aware e-health services.

1.6 Outline of the Thesis

This thesis is organized as follows: chapter 1 introduction, this chapter provides the background of the research, formulation of problem, research objectives and questions. Chapter 2 is the literature review it explains the health services in Kenya, it describes context, context awareness, blockchain and the existing trust models. Chapter 3 is the methodology it explains how the trust model is implemented and the evaluation of the model. Chapter 4 presents and discusses the results of the trust model evaluation conducted in chapter 3 and finally chapter 5 is the conclusion it gives a summary of the thesis and the future work to be done.

CHAPTER TWO

LITERATURE REVIEW

This chapter focuses on understanding health services, context awareness, blockchain, trust and privacy models. We review existing literature on trust models, health services, context-awareness and the technologies enabling context aware systems and blockchain.

2.1 Kenya's Healthcare System

Kenya is a lower-middle income country located in the East African region. Kenya's healthcare system is a complex web of public and private providers, ranging from community health workers to tertiary care hospitals (Odhiambo, 2015). Figure 2.1 illustrates the health care system in Kenya.

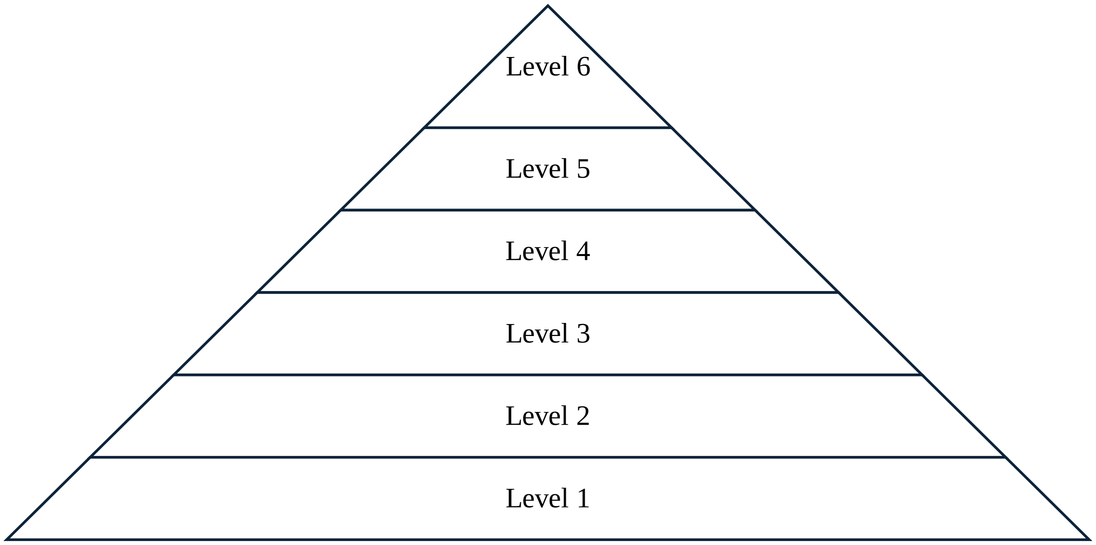


Figure 2.1: The Kenyan Health System

Kenya's health system consists of different levels of care, level 6 are the national referral hospitals, providing specialized and advanced treatments. Level 5 are the provincial referral hospitals, serving specific regions with comprehensive healthcare. Level 4 are the district and sub-district referral hospitals, offering general medical care and diagnostics.

Level 3 are the health centres and level 2 are the dispensaries, providing primary healthcare services to communities. Lastly, level 1 are the community centres they focus on health promotion and disease prevention through outreach programs.

The Kenyan health system is underfunded and faces numerous challenges, including inadequate infrastructure, limited access to essential medicines and supplies, a shortage of trained healthcare workers, and high rates of poverty and disease burden. The government of Kenya has prioritized healthcare in its development agenda, with a goal of achieving universal health coverage. In recent years, the government has made significant investments in healthcare infrastructure, including the construction of new hospitals and clinics, as well as the deployment of technology solutions to improve healthcare delivery.

Despite these efforts, challenges remain in providing equitable access to quality healthcare for all Kenyans. The country continues to face significant health challenges, including high rates of maternal and child mortality, HIV/AIDS, malaria, and non-communicable diseases such as cancer and diabetes (Ministy of Health & Ministry of Public Health Sanitation, 2012).

Context-aware e-health services have the potential to transform the healthcare landscape in Kenya by improving access to care, enhancing the quality of care, and reducing healthcare costs. However, the successful implementation of these services depends on the development of robust trust models that address the unique challenges of the Kenyan context.

2.1.1 Health services in Kenya

Health services include all services dealing with the diagnosis and treatment of disease, or the promotion, maintenance, and restoration of health. They include personal and non-personal health services. Health services are the most visible functions of any health system, both to users and to the public. Service provision refers to the way inputs such as money, staff, equipment, and drugs are combined to allow the delivery of health interventions. Improving access, coverage and quality of services depends on these key resources being available, on the ways services are organized and managed, and on incentives influencing providers and users (World Health Organization & World Bank Group, 2018).

Kenya provides a range of health services to its citizens. The healthcare system is divided into four levels: primary, county, regional, and national. The primary healthcare level is the first point of contact for most Kenyans, and it is made up of dispensaries and health centres. The county level is responsible for implementing health policies and is made up of county hospitals and referral hospitals. The regional level consists of specialized hospitals that provide tertiary care, while the national level consists of national referral hospitals these include Moi Teaching and Referral Hospital and Kenyatta National Hospital.

The government plays a major role in providing healthcare services, but the private sector also contributes significantly. Private hospitals and clinics provide services that are complementary to those provided by the government, and they serve as an alternative for those who can afford to pay for healthcare.

2.1.2 E-health in Kenya

E-health is the means of ensuring that the right health information is provided to the right person at the right place and time in a secure, electronic form to support the delivery of quality and efficient healthcare. E-health is a generic expression to refer to any form of Information Technology enabled health system reform (Kilwake et al. 2012). It encompasses a wide range of activities such as telemedicine, electronic health records, mobile health, and health information systems.

In recent years, the Kenyan government has been making efforts to embrace e-health as a means of improving healthcare delivery and access to health services in the country. In April 2011 the Kenyan e-health strategy was developed, the purpose of the 2011 strategy is to ensure achievement of Vision 2030. The overall goal of Vision 2030 in health is to have equitable and affordable healthcare at the highest achievable standard to all citizens both in the rural and urban areas (Obosi, 2019).

One of the most significant e-health initiatives in Kenya is the National Hospital Insurance Fund (NHIF) scheme, which is a government-sponsored health insurance program that covers medical expenses for Kenyan citizens. NHIF has launched a mobile platform that enables members to access health services and information through their mobile phones (Barasa, Rogo, Mwaura, & Chuma, 2018).

Another notable e-health initiative in Kenya is the use of telemedicine to provide healthcare services in remote areas. This involves the use of video conferencing and other communication technologies to enable healthcare providers in urban areas to consult with patients and healthcare providers in rural areas (Zalo, 2020). This has the potential to significantly improve access to healthcare services in rural areas where there is a shortage of healthcare professionals. Overall, e-health in Kenya has the potential to transform the healthcare system and improve access to health services for all Kenyans.

2.1.3 Trust in healthcare systems

Trust in healthcare systems is fundamental for efficient healthcare delivery, patient satisfaction, and positive health outcomes (Katarzyna Krot, 2021). It forms the basis of the patient-provider relationship and has a significant impact on various aspects of healthcare, including patient adherence to treatment plans, satisfaction with care, and willingness to disclose sensitive information (Baker, 2020) . During the COVID-19 pandemic, trust in e-health services became increasingly significant. The rapid development and adoption of telemedicine and other e-health technologies have provided remote healthcare options, offering convenience, access to specialty care, and improved monitoring of treatment (Aneka, Jeremy, & Laura, 2020). However, ensuring trust in these services has emerged as a critical consideration. Altinisik et al. (2022) in their research show that patients' trust in telemedicine can be influenced by factors such as accessibility, service quality, and the presence of pre-established relationships with healthcare providers (Altinisik, et al., 2022). Patients are more likely to trust telemedicine when it is easily accessible and when they perceive the services to be of high quality. Furthermore, cultural backgrounds and previous experiences with healthcare play a role in shaping individuals' trust in technology and their willingness to adopt e-health services (Chew, et al., 2023). To foster trust in healthcare systems, it is essential to address these factors and ensure that e-health services are accessible, provide high-quality care, and consider patients' cultural backgrounds and experiences. By prioritizing these elements, healthcare providers and policymakers can build trust in telemedicine and other e-health technologies, thereby enhancing patient satisfaction, improving health outcomes, and promoting the widespread adoption of remote healthcare solutions.

2.2 Context Awareness

Dey defines context as any information that describes the condition of a person or object (Dey, 2001). Context is categorised as *why, what, when, where, and who*, *who* describes the person, *where* is their location, the *why* is the reason we are monitoring the patients' health status which is to enhance and provide better health care. *When* is the time, which is important especially when ensuring only authorized personnel have access and we are tracking their time zones when we are checking if a healthcare facility near a patient is open in the event it does not operate for 24 hours or scheduling an appointment with a doctor is required. The *how* is the kind of service the patient is offered (Wigmore, 2016).

Context awareness is the capability of systems or applications to collect data about its environs and adapt based on the situation, for example, a device should mute all calls and notifications when a user is in a meeting. Sensors, trackers, camera, and smart devices collect contextual data. Context-aware applications and systems collect data through these sources and react depending on the rules set (Wigmore, 2016) and (Santhiyagu, Kumar, & Prabhu, 2017).

In Kenya, there is a growing interest in developing context-aware services, particularly in the healthcare sector, to improve the quality and accessibility of healthcare services. One example of context-awareness in Kenya's healthcare system is the use of mobile health (mHealth) applications that can collect and analyse patient data in real-time. These applications can adapt to the patient's specific health needs, location, and other contextual factors, enabling healthcare providers to deliver more personalized and effective care. Another example is the use of wearable devices and sensors to monitor patients remotely. These devices can collect and transmit data on a patient's vital signs and other health indicators, allowing healthcare providers to monitor patients in real-time and intervene quickly if necessary.

Overall, context-awareness has the potential to transform healthcare in Kenya by enabling healthcare providers to deliver more personalized and effective care, improve patient outcomes, and reduce healthcare costs.

2.3 Context-Aware e-Health Services and Applications

Context–Awareness is a concept and the technologies such as sensors, wearable instruments, intelligent artefact’s, handheld computers etc. are available for the development of the new application, which will enable the health care professionals to manage their tasks, and it will increase the quality of the patient care (Shankari, Saravanagru, & Thangavelu, 2011). Context-aware systems are also known as pervasive or ubiquitous systems. These systems offer personalized health services. They monitor patients as they maintain their normal everyday activities, to warn the patients or healthcare providers of problems as well as collecting data for trend analysis and medical research. The continuous monitoring of the health status provides better diagnosis, treatment, and emergency services (Gelogo & Kim, 2015).

2.3.1 Pathogen Outbreak Prevention Instruction System (PORPOISE)

The PORPOISE system was designed by Tortorella and Kirshuk to provide medical training information to the end-user/learner on the spread of potential pathogens present within the system’s proximate environment (Tortorella & Kinshuk, 2017). It is a mobile context-aware medical training system aims to reduce the transmission of pathogens by providing training and guidance to healthcare professionals in real-time. This system utilizes mobile technology and context-awareness to deliver personalized and relevant information based on the user's specific situation and environment. The system leverages the capabilities of mobile devices to gather contextual information such as location, time, and environmental conditions. This information helps tailor the training content to the user's specific context, ensuring its relevance and applicability. It provides comprehensive training on the transmission of pathogens, including information on common pathogens, modes of transmission, and preventive measures. This training content is designed to enhance the user's knowledge and understanding of pathogen transmission dynamics. The system continuously monitors and analyses real-time data from various sources, such as local healthcare facilities, public health agencies, and research institutions. This allows it to provide up-to-date information on emerging pathogens, disease outbreaks, and changing transmission patterns. Based on the user's profile and context, the system delivers personal recommendations for infection prevention and control measures. These recommendations can include guidelines on hand hygiene, personal protective equipment (PPE) usage, disinfection protocols, and environmental management. Figure 2.2 illustrates the features of the PORPOISE system. One of the key strengths of PORPOISE is its ability to provide real-time updates on the status of an outbreak, including the number of cases and deaths, as well as information on testing and treatment options. The system can also provide targeted advice based on the user's location and other contextual information, such as travel history and occupation. PORPOISE is a promising platform that has the potential to play a key role in preventing the spread of infectious diseases.

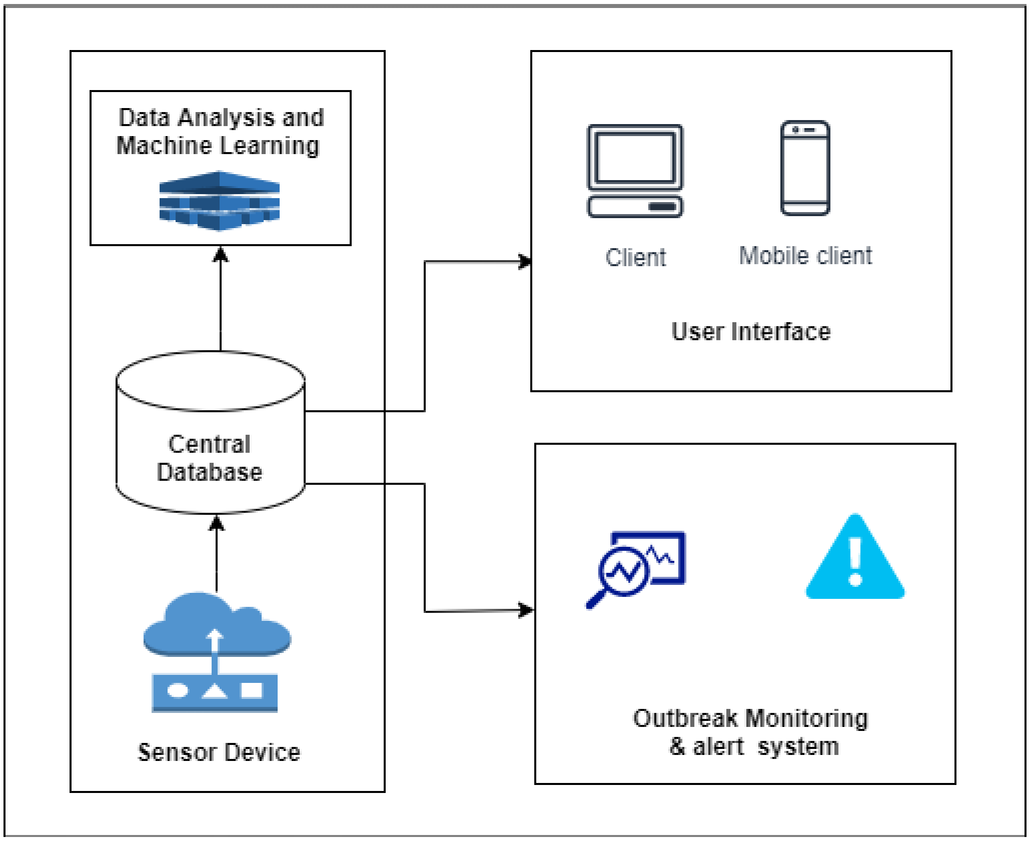

Data Analysis and Machine Learning
Client
Mobile client
User Interface
Central Database
Sensor Device
Outbreak Monitoring & alert system

Figure 2.2: Pathogen Outbreak Prevention Instruction System (PORPOISE)

The PORPOISE does perform any trust computation to verify the trust worthiness of its users. To ensure security the system use authentication and authorization to verify the users. Our trust model will improve of the Porpoise by evaluating the reputation and credibility of data sources used for training materials. Trustworthy and reputable sources, such as official health organizations and reputable research institutions, can be given higher trust scores. Another improvement that or model address that can be implemented on the PORPOISE will be to validate the medical experts based by computing their trustworthiness using direct and indirect trust computation. Their score will determine if they should contribute to the system on not.

2.3.2 Personalized Active Learner (PAL)

Fadelli developed a wearable system for real-time, bespoke, and context-aware health and awareness support. PAL's system has machine learning capability, its database is hosted in the cloud and the users track their physiological status and context information using the wearable devices. To access the system a mobile a web application is available for the users. The data visualisation capabilities enable in decision making and tracking (Fadelli, 2019). The modular nature of the system gives room for scalability. Figure 2.3 illustrates the personalized active learner system.

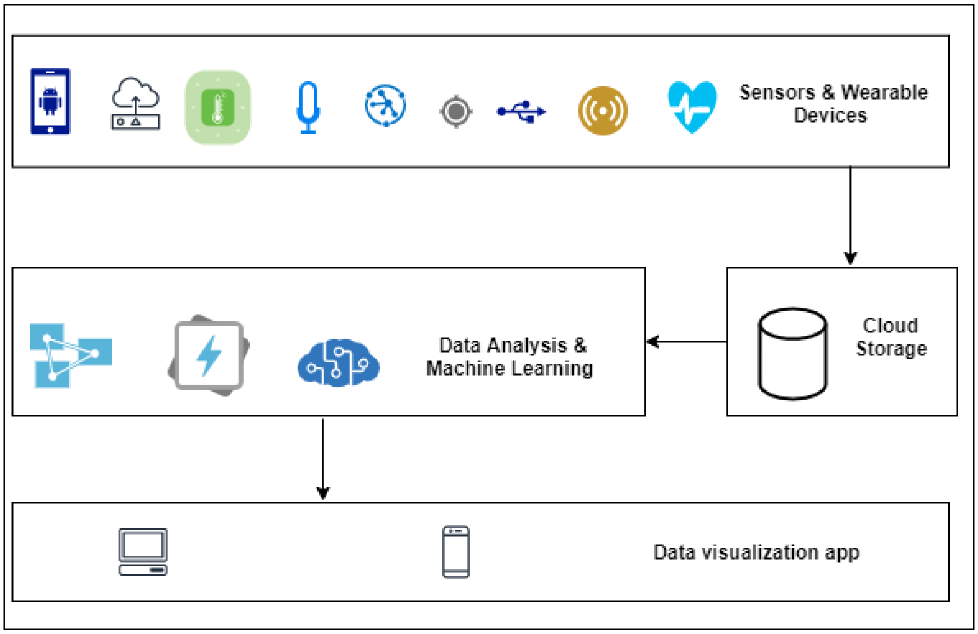


Figure 2.3: Personalized Active Learner (PAL)

In the context of our trust model for context-aware e-health services, context awareness plays a crucial role in ensuring the secure handling of patients' contextual and health information. Like Fadelli's work, our context-aware e-health services leverage real-time, bespoke, and context-aware health and awareness support.

Like PAL's system, our trust model analyses and interpret the contextual information collected from wearable devices. This information includes physiological data and other relevant context parameters. The collected data is securely stored in a database, ensuring accessibility and scalability.

To access the system, users can utilize a mobile or web application specifically designed for this purpose. The application serves as a gateway for users to track their physiological status and context information, providing them with valuable insights into their health and well-being. Within our trust model, context awareness enables personalized and adaptive functionalities. By continuously monitoring and analysing the context information of patients, the system can detect changes in health status, identify abnormal patterns, and prompt appropriate actions, such as sending alerts to healthcare facilities or dispatching an ambulance in case of emergencies.

Overall, context awareness is an essential component of our trust model, allowing for the dynamic adaptation of services and personalized support based on the specific context of everyone. This context-aware approach enhances the security, reliability, and effectiveness of the e-health service, ultimately improving the quality of healthcare provided to the patients.

2.4 Existing Trust Models

2.4.1 Reputation Experience and Knowledge Trust Evaluation Model (REK)

The Reputation Experience and Knowledge (REK) Trust Evaluation Model is a framework for evaluating trust in a system based on three factors: reputation, experience, and knowledge. Reputation is based on the past behaviour of a user or system, experience is based on the user's personal experience with the system, and knowledge is based on the user's understanding of the system as illustrated in figure 2.4 (Truong, Um, Zhou, & Lee, 2017).

- Reputation: This component assesses the public opinion and feedback of an individual or entity based on their past behaviour and interactions. Reputation is measured through various metrics, such as ratings, reviews, endorsements, and testimonials.

- Experience: This component evaluates the level of expertise and proficiency of an individual or entity in a particular domain. Experience is determined by the number of years of experience, qualifications, certifications, and achievements.
- Knowledge: This component assesses the level of understanding and comprehension of an individual or entity in a specific field. Knowledge is measured by assessing the person's education, training, publications, and contributions to the field.

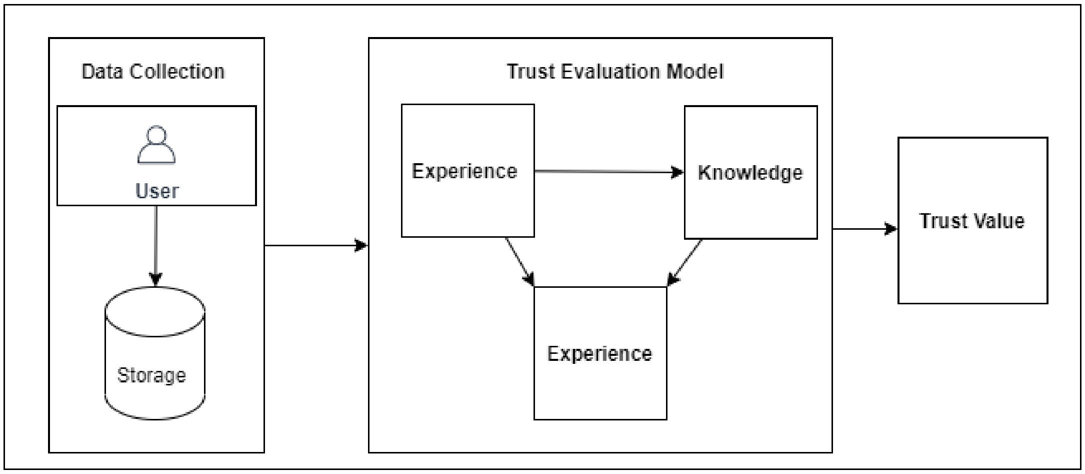


Figure 2.4: REK trust evaluation model

The model is designed to be used in situations where there is limited information available about the trustworthiness of a system or user. By considering these three factors, the model can provide a more comprehensive evaluation of trust. One potential limitation of the REK model is that it relies on subjective judgments about reputation, experience, and knowledge. Different users may have different opinions about these factors, and this could lead to inconsistent evaluations of trust. Another limitation is that the model does not consider external factors that may affect trust. For example, a user's trust in a system may be influenced by media reports or social media discussions, even if they have no direct experience with the system.

To address this limitation, the trust model in this thesis can incorporates objective measures of trust such as system performance, security features, and privacy policies. By combining subjective and objective measures of trust, the model provides a more comprehensive and accurate evaluation of trust in a system. Another limitation of the REK Model is that it assumes that trust is a static attribute that does not change over time. However, trust in a system can change due to various factors such as changes in system performance, security breaches, and new user experiences. To address this limitation, our trust model incorporates dynamic measures of trust that captures changes in trust over time. The model considers user feedback and system performance metrics to adjust trust scores in real-time.

In summary, trust model in this thesis improves on the limitations of the REK Model by incorporating objective measures of trust and dynamic measures of trust to provide a more comprehensive and accurate evaluation of trust in a system.

2.4.2 Trust-based context-aware recommender systems

The trust evaluation model for recommender systems proposed by Otebolaku and Lee is a framework that is used to evaluate the trustworthiness of users in online recommender systems (Otebolaku & Lee, 2018). This model is based on a Bayesian network approach that considers multiple factors, including user preferences, item attributes, and trust relationships, to estimate the trustworthiness of a user as illustrated in figure 2.5.

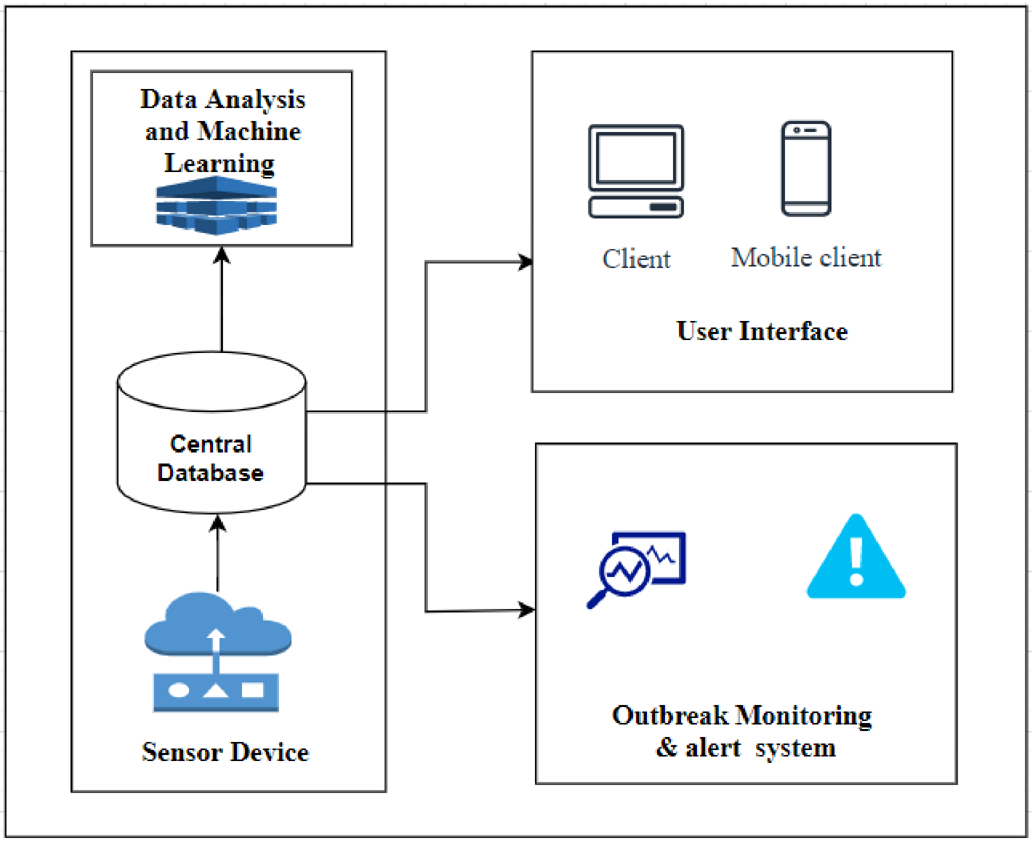

Data Analysis and Machine Learning
Central Database
Sensor Device
Client
Mobile client
User Interface
Outbreak Monitoring & alert system

Figure 2.5: Trust evaluation model conceptual framework.

One of the key advantages of this model is its ability to address the problem of data sparsity in recommender systems. The model uses a combination of user preferences and item attributes to estimate the trustworthiness of a user, even in cases where the user has limited interaction history. Additionally, the model can be adapted to different types of recommender systems, including collaborative filtering and content-based systems, by incorporating different types of data and features (Otebolaku & Lee, 2018).

Another strength of this model is its ability to handle uncertainty and incomplete data. The Bayesian network approach allows for probabilistic inference, which can account for uncertainty and variability in the data. This can help to improve the accuracy and reliability of the trust evaluations, even in cases where the data is noisy or incomplete.

However, the model also has some limitations. One of the main limitations is its reliance on explicit trust ratings or feedback from users. This means that the model may not work well in cases where trust is implicit or where users do not provide feedback or ratings. Additionally, the model assumes that the trust relationships are transitive, which may not always be the case in practice. Our trust model addresses this limitation by incorporating implicit trust signals, such as user behaviour or social connections. For example, a trust model can consider the behaviour of users who are connected to the target user in the context-aware e-health service to infer trustworthiness.

Overall, out trust model potentially complements and enhances the trust evaluation model proposed by Otebolaku and Lee by incorporating additional sources of trust signals, considering non-transitive trust relationships, and enhancing robustness to attacks.

2.4.3 Trust degree model

The Pervasive Trust Model proposed by Almenárez-Mendoza et al. (2006) is a framework that is used to assess the trustworthiness of entities in pervasive computing environments. The model is based on a multi-dimensional approach that considers multiple factors, including context, reputation, and experience, to estimate the level of trustworthiness of an entity (Almenárez-Mendoza, Marín-López, Campo, & García, 2006).

One of the key advantages of the Pervasive Trust Model is its ability to handle the dynamic and heterogeneous nature of pervasive computing environments. The model considers the context in which the entity operates, such as the location, time, and social environment, to adjust the trust evaluation accordingly. Additionally, the model incorporates different types of trust factors, such as reputation and experience, to provide a comprehensive assessment of the trustworthiness of an entity.

The model addresses the problem of uncertainty and incomplete data. The model uses a probabilistic approach to estimate the level of trustworthiness, which can account for uncertainty and variability in the data. It incorporates feedback from different sources, such as direct observation or indirect inference, to provide a more reliable and accurate assessment of trustworthiness as illustrated in figure 2.6.

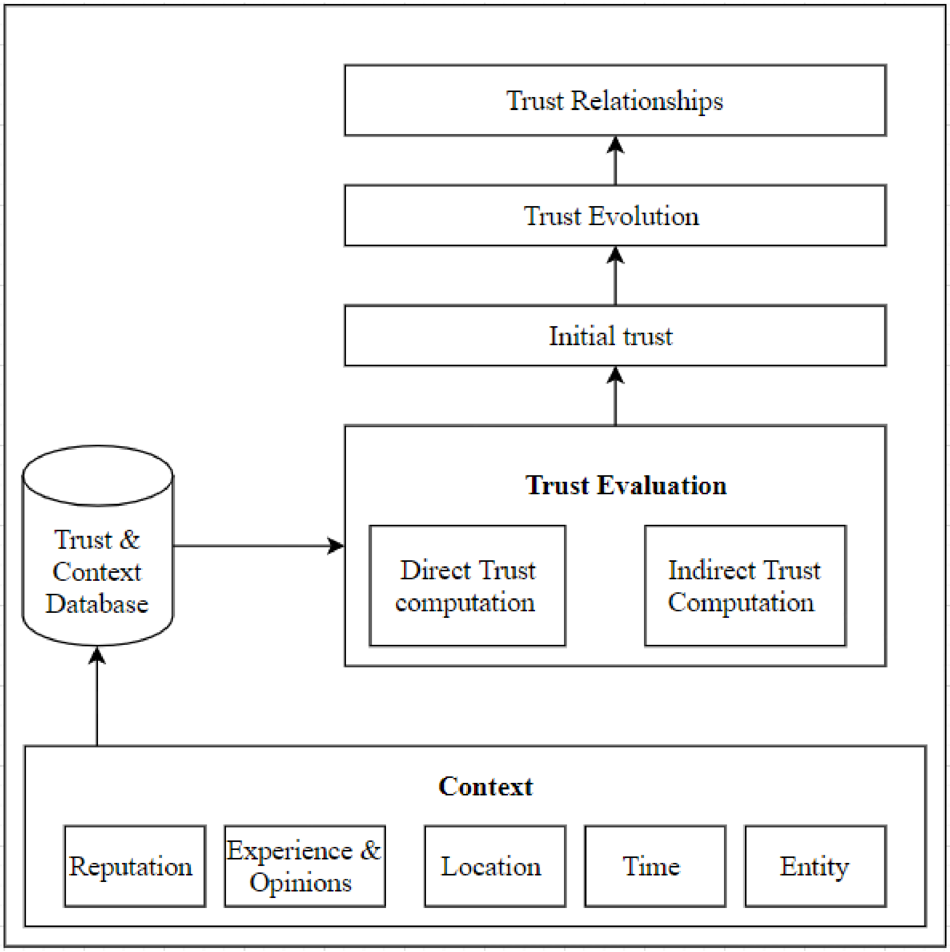


Figure 2.6: The Pervasive Trust Model.

The Pervasive Trust Model uses a combination of direct and indirect trust computation to estimate the level of trustworthiness of an entity in a pervasive computing environment. Direct trust is based on the direct observations and interactions between the trustor (the entity that needs to trust) and the trustee (the entity that is being trusted). The direct trust is computed as illustrated in (1):

$$(DT) = f(C, O) \qquad (1)$$

Where *C* represents the context in which the interaction takes place, and *O* represents the direct observations or interactions between the trustor and the trustee. The function f () represents the mapping between the context and the direct observations and can be defined based on the specific requirements of the trust evaluation (Almenárez-Mendoza, Marín-López, Campo, & García, 2006).

Indirect trust, on the other hand, is based on the opinions and experiences of other entities in the environment, such as friends or colleagues of the trustee. The indirect trust is computed using a Bayesian approach that considers the direct trust, the reputation of the trustee, and the experiences of the other entities. The indirect trust is computed as illustrated in (2):

$$(IT) = P(T|F, R, DT) \tag{2}$$

where *T* represents the trustworthiness of the trustee, *F* represents the set of feedback received from other entities about the trustee, *R* represents the reputation of the trustee, and *DT* represents the direct trust computed based on the direct observations and interactions. The Bayesian approach computes the probability of the trustee being trustworthy given the feedback from other entities, the reputation, and the direct trust. The computation of the probability can be done using the Bayes theorem illustrated (3):

$$P\ (T|F, R, DT) = P(F|T) * P(R|T) * P\ (T|DT) * P(R) \tag{3}$$

where $P(F|T)$ represents the probability of the feedback given the trustworthiness, $P(R|T)$ represents the probability of the reputation given the trustworthiness, $P(T|DT)$ represents the probability of the trustworthiness given the direct trust, $P(F)$ represents the probability of the feedback, and $P(R)$ represents the probability of the reputation.

The Pervasive Trust Model proposed by Almenárez-Mendoza et al. (2006) is a comprehensive framework for trust evaluation in pervasive computing environments. However, like any other trust model, it has some limitations that can be addressed by our trust model. The Pervasive Trust Model assumes that all entities are willing to share their data and interactions with others.

However, in real-world scenarios, privacy concerns can be a significant barrier to trust evaluation. Our trust model can incorporate privacy-enhancing techniques such as the use of blockchain. Blockchain technology is a useful tool for addressing privacy concerns in the Pervasive Trust Model. One of the key features of blockchain is its decentralized and immutable nature. This means that once data is recorded on the blockchain, it cannot be altered or deleted, and it can only be accessed by authorized parties. To leverage this feature, our model incorporates a blockchain-based trust model to ensure that entities' (patients, medical personnel, and administrators) identities are protected and that their data is only accessible to authorized parties. This is achieved using public and private key cryptography, which enables secure and verifiable transactions on the blockchain. In addition, blockchain-based smart contracts are used to define and enforce data sharing agreements among entities. Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. This can ensure that data is shared only under specific conditions, such as with the consent of the data owner or for specific purposes.

Overall, using blockchain technology in our trust model provides a secure and trustworthy way to address privacy concerns in the Pervasive Trust Model, while enabling entities to share their data and interactions with others.

2.4.4 Context-based Trust Management Model for Pervasive Computing Systems

The Context-based trust management model for pervasive assigns the trust value of zero to the new entity (Negin, Rahmani, & Mohsenzadeh, 2009). Thus, the interactions with the new entity can happen when other entities have negative trust values (untrustworthy entities).

Recommendations help a service requester to compute indirect trust in the case that there are not adequate records in interaction history for direct trust computation. False recommendations have a negative effect on the computed trust value. Dishonest and malicious recommenders can provide false recommendations. (Negin, Rahmani, & Mohsenzadeh, 2009) in their model identify dishonest recommenders and all recommendations provided by these recommenders are excluded from indirect trust computation. To identify a dishonest Recommender, the service requester uses all recommendations, which are received from a specific recommender, and calculates the value of the suggested trust values. In the case that the mean value is so low or so high (not in an adequate range), the service requester judges the recommender to be dishonest. The method of assigning weights to the interactions over time causes each past interaction to be effective in trust computing according to the assigned weight. Therefore, the weighting mechanism can protect the entity against the dynamic behaviour of malicious recommenders. Context-aware agent in the trust management model provides a service selection mechanism, which is based on contexts. As a result, target entities are restricted to the domains, which are identified by context-aware agent. Sending requests to domains, considering the context, facilitates the functionality of request management module and in this case, service providers with accurate context have more priority over other service providers (Negin, Rahmani, & Mohsenzadeh, 2009).

The trust management model comprises of the trust database, maintenance, interaction history, transaction management, computation method selection and recommender management module explained below.

Trust records DB: It is a repository consisting of trust records. The important fields of record are service type, service attributes, last updated time, and service provider ID (Razavi et al. 2009).

Trust maintenance: This module initializes, fetches, and updates records in trust records DB. If the last updated time field of a record contains an expired time, then it must be updated (Negin, Rahmani, & Mohsenzadeh, 2009).

Interaction history: It is a repository consisting of records that each record contains service attributes, context attributes, satisfaction degree, and the interaction time. For each interaction there exists a record in interaction history (Negin, Rahmani, & Mohsenzadeh, 2009).

Transaction management module: This module monitors the behaviour of each transaction and then calculates the satisfaction degree. Context and critical attributes directly

Influence on satisfaction degree. Satisfaction degree is computed as in (4).

$$D = \sum |EVnorm \quad - PVinorm\,|/n$$
$$1 \leq i \leq n \tag{4}$$

Where *SD* is the satisfaction degree, *n* is the number of attributes, norm. *EV* i^{norm} is the expected value and *PV* i^{norm} is the provided value for the attributes that are normalized.
Computation method selection: In the case that there is not any trust for a specific entity in trust records database, or the trust records database needs to be updated, this module computes the trust value by selecting the corresponding computation method. In the case that there are adequate records in interaction history and the occurrence times are acceptable, trust value is computed directly. Otherwise, trust value is computed indirectly by the help of recommenders. Trust computations are mostly based on the records in interaction history. The results of recent interactions, which represent the current behaviour of the entity, are more important than those of older interactions. Hence, we give weights to records based on the time they occur. Direct trust computation illustrated in (5) calculates an entity's direct trust value" (Negin, Rahmani, & Mohsenzadeh, 2009).

$$DT \;=\; \sum((W)(tcur - tiocc)\,.SDi)/\sum(W)\;(tcur - tiocc)$$
$$1 \leq i \leq k; 0 < W \leq 1 \tag{5}$$

Where *DT* this is the direct trust, SD_i is the satisfaction degree for i^{th} interaction, t^{cur} is the current time, t^{occ} is the occurrence time of the i^{th} interaction, *W* is a weight factor which is used to give a moving weight ((*W*) (t^{cur} –t^{occ}) to ith interaction based on the occurrence time, and *k* is the number of interactions with the corresponding entity.

Recommender assessment module: Different recommenders have different weights that can be mentioned as their trust values. Recommender assessment module judges' recommenders according to their honesty and context. Recommenders who are more trustworthy have more effect in computing the trust value of the recommended entity. Initialization function of a recommender's trust value is illustrated in (6) (Negin, Rahmani, & Mohsenzadeh, 2009).

$$RT \ = \ \sum TRVi/n. \qquad 0 \leq i \leq n \tag{6}$$

Where *RT* is recommender's trust value, *n* is sum of records in the trust DB whose service provider identity is like the recommender identity, TRV_i is trust record value of the *i*th trust record. Recommenders will be updated after each interaction with the corresponding recommended entity. Indirect trust value for a recommended entity is computed as illustrated in (7), (Negin, Rahmani, & Mohsenzadeh, 2009).

$$IT \ = \ \sum(RTi \, . TRVi)/\sum RTi \qquad 1 \leq i \leq n \tag{7}$$

Where IT is the indirect trust value for the recommended entity, n is the number of recommenders for that recommended entity, RT_i is the recommender's trust value corresponding to i^{th} recommender TRV_i is the trust value which is recommended by the i^{th} recommender.

The selection of an entity as a service provider will depend on the trust value the service requestor makes on the service provider. This Trust Computing Model is responsible for computing the trust values; these aids the service requestors in the selection of trustworthy service providers (Negin, Rahmani, & Mohsenzadeh, 2009).

2.4.5 Computational Trust Models

Computational trust unlike recommended and belief trust is built on notions of human concept of trust. Within ubiquitous computing, computational trust means automation of decisions in the presence of unknown, uncontrollable, and possibly harmful agents (Krukow , Nielsen, & Saassone, 2008). Computational trust value has been calculated using trustor's experience, recommendations, interactions, knowledge, measurements, distance, and density of events. They consider a probabilistic model of principal behaviour, say l. Their model considers only the behaviour of a single fixed principal p and consider only algorithms that attempt to solve the following problem. Suppose they are given an interaction history X obtained by interacting n times with principal p. Suppose also that there are m possible outcomes (*y1…, ym*) for each interaction. The goal of the probabilistic trust-based algorithm, say A, is to approximate a distribution on the outcomes (*y1…, ym*) for each interaction. That is, A satisfies as illustrated in (8) (Krukow , Nielsen, & Saassone, 2008).

$$A(yi|X) \in \ [0,1] \quad (for\ all\ i),\ \sum_{i=1}^{m} A\ (yi|X = 1 \qquad (8)$$

The trust models mentioned above have evident limitations in ubiquitous environment. Recommendations are undependable because they are based on unsecure opinions. Trust manifesto assumes that the user blindly trusts that service providers will deliver their promises, and the reliability of reputations is hard to measure.

2.4.5 Context-aware modelling of trust and access control

The research done by M'Hamed et al. (2013) proposed a context-aware trust and access control model that considers the user's behaviour and capabilities alongside other contextual factors. The model aims to enhance trustworthiness assessments and access control decisions by incorporating dynamic user-specific information. The key components of the model include context management, user behaviour modelling, capability modelling, trust and access control decision-making, and dynamic adaptation (M'Hamed, Zerkouk, Husseini, & Messabih, 2013).

Context management involves considering contextual factors like time, location, and device characteristics to provide context for trust evaluations and access control. User behaviour modelling incorporates information about the user's past interactions and preferences to inform trust and access control decisions. Capability modelling considers the user's skills and knowledge to assess their ability to perform tasks or access resources (M'Hamed, Zerkouk, Husseini, & Messabih, 2013).

M’Hamed et al. (2013) safeguarded the trust evaluation process against malicious threats. They further enhanced the precision of trust metrics centred on the correct human conduct in conditions that necessitate trust. The trust and access control decision-making process integrates contextual, behavioural, and capability information to make informed decisions. It combines quantitative and qualitative factors, such as trust scores and user feedback, to determine trustworthiness and access privileges. The model also includes mechanisms for dynamic adaptation, enabling updates to trust and access control decisions as the context changes or as the user's behaviour and capabilities evolve.

Their model has features from other models, these features include access control, authentication, opinions, and trust distribution. The computation of trust includes both direct obtained from personal experience and indirect trust obtained from recommendation from other, entities in the environment or network. Direct trust is sometimes termed as risk assessment; this is because an entity *A* has no prior relationship with entity *B* therefore no past record in their knowledge base to use to evaluate the trustworthiness of the entity. In cases where there is a trust dependency, they use a multiplicative factor to the negative actions called the Security Action Coefficient (SAC). SAC is the level of security a service has (M'Hamed, Zerkouk, Husseini, & Messabih, 2013).

They attain direct trust using (9):

$$DT = \frac{\sum PAi}{\sum PAi + SAC \times \sum NAi} \tag{9}$$

PAi represent the positive engagements (M'Hamed, Zerkouk, Husseini, & Messabih, 2013).

NAi presents the negative actions (M'Hamed, Zerkouk, Husseini, & Messabih, 2013).

They compute indirect trust as illustrated in (10):

$$T = \frac{\sum Twi \times Ji}{n} \tag{10}$$

Twi value of trustworthiness of a node or entity (M'Hamed, Zerkouk, Husseini, & Messabih, 2013). *Ji* the value of judgment node or entity *i* (M'Hamed, Zerkouk, Husseini, & Messabih, 2013). To get the total or net trustworthiness value they compute the direct and indirect trust values as illustrated in (11):

$$Tw = \alpha DT \times DT + \alpha\, IT \times IT \tag{11}$$

IDTrust is an iterative computation model proposed by (Tan, Wang, & Wang, 2016) that models compute trust and the trust evidence vector. The major contribution of the iterative computation model is reduction of the computation cost of trust and generally enhancing the computation performance. The model includes both direct and indirect collected through sentiments of other nodes to improve the evidence integrity (Tan, Wang, & Wang, 2016).

2.4.6 Trust management model for context-aware services computing

Mousa et al. (2021) proposed trust management model that introduces a novel approach to evaluating trust in cloud, fog, and IoT services. It employs a graph theory-based objective trust evaluation technique, which enables the detection of collusion attacks and provides a more accurate assessment of trustworthiness. This evaluation process involves the construction of a dependency network that captures the relationships between various quality of service (QoS) metrics and context variables. By modelling these dependencies, the model can identify the impact of changes in one variable on others, considering their cyclic relations. This approach enhances the model's ability to adapt to the dynamic nature of the running environment and improves the accuracy of trust evaluation. Furthermore, the model incorporates a trust bootstrapping mechanism that estimates the initial trust values of newcomer services. This mechanism helps address the challenge of assessing trust in services with no prior history or reputation. By leveraging available information and context, the model establishes an initial trust level for newcomers, allowing for a more comprehensive evaluation of their trustworthiness (Mousa, Bentahar, & Alam, 2021). A limitation of their model is it does not put into consideration the dynamic nature of the context-aware environment. While the model incorporates the concept of context-aware services and considers the dynamic environment, it assumes that the cyclic dependency relations among context variables and QoS metrics are static. This neglects the possibility of new context variables or changes in existing relations, which can affect the trust estimation accuracy. The trust model for context-aware e-health services improve on this by incorporating a feedback mechanism from users. The users rate the quality of services service and the medical personnel. The feedback is used to compute the trustworthiness of the model and later can be integrated to further improve the context-aware w-health service.

Overall, the proposed trust management model offers a robust and effective framework for evaluating trust in cloud, fog, and IoT services. By considering cyclic relations, employing objective trust evaluation techniques, and incorporating a trust bootstrapping mechanism, the model provides a comprehensive solution to address the gaps in existing trust management approaches.

2.5 Blockchain

Healthcare systems are increasingly being digitized to make it easier to manage patient data and health. Modern healthcare is a data-intensive domain representing an amalgamation of long-term electronic medical records, real-time patient monitoring data, and more recently sensor data from wearable computing. Blockchain in healthcare can address a multitude of challenges in healthcare, including care coordination, data security, and interoperability concerns, as technology advances (Vahiny, et al., 2022).

Blockchain is a decentralized, distributed, and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network (Armstrong, Stephen 2016). This allows the participants to verify and audit transactions inexpensively. A blockchain database is managed autonomously using a peer-to-peer network and a distributed timestamping server. They are authenticated by mass collaboration powered by collective self-interests (Don and Alex, 2016). The result is a robust workflow where participants' uncertainty regarding data security is marginal. The use of blockchain removes the characteristic of infinite reproducibility from a digital asset. It confirms that each unit of value was transferred only once, solving the long-standing problem of double spending.

2.5.1 Blockchain based Access Control Framework

Ouaddah implemented an access control block chain model, in their framework, users comprised of an Information Owner also known as the requester whose information has addresses which is a cryptographic identity (Ouaddah, 2017). These addresses are public keys public in the network and their purpose is to grant and request for access tokens. This hash is generated from the public key of an Elliptic Curve Digital Signature Algorithm (ECDSA). The user has the private key of the public key. The addresses uniquely identify the participants in the network and their resources. They had two types of transactions namely the Grant Access transaction and Get Access transaction. The grant access transaction is token based where an Information Owner defines the access policy, and a token is generated. The get access transaction a user spends a token that he/she obtains from a grant access transaction, to access information identified with an address. The requester has the rights to delegate access, by transferring a token that they already own to the new party under new conditions (Ouaddah, 2017).

All the access tokens are encrypted with a public key, retrieved from the address of the user asking for access to which the token is designated. This guarantees that only the users with a valid token will be able to decrypt the information using their private key. All the transactions have an identifier, input, and output. They uniquely identify transactions using their cryptographic hash (Ouaddah, 2017).

Each input in a transaction contains an index, reference to the previous token or the previous output. This reference is identified by the hash and index. The hash is the transaction identifier of the previous transaction while the index is the output within the transaction. When granting access there are no existing transactions for the block to point because this request generated a new access token. The user satisfies the access control policies as expressed in the script. Each output consists of index and value. The value is the transactional cost (Ouaddah, 2017).

2.5.2 Blockchain for increased Trust in Virtual Health Care

The blockchain for increased trust in virtual health care is a proof of concept by Hasselgren et al., (2021). They focused on utilizing blockchain technology to enhance trust in virtual healthcare settings. The study highlights the importance of trust in virtual health care interactions and identifies several trust-related challenges in the current healthcare landscape. The use of blockchain technology is proposed as a solution to improve trust by providing transparency, security, and data integrity (Narayanan, 2016). It explores the implementation of a blockchain-based system that enables trustworthy interactions in virtual health care using smart contracts. Smart contracts allow for automated and trustworthy transactions, ensuring that agreements and transactions are executed according to predefined rules without the need for intermediaries. This reduces the reliance on trust in human actors and provides a reliable and transparent framework for virtual healthcare interactions (Hasselgren, Rensaa, Kralevska, Gligoroski, & Faxvaag, 2021).

By leveraging blockchain technology and smart contracts, the study demonstrates how trust can be enhanced in virtual health care environments. The immutability and transparency of the blockchain ensure that patient data and interactions are securely recorded and accessible only to authorized parties. This increases trust in the integrity of the data and reduces the risk of unauthorized access or tampering (Hasselgren, Rensaa, Kralevska, Gligoroski, & Faxvaag, 2021).

While the study focuses on the application of blockchain technology, it does not delve into a comprehensive trust model. This is where our trust model improves on it. Our trust model provides a holistic assessment of trustworthiness by considering various factors such as the trustworthiness of medical personnel, context-aware systems, transparency, privacy, security, reliability, and performance. By incorporating these trust factors, our model can complement the blockchain-based system described in the study and provide a more comprehensive and fine-grained evaluation of trust in virtual health care environments.

Overall, the "Blockchain for Increased Trust in Virtual Health Care: Proof-of-Concept Study" highlights the potential of blockchain technology to enhance trust in virtual health care. Our trust model can build upon this by providing a more nuanced and comprehensive evaluation of trust, considering multiple dimensions and factors that contribute to trustworthy interactions in virtual health care settings.

2.6 Conceptual Framework

Figure 2.7 proposes a conceptual context-aware e-health services trust model framework. The model comprises of independent and dependant variables selected for this model. The independent variables used in this research include data, system, and people. The dependant variable is the trust perception of the end user in this paper being the patient. The variables explained below are not the only ones.

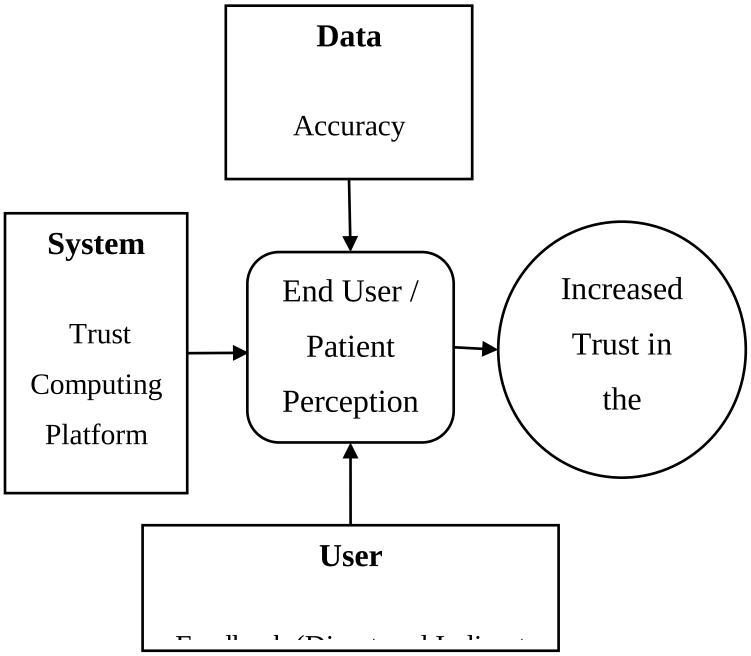


Figure 2.7: Context-aware e-health service conceptual framework

2.6.1 Data

Data is acquired by integrating the various features of context, we integrate these features using cognitive reasoning for example an activity like a patient walking, and a location we equate it to a hospital or a home. From this, we infer context to a patient walking home or a patient driving to the hospital. The conceptual framework, which translate to our trust model, recommends health facilities to the patients based on their current context and their preference. For example, a patient needing medical assistance who has travelled to a different town for work or business will be recommended a health care facility available in that town. In the event their preferred facility has a branch in the town, their visiting it will be on the top of the recommended facilities (Ayuku, Okeyo, Mindila, & Chemwa, 2021).

2.6.1.1 Accuracy

It presents how trust can be incorporated into context-aware e-health Services. For data to be trusted, it must be accurate the data collected from the IoT devices must be verifiable. For example, a context aware e- health system should provide precise user location and physiological data of a patient. The temperature of the patient or their pressure measurements should be correct. When the data is accurate, the users are most likely to trust the system (Ayuku, Okeyo, Mindila, & Chemwa, 2021).

2.6.1.2 Accountability

Other than the data being accurate, it is important for all entities to know the source of the data for accountability purposes in case of faulty sensors, attack, or malice. In the event a sensor is malfunctioned, an alert is sent, and the device is fixed. Apart from accountability, it also helps to determine whether the source of the data can be trusted. A patient can know the medical personnel who reviewed their records (Ayuku, Okeyo, Mindila, & Chemwa, 2021).

2.6.1.3 Aggregating

Since the data used in the context-aware services is collected from different devices, aggregating the data from different sources makes the trustworthiness of these services difficult. For example, our context-aware system would make flawed recommendations to a patient if it relied on a single review of a medical personnel or a health care facility. In contrast if the reviews were aggregated from numerous sources, having one of them being inaccurate would be mitigated by the other data being accurate. Hence, our adoption of Razavi’s recommended trust computation as explained in section 2.4.4 (Negin, Rahmani, & Mohsenzadeh, 2009).

2.6.2 System

Users should be confident that the systems they are using are trustworthy, hence the reason why the trusted computing platform focuses on the development of security standards. Another factor is explaining how the system works in a simple manner to enable users know how the algorithm works and how to use it to achieve the best results. Increased user understanding on the functioning of a system increases their trust levels (Ayuku, Okeyo, Mindila, & Chemwa, 2021).

2.6.2.1 Integrity

The systems the patients interact with should provide accurate data. Integrity focuses on maintenance and assurance of the accuracy and consistency of data provided by a system over its entire life cycle. For example, temperature measurements delivered by thermometer must be reliable and not modified by any entity (Ayuku, Okeyo, Mindila, & Chemwa, 2021).

2.6.2.2 Availability

System availability focuses on ensuring that IoT devices are available to the authorized entities. A GPS receiver must ensure to provide user's location anywhere and anytime. When considering that the application logic and the security configuration can depend on context, we must ensure that context information is trustworthy. We must be able to estimate the level of trust a context information requester can put in the delivered context information. Because context information provider and the context-aware system might be members of different administrative domains, it is very important to be able to differentiate trustworthy parties from un-trustworthy ones (Ayuku, Okeyo, Mindila, & Chemwa, 2021).

2.6.2.3 Blockchain

Blockchain technology has proven to be an effective tool for removing intermediaries in some processes, as it can force users of different systems to adopt behaviours and therefore lead to trust in the model. More specifically, blockchain characteristics that are making it beneficial to the different industries including the healthcare sector are its immutability and distributed properties, its potential for managing identification and access control to data, and its connection to off-chain data storage via distributed hash tables. In addition, enabling complementary technologies such as smart contracts have been used to propose a decentralized and token-curated data quality check mechanism.

2.6.3 User

The users in this trust model consists of the patients, system, and hospital administrators and all the medical personnel. The most critical users are the patients' and the medical personnel. Their context and personal identifiable information are required to ensure only authorised personnel have access to the information in the system. Trust in users is based on personal experience from directly interacting with them and from feedback from other users. In our model, a patient is most likely to choose a medical provider with whom they have interacted before rather than a stranger. In the event they have not interacted, with the system any they shall seek recommendations from friends or people they can trust. Our model computes indirect trust to enable patients select medical personnel based on reviews of other patients (Ayuku, Okeyo, Mindila, & Chemwa, 2021).

2.7 Summary

The literature review of the existing trust models in ubiquitous and context aware environments, concludes time, location, users are among the components of context measured during trust computation. However, none of the existing works provides a collective and cohesive consideration on all features that influence trust. These trust models either propose special-purpose solutions that are not easily portable to this context-aware e-health service domain as they specify incomplete trust relationships related to at most one trust aspect or make no distinction between different trust aspects because users need to trust a centralized service, for instance, in the way it is done by e-bay. We define a trust model for context-aware e-health service platforms that addresses the existing trust concerns. This trust model addresses trust aspects related to identity provisioning and privacy enforcement. The model supports both direct trusts resulting from direct experience and indirect trust derived from trust calculations, for example, based on recommendations from other entities.

CHAPTER THREE

METHODOLOGY

In this section, we discuss the various components and modules that make up the trust model. Our trust model uses direct and indirect trust to determine the trustworthiness of the context-aware e-health service and the medical personnel. To further enhance the security and privacy of the trust model we incorporate the use of blockchain due to its tamper proof nature. The cryptographic hashes are the key element that makes blockchain immutable and therefore tamperproof. The hash ensures the trust model cannot be reverse engineered and the model maintains high data integrity. The distributed nature of blockchain, enables the different health facilities in the network to have access to the patient’s medical information for ease of assistance in the event of a medical emergency. It notifies the patient whenever their information is accessed, modified, and provides feedback. Most importantly, it detects anomalies in the patient’s bio-signal patterns (Ayuku, Okeyo, Mindila, & Chemwa, 2021).

3.1 Trust Model for Context-aware E-Health services

3.1.1 Overview of the proposed model

The proposed trust model illustrated in figure 3.1 consists of three layers, i.e., the context information and access-processing layer, the trust model layer, and the application services layer. The context information and access-processing layer is responsible for gathering and processing contextual information relevant to context-aware e-health services. It collects data about the user's current situation, such as their location, health status, preferences, and environmental conditions. The collected context information is processed to extract meaningful insights and provide a comprehensive understanding of the user's context. The context information collected and processed in this layer is then passed on to the trust model layer for further analysis and evaluation. The trust model

layer relies on accurate and up-to-date context information to make informed decisions regarding trustworthiness (Ayuku, Okeyo, Mindila, & Chemwa, 2021).
The trust model layer is the core component of the system and is responsible for evaluating and determining the trustworthiness of context aware e-health services and entities involved in the service delivery. It employs various trust metrics and mechanisms to assess the reliability, credibility, and integrity of different entities, such as healthcare providers, devices, and data sources. The trust model layer utilizes the contextual information provided by the context information and access-processing layer to make context-aware trust evaluations. It considers the specific context of the user and the context-aware e-health service being accessed to provide accurate trust assessments. The trust evaluations generated by the trust model layer are then used to inform decision-making processes within the application services layer (Ayuku, Okeyo, Mindila, & Chemwa, 2021).

The application services layer represents the functional layer of the system where e-health services are delivered to the users. This layer encompasses a range of services, such as remote monitoring, personalized treatment recommendations, health data analysis, and communication between healthcare providers and patients. The trust evaluations from the trust model layer play a crucial role in the application services layer. They are used to make decisions related to service selection, data sharing permissions, access control, and personalized recommendations. The trustworthiness of context aware e-health services and entities, as determined by the trust model layer, influences the overall quality and reliability of the services provided in the application services layer (Ayuku, Okeyo, Mindila, & Chemwa, 2021).

In summary, the components in figure 2.7 are interconnected in a way that the context information and access-processing layer provides relevant context information, which is then utilized by the trust model layer to evaluate the trustworthiness of context-aware e-health services and entities. The trust evaluations generated by the trust model layer influence decision-making processes in the application services layer, ultimately ensuring the delivery of context-aware and trustworthy e-health services to users.

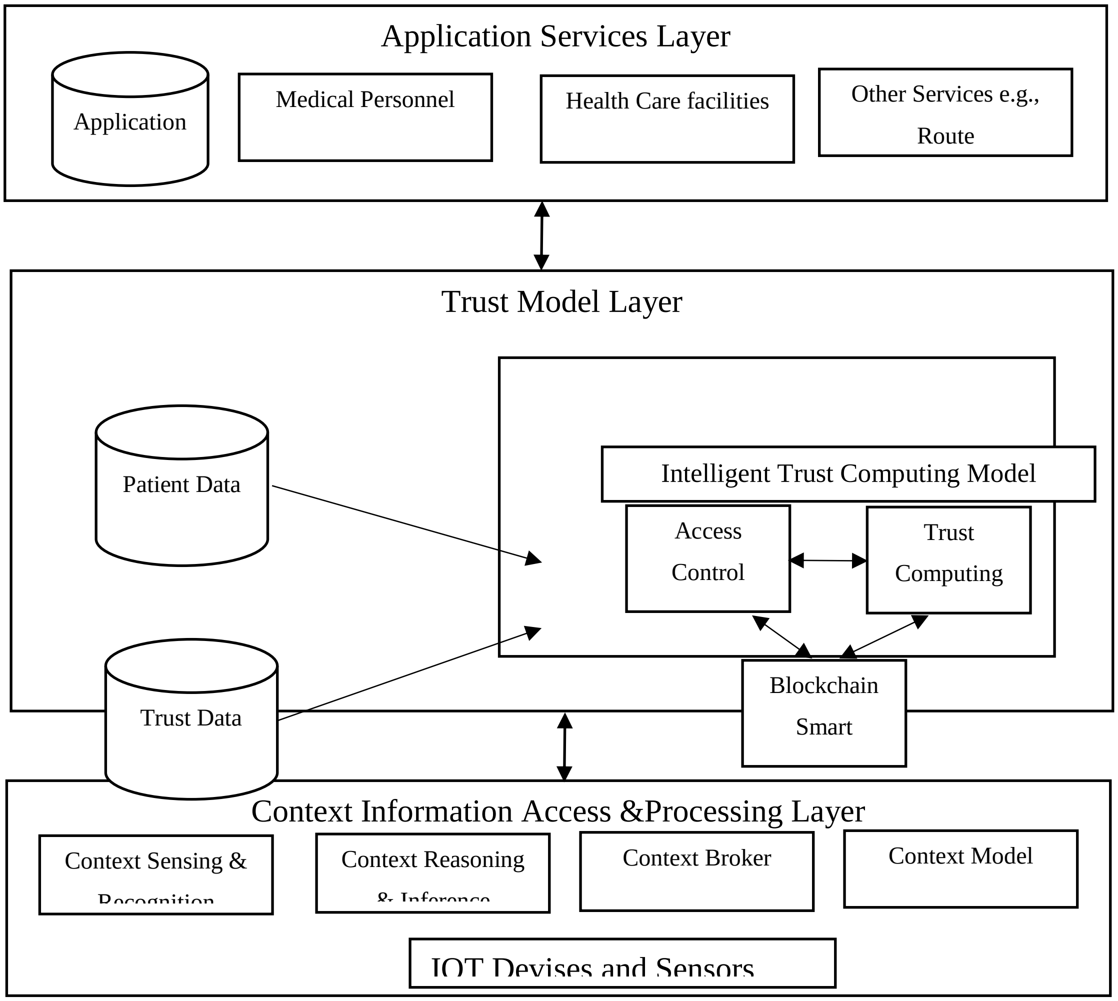

Application Services Layer
Application
Medical Personnel
Health Care facilities
Other Services e.g., Route
Trust Model Layer
Patient Data
Trust Data
Intelligent Trust Computing Model
Access Control
Trust Computing
Blockchain Smart
Context Information Access &Processing Layer
Context Sensing & Recognition
Context Reasoning & Inference
Context Broker
Context Model
IOT Devises and Sensors

Figure 3.1: Trust model for Context-Aware e-Health Services

3.1.2 Context-aware Information Access and Processing Layer

The *context-aware information access and processing* layer introduces context awareness component as illustrated in figure 3.1. The layer comprises various modules that ensure high-level context classification, using machine learning and ontologies for context classification, semantic processing, and reasoning. The modules include context sensing & recognition, context reasoning and inference, context broker and context model (Ayuku, Okeyo, Mindila, & Chemwa, 2021).

The *context sensing and recognition*, for a context-aware system to make an informed decision the contextual data collected needs to be accurate. It is unfortunate, sensors emit low-level format data unsuitable for decision making by mobile applications. The context recognition process collects raw data from sensors and transforms them into information that can be used to build intelligent applications. To provide an accurate context information about service consumers, the proposed model uses the context recognition process to identify contextual information such as user activities, from smartphone embedded and IoT sensors (obtained in the form of Web Services APIs from IoT platforms). This component gathers the physiological status, location, and activity of the users. It then processes this data to useful information.

The *context broker* provides the capabilities to obtain IoT context data in addition to context information obtained directly from the user's mobile devices.

The *context model* incorporates reasoning mechanisms based on ontology reasoning mechanism and Semantic Web Rule Language (SWRL). Ontology reasoning mechanism is responsible for checking class/concept consistency and implied relationships. It uses the inference engine such as Pellet or Jena to provide functionality for checking the consistency of ontologies, computing the classification hierarchy, explaining inferences, and answering queries. The other reasoning mechanism is Semantic Web Rule Language which extends OWL. Because OWL does not provide the mechanisms for expressing all relations between concepts in the ontology model. It allows inferring new knowledge from multiple facts or conditions at the same time by providing mechanisms for expressing complex relations. In the context of our trust model, ontological concepts can be used to define and represent entities, attributes, and relationships related to trust. For example, ontological concepts can be defined for entities such as users, medical personnel, context variables, and trustworthiness indicators. For instance, relating that a user called Njeri is the child of the married parents Nekesa and Mwangi using SWRL (Ayuku, Okeyo, Mindila, & Chemwa, 2021).

The integration of ontology reasoning mechanisms in the context model of our trust model for context-aware e-health services enable the model to effectively reason about trust based on the available contextual information. It allows for the extraction of valuable insights from the context variables and facilitates the automated inference of trust evaluations, leading to more accurate and contextually informed trust assessments in the e-health domain.

The *context reasoning and inference* component in figure 3.2 plays a crucial role in our trust model by supporting the evaluation and decision-making process. It analyses the collected context information, identifying patterns, correlations, and anomalies within the data. It helps in understanding the context variables that may affect trustworthiness, such as user behaviour, environmental factors, or device reliability. By performing data analysis and interpretation, this component provides valuable insights to our trust model, enabling it to make informed trust evaluations (Ayuku, Okeyo, Mindila, & Chemwa, 2021).

The context reasoning and inference component assists the trust model in understanding the context in which trust evaluations are computed. It considers the relationships between different context variables and their impact on trust. For example, it considers factors such as the location, time, and user's historical behaviour to determine the level of trustworthiness. By incorporating contextual understanding, the trust model can adapt its evaluations based on the specific context, making them more accurate and relevant (Ayuku, Okeyo, Mindila, & Chemwa, 2021).

The context reasoning and inference component helps in assessing the potential risks associated with different context variables. It identifies situations or events that may increase or decrease trustworthiness. For instance, it may recognize that a sudden change in a user's vital signs indicating an emergency, or the presence of a suspicious network connection could indicate a higher risk of untrustworthiness. By incorporating risk assessments, our trust model can adjust evaluations, accordingly, taking initiative measures to mitigate potential risks.

The context reasoning and inference component provides decision support to the trust model by generating recommendations or suggestions based on the analysed context data. It assists the trust model in making informed decisions regarding trust evaluations. For example, if the context reasoning and inference component detects a potential security threat, it may advise the trust model to lower the trust level or trigger additional authentication measures. By offering decision support, this component enhances the reliability and accuracy of the trust model's evaluations.

In summary, the context reasoning and inference component facilitates data analysis, contextual understanding, risk assessment, and decision support. It helps our trust model to incorporate contextual information, identify patterns and anomalies, and make informed trust evaluations. By leveraging the capabilities of the context reasoning and inference component, the trust model becomes more adaptive, accurate, and effective in assessing the trustworthiness of entities, systems, or interactions in a context-aware environment.

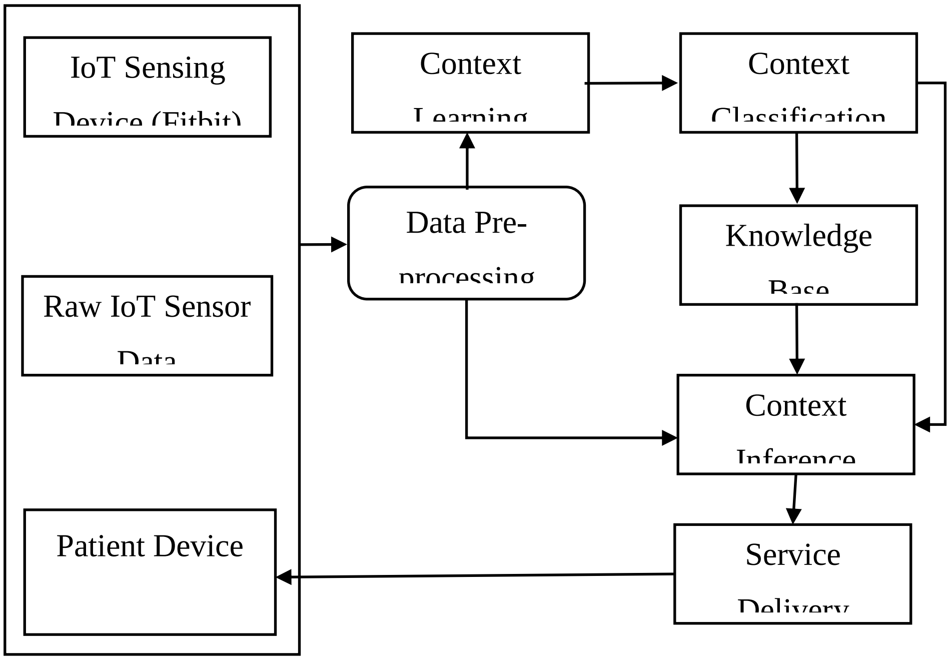


Figure 3.2: Context Sensing and Recognition Process.

In this model, we define context as the patient, medical personnel, patient’s activity, time, environment, and health status of the patient. The medical personnel and patient are the essential focus of this context-aware system. Location, activity, time, and preferences of the patients are critical to ensuring the context-aware e-health service adapts to their needs. Time answers the context factor when. Time is used hand in hand with location. A medical superintendent accessing a patient's data at 10:00 am on Tuesday 25th June 2020 in Nairobi, Kenya will be granted access to the patient's records. The same superintendent accessing the patient's records at 11:00 am on Tuesday 25th September in Istanbul, Turkey will raise an alarm in the system. Even though he/she is authorised to access the patient's medical data the location and time of access raises concern. This is because it is not possible for an individual to be in Nairobi at 10:00 am and an hour later in Istanbul (Ayuku, Okeyo, Mindila, & Chemwa, 2021).

Another significant concept of context "is the environment. The environment play an important role in determining situational context, information about the current location will be useful in recommending health care facilities and medical personnel near the patient. Ambulance services will also be dispatched based on proximity to the patient. Weather condition will help the ambulatory services to know which route to avoid in case of flash floods (Ayuku, Okeyo, Mindila, & Chemwa, 2021).

Patient health status includes context data about patient biomedical parameters (e.g., Temperature, Blood Pressure, Heartbeat Rate, ECG, and LabVIEW) and activity. This information is used by the system to automatically deduce patient health status and detect alarm situations by means of rule-based reasoning. Biomedical parameters instances are represented together with some relevant properties, such as measurement values and parameter ranges. Each range is specified in terms of upper and lower thresholds and related alarm level; when a measured value falls out of the thresholds, an alarm of the corresponding level is detected. Patient health status is thus determined by comparing biomedical parameter's measured values with a set of parameter ranges. In this model, we specify four basic alarm levels very low, low, medium, and high (Paganelli, Spinicci, & Giuli, 2008).

3.1.3 The Trust Model Layer

The trust model is responsible for computing the trustworthiness of our context-aware e-health service. It ensures that the patients can trust the system and are confident to use it. It comprises of the trust computing model, smart contracts, and data i.e., contextual data, medical personnel data, and patient data. The data also comprises information of the available medical personnel, medical facilities and the services offered (Ayuku, Okeyo, Mindila, & Chemwa, 2021).

The association between our trust computing model and blockchain smart contracts implemented lies in their complementary capabilities and shared goals of enhancing trust and security in the context-aware e-health service. The trust computing component aims to evaluate and quantify the trustworthiness of various the users, systems, and interactions in the context-aware e-health service. It considers factors such as user behaviour, context variables, and historical data to make informed trust evaluations. The trust model provides a framework for establishing trust and enabling secure interactions in the context-aware e-health ecosystem.

Blockchain technology provides a decentralized, immutable, and transparent ledger that securely records and verifies transactions or data exchanges. It ensures data integrity, enhances transparency, and eliminates the need for intermediaries in trust-dependent scenarios. Blockchain can provide a tamper-proof infrastructure for maintaining and validating trust-related information, such as user credentials, consent management, or access. The semantic association between the trust computing component and blockchain stems from their shared objective of improving trust and security in the context-aware e-health service. By integrating blockchain technology into our trust model, we can leverage the unique properties of blockchain to enhance the trustworthiness and security aspects of our system.

3.1.3.1 Trust Modelling

In our trust model, we have adopted and built upon several aspects of Tan et al., (2016) trust modelling work. Specifically, we have incorporated their approach to trust evaluation and decision-making, which involves the use of ontological reasoning and the Semantic Web Rule Language (SWRL).

$$fen\ (p, q)\ =\ update\ (fen - 1\ (p, q), gn\ (p, q)), \tag{12}$$

$$gn\ (p, q)\ =\ update\ (gn - 1\ (p, q), evidence\ (p, q)) \tag{13}$$

Where *p* computes the trust degree of $q.$ $(p,\ q)$ represents the n^{th} trust decision computing in $p.\ gn$ $(p,\ q)$ represents the n^{th} evidence modelling (Tan, Wang, & Wang, 2016).

Tan et al. (2016) equation represents a recursive update function for computing trust. While it is a valid approach for updating trust values based on previous values and evidence. We improve on their equation by considering trust factor as represented (13).

$$DT\ =\ \alpha\ *\ (C\ +\ R\ +\ S)\ +\ \beta\ *\ (P\ +\ T) \tag{13}$$

Where *DT* represent direct trust, *C* represents credibility, *S* represents security, *P* represents privacy and *T* represents transparency We calculate the direct trust value based on the weighted sum of different trust factors. The trust factors considered in the equation are credibility, reliability, security, privacy, and transparency. Credibility indicates the level of trustworthiness based on past experiences, user feedback, and ratings. Reliability of the e-health service considers factors such as availability, consistency, and performance. It assesses the extent to which the service can be relied upon delivering accurate and timely information. Security evaluates the security measures implemented in the context-aware e-health service, including data protection, access control, blockchain and encryption. It determines the level of trust in terms of protecting sensitive health information. Privacy focuses on the privacy protection measures employed by the context-aware e-health service. It assesses the control and safeguarding of personal health data, ensuring compliance with privacy regulations and user consent. Transparency assesses the level of openness and clarity in how the service handles user data and provides information to users. The coefficients α and β represent the weights we assign to each trust factor, indicating their relative importance in the computation.

Direct trust is personal evidence while indirect trust consists of evidence retrieved from recommendations and opinions of other elements in the network. Tan et al., (2016) represent trust in their model as Evidence (p, q) to represent proof that node p has upon node q.

$$Evidence\ (p, q)\ =\ \langle\langle\varphi\rangle, \langle\lambda, \nu, \rho, sim\rangle\rangle. \tag{14}$$

Explicit or direct trust evidence vector in Tan et al., (2016) model is mainly entailing of user ratings φ. Implicit or indirect trust evidence vector in their model mainly entails similarity from other nodes or entities, transaction accomplishment rate λ, transaction cost ν, trust degeneration factor ρ. The following will model both direct $\langle\varphi\rangle$ and indirect trust $\langle\lambda$, ν, ρ, sim$\rangle$ in iterative style as illustrated in (14) above (Tan, Wang, & Wang, 2016).

The indirect trust computation in our model evaluates the trustworthiness of a medical personnel based on the recommendations and opinions of other trusted entities in the system. By considering the recommendations and trustworthiness of intermediaries or third-party entities, the indirect trust computation expands the evaluation scope beyond direct interactions. It enables the trust model to leverage the collective wisdom and experiences of the network, improving the accuracy and reliability of trust assessments. We compute indirect trust as illustrated in (15).

Let *IT (p, q)* represent the indirect trust from entity p to entity q.

$$IT\ (p, q) = \ \alpha\ *\ DT\ (p, q) +\ (1\ -\ \alpha) *\ Sum\ [\beta\ *\ DT\ (p, r) * IT\ (r, q)] for\ all\ r\ in\ R(p) \tag{15}$$

Where *DT (p, q)* represents the direct trust from entity p to entity *q*, as computed using the direct trust computation in (13). *IT (r, q)* represents the indirect trust from entity *r* to entity *q*, which is recursively computed. *R(p)* represents the set of entities that directly trust entity *p*. The indirect trust value in (15) is calculated by considering a weighted combination of the direct trust values between entities. The α parameter determines the weight given to the direct trust, while the *(1 - α)* term computes the sum of the products of the direct trust, indirect trust, and a weight parameter β. The β parameter determines the weight given to the influence of the indirect trust relationship.

The recursive computation of indirect trust relies on the direct trust values between entities and their respective indirect trust relationships. The process continues until the desired level of recursion is reached or until a convergence condition is satisfied. The specific values of α and β may vary depending on the specific implementation and requirements of the trust model for context aware e-health services. These parameters can be adjusted to reflect the relative importance of direct and indirect trust in the context of the application.

We adopted the concept of direct and indirect trust to compute the trustworthiness of context-aware e-health service and the medical personnel. The patient computes the medical personnel’s and the context aware e-health service trust degree, weighing by their trust degree. Direct trust is achieved from the patients experience with the service and the medical personnel while indirect trust is from recommendations from other patients. The patients rate the service and medical personnel on a scale of zero to one, with one being trustworthy and zero being untrustworthy.

The selection of a medical personnel as a service provider and the adoption of the service will depend on the trust value ratings. The assigned trust values aid the patients in the selection of trustworthy medical personnel and the confidence of using the service. When the trust value is 1 it indicates that the medical personnel is trusted while the trust value is 0 it indicates they are not trusted hence access is denied.

We also incorporate some features from REK trust evaluation model. We compute direct trust based on the patient’s knowledge, experience, and reputation trust indicator. We obtain knowledge trust indicator from the information about the medical personnel’s characteristics and the environment. Experience trust indicator is obtained by analysing the interactions a patient has had with the service and medical personnel. Reputation trust indicator in our model is indirect trust, whereby we aggregate all previous experience from the patients in our network. The recommendation manager screens the opinion of other entities and proposes the relevant ones based on the users' preferences. It uses algorithms to filter through the trust values available. The Trust Model aggregates context and trust-related information obtained from patients whenever they use the service. It derives an assessment for the trust degree of the service. This thesis aims to increase the adoption of context-aware e-health services by ensuring they understand their data is secure and therefore led to increased use. The system should be able to preserve the integrity of their data, protect the patient's personal information and be available. Confidentiality, integrity, and availability are the building blocks for a trustworthy e-health system. Figure 3.3 illustrates the trust computation process.

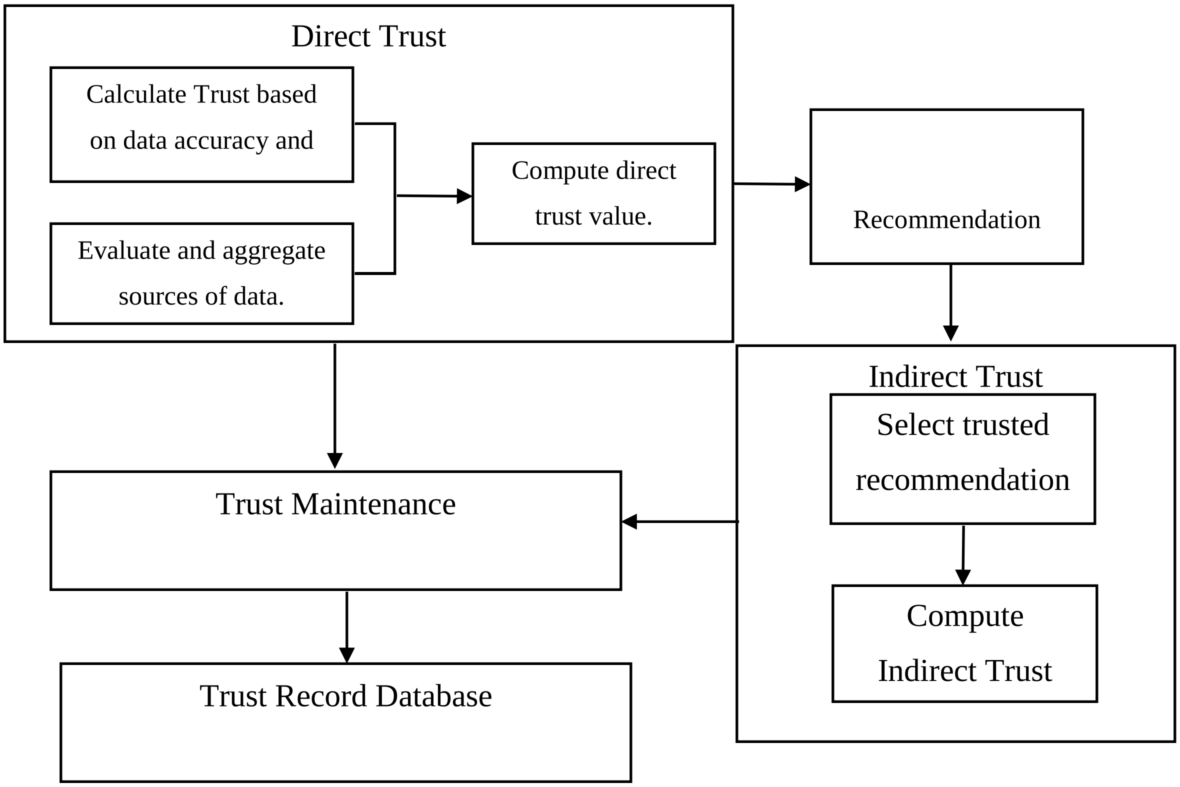

Direct Trust
Calculate Trust based on data accuracy and
Evaluate and aggregate sources of data.
Compute direct trust value.
Recommendation
Indirect Trust
Select trusted recommendation
Compute Indirect Trust
Trust Maintenance
Trust Record Database

Figure 3.3: Computation Model.

3.1.3.2 Direct and Indirect Trust Computation

Our direct and indirect trust computation in our trust model contribute to the overall evaluation and assessment of trustworthiness in context-aware e-health services. The direct trust computation in our model assesses the trustworthiness of a target entity based on direct interactions and feedback received from that entity. This computation allows for a more immediate and specific evaluation of trust, considering the history of direct interactions and experiences with the target entity. It contributes to building a trust profile for each entity and provides a basis for making trust decisions.

The indirect trust computation in our model evaluates the trustworthiness of a medical personnel based on the recommendations and opinions of other trusted entities in the system. By considering the recommendations and trustworthiness of intermediaries or third-party entities, the indirect trust computation expands the evaluation scope beyond direct interactions. It enables the trust model to leverage the collective wisdom and experiences of the network, improving the accuracy and reliability of trust assessments.

Together, the direct and indirect trust computations provide a comprehensive evaluation of trustworthiness by considering both direct interactions and the reputation and recommendations from trusted entities. This dual approach enhances our trust model's robustness and adaptability, making it more effective in capturing the complexities of trust relationships in context-aware e-health services.

3.1.4 Application Services Layer

The application services layer is responsible for providing users with the most relevant services. These services include medical personnel recommendation, health care facilities recommendations and route recommendations. Context-aware services and systems apply sensing and analysis of user context to deliver personalized services. These layer uses efficient tools that overcome the information overload problem by providing users with the most relevant contents. This is done through user’s preferences/ratings acquired from the *application* and *trust* data stores. Besides user preferences, considering the interaction context of the user improves the relevancy of recommendation process. In this thesis, services recommended to the patients are based on both user preferences, ratings, and context.

The context-aware e-health service uses context information to extract, interpret and adapt its functionality to the current context of use. The service seamlessly monitors the context of the users and deliver appropriate recommendations by considering context. Assisting the patients to live independently and safely in their own homes by providing appropriate services for them and ensuring that medical personnel are immediately alerted in the event of an emergency is crucial. The application layer acquires and utilizes information on an entity to provide appropriate services to a particular patient, such as the nearest medical facility, the best route to use and trusted medical personnel to attend to them. By dynamically learning the historical data of the patterns of a patient in a specific environment, recommendations can be adapted to match the patient's needs.

3.2 Proof of Concept Implementation

We have implemented a proof-of-concept system for the trust model described in 3.1 The model comprises of a user interface, trust model, blockchain smart contracts and a context aware system.

3.2.1 User Interface

The user interface is built on a web application using Flask web framework and integrated with Ethereum based blockchain to ensure the data is secure. In this model a transaction equates a patient getting an emergency and an ambulance being dispatched, a patient visiting the hospital, medical personnel writing a patients diagnosis/ patient note, results obtained from the sensors and laboratory tests, among others. In this model, the patient has control of their records and can choose to grant or revoke access. This model will be very useful for medical personnel to treat their patients properly and efficiently. Blockchain being decentralized promotes interoperability across different hospitals or organizations and hence everyone can make use of one standard system to store health data. Figure 3.4 shows the login interface for the patient, doctor, and hospital administrator.

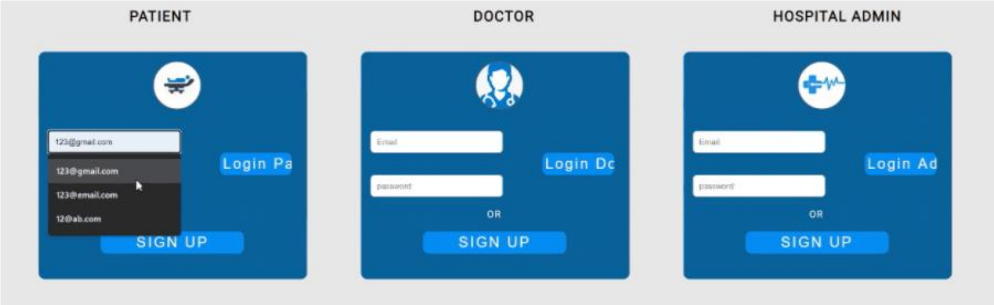


Figure 3.4: Login Interface

3.2.2 Context-awareness

In this model we consider context in terms of the person, their physiological data in case of a patient and their location. When a patient arrives at the hospital the medical personnel is granted access to their records based on his/her access writes and current location. Upon login we verify the device the doctor users to login and their location.

To get the medical personnel's location we obtain the originating IP Address by using: *X-Forwarded-For – the de facto* standard header for identifying the originating IP address of a client connecting to a web server through an HTTP proxy or load balancer. Once we retrieve the IP address, we convert it to a real-world location through geolocation. We use the User-Agent which carries the information about the device used to login to the application. The information it carries is used to identify the application type, software vendor and the operating system of the device used. We use code 1 to extract the device details.

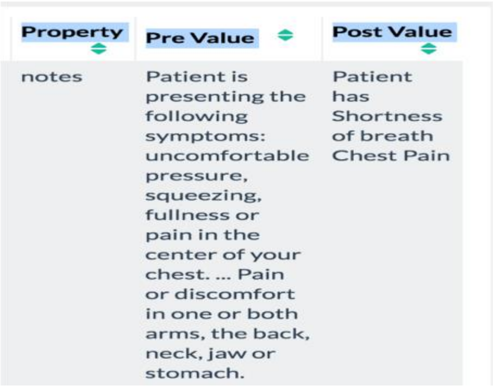
3.2.3 Blockchain and Smart Contracts

To establish a trusted context-aware e-health system, our trust model incorporates the utilization of Ethereum blockchain, smart contracts, and associated functionalities. We have chosen to implement a public blockchain, as our solution is open to the public, while a private blockchain would limit access to predefined users. By employing specialized protocols that offer varying degrees of anonymity, confidentiality, and privacy, we can effectively safeguard the data used in context-aware e-health services.

One key aspect of our trust model is the use of smart contracts within the blockchain. Smart contracts are self-executing agreements with predefined rules and conditions that are stored and automatically enforced on the blockchain. In the context of context-aware e-health services, smart contracts facilitate secure and automated interactions between different entities, such as patients, medical personnel, and service providers.

For instance, consider the example of Jane, a patient with an underlying heart condition, using the context aware e-health service. When Jane's doctor advises her to monitor her health status using the service, a smart contract is created and deployed on the blockchain. This smart contract contains the agreed-upon terms and conditions, such as data access permissions and emergency response protocols. In the event of a cardiac arrest alert being triggered for Jane, the smart contract automatically executes predefined actions. It may initiate the dispatch of an ambulance to her location, grant access rights to the medical personnel responding to the emergency, and trigger notifications to the relevant parties involved. Furthermore, smart contracts enable secure and auditable updates to the patient's medical records as illustrated in figure 3.5. When Jane is presented to the hospital and her doctor performs a diagnosis, the smart contract can facilitate the appending of new information or modifications to her medical records on the blockchain. This ensures that the data remains tamper-proof, transparent, and accessible to authorized parties while maintaining the integrity and trustworthiness of the e-health service.

By incorporating smart contracts into our trust model, we enhance the automation, transparency, and accountability of the interactions within the context-aware e-health system. These self-executing agreements streamline processes, enforce predefined rules, and provide a secure framework for seamless communication and collaboration among stakeholders, ultimately improving the overall quality of healthcare delivery.



Property	Pre Value	Post Value
notes	Patient is presenting the following symptoms: uncomfortable pressure, squeezing, fullness or pain in the center of your chest. ... Pain or discomfort in one or both arms, the back, neck, jaw or stomach.	Patient has Shortness of breath Chest Pain

Figure 3.5: Modified patient record.

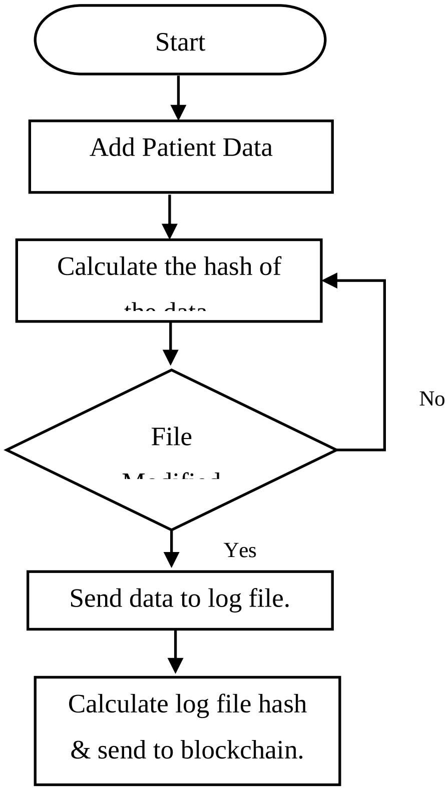

Start
Add Patient Data
Calculate the hash of the data
File Modified
No
Yes
Send data to log file.
Calculate log file hash & send to blockchain.

Figure 3.6: Patient Data hashing flow chart diagram

To ensure integrity of the patient’s records are consistent, accurate and trustworthy meaning the data is not tampered while on transit or in storage. We implement data hashing as illustrated in figure 3.6. Once a patient’s medical data is recorded, it cannot be altered due to the immutable nature of blockchain. The changes are appended as new blocks creating a chain; each block contains the previous blocks hash, its own hash, data, and a timestamp as illustrated by figure 3.7.

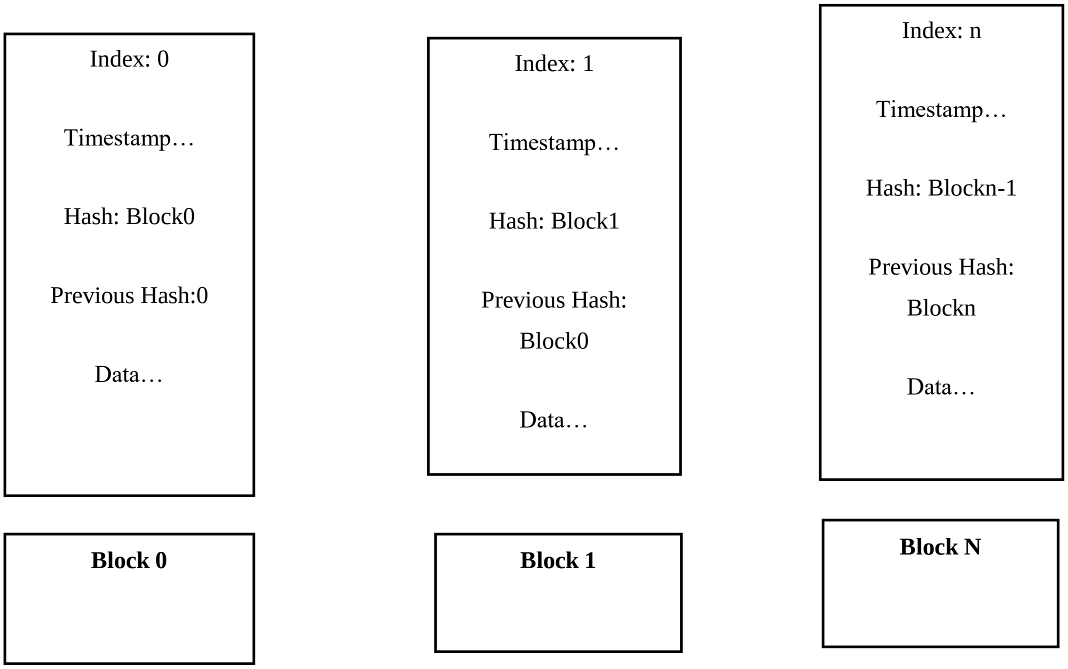
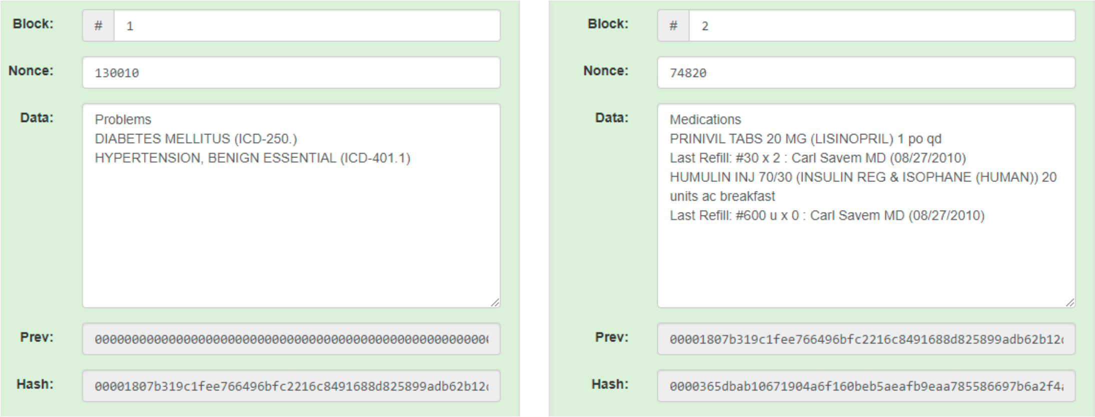


Figure 3.7: Context-aware e-health service network data

Blockchain is a list of blocks where each block stores a cryptographic hash of the previous block. It is only valid if the hash in the chain matches the hash in the next one. This means if data changes in any block all the consequent blocks will change invalidating the blockchain. Figure 3.8 displays two blocks before changing the data, which represents the medical records of the patient.



Block: # 1

Nonce: 130010

Data:
Problems
DIABETES MELLITUS (ICD-250.)
HYPERTENSION, BENIGN ESSENTIAL (ICD-401.1)

Prev: 00000000000000000000000000000000000000000000000000000

Hash: 00001807b319c1fee766496bfc2216c8491688d825899adb62b12

Block: # 2

Nonce: 74820

Data:
Medications
PRINIVIL TABS 20 MG (LISINOPRIL) 1 po qd
Last Refill: #30 x 2 : Carl Savem MD (08/27/2010)
HUMULIN INJ 70/30 (INSULIN REG & ISOPHANE (HUMAN)) 20 units ac breakfast
Last Refill: #600 u x 0 : Carl Savem MD (08/27/2010)

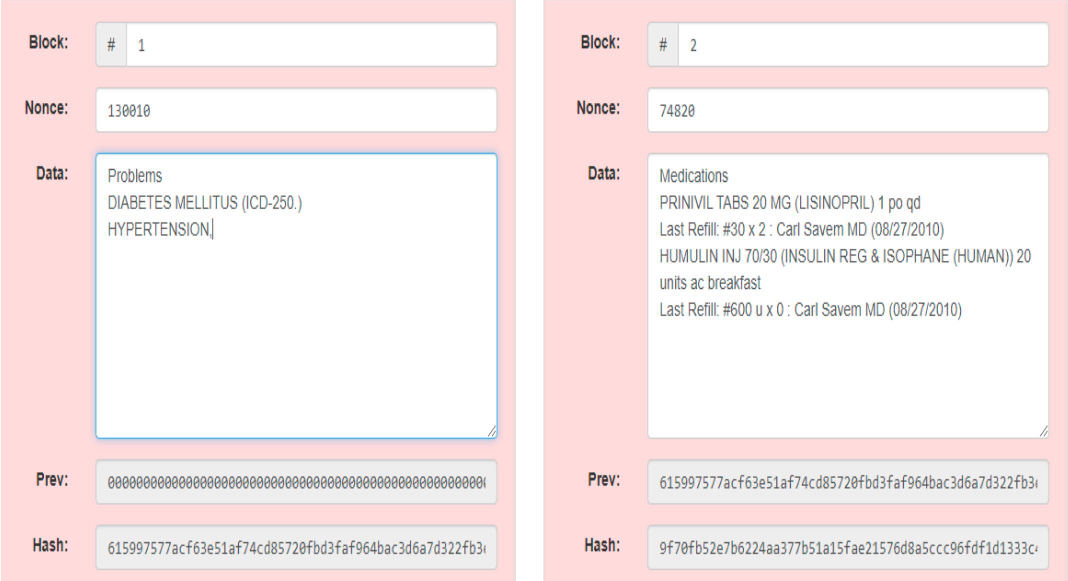
Prev: 00001807b319c1fee766496bfc2216c8491688d825899adb62b12

Hash: 0000365dbab10671904a6f160beb5aeafb9eaa785586697b6a2f4

Figure 3.8: Patient Data in a Blockchain

The background colour is green because the patient's record has not been tampered with. Block 1 is the genesis block and therefore its previous hash is zero.

Figure 3.9 is red because the block one has been altered, this caused its hash to change therefore affecting the hash in the next block hence the error. The semantic association between our trust computing model and blockchain lies in leveraging the transparency, security, and automation capabilities of blockchain and smart contracts to enhance the trustworthiness of context-aware e-health services. By integrating our trust model with blockchain, we can ensure that trust evaluations and transactions are recorded and auditable, providing a robust and trustworthy infrastructure for e-health interactions.



Block: # 1

Nonce: 130010

Data:
Problems
DIABETES MELLITUS (ICD-250.)
HYPERTENSION.

Prev: 00000000000000000000000000000000000000000000000000000

Hash: 615997577acf63e51af74cd85720fbd3faf964bac3d6a7d322fb3

Block: # 2

Nonce: 74820

Data:
Medications
PRINIVIL TABS 20 MG (LISINOPRIL) 1 po qd
Last Refill: #30 x 2 : Carl Savem MD (08/27/2010)
HUMULIN INJ 70/30 (INSULIN REG & ISOPHANE (HUMAN)) 20 units ac breakfast
Last Refill: #600 u x 0 : Carl Savem MD (08/27/2010)

Prev: 615997577acf63e51af74cd85720fbd3faf964bac3d6a7d322fb3

Hash: 9f70fb52e7b6224aa377b51a15fae21576d8a5ccc96fdf1d1333c

Figure 3.9: Tampered Blockchain

3.2.4 Access Control

Only authorised entities participate in the network, the model aims at providing the patient with the capacity of defining the access rights to his/her data and of dynamically deleting these rights when needed. Rights are expressed per medical personnel and registered in a smart contract as a whitelist of authorized doctors with a detailed specific access control list. No one can alter the list of authorized entities to access certain resources, as all blockchain specific operations are secure and non-corruptible, thus ensuring non-tamper proofs of data access activities as illustrated in figure 3.9.

The entire identification system and the robustness of the authentication process rely on blockchain properties. When a patient requires medical attention, the doctor should have access to the patient's context and medical data. This information will only have value if the accessed at the right time and by the right person. Blockchain ensures a replica of the ledger is available in the devices of all authorized participants in the network.

3.3 Trust Model Evaluation

The model evaluates the trustworthiness of a medical personnel and the context-aware model using precision, recall and F-score.

3.3.1 Operationalization of Variables

Once the context-aware e-health services are proven to be trustworthy more patients will use the services this will in return lead to improved healthcare. Table 3.1 illustrates how we define and measure the specific independent and dependent variables as we have implemented in this trust model and explained in the conceptual framework in section 2.6.

Table 3.1: Operationalization of variables

Metric	Definition
Accuracy	Extent to which data is correct and free of errors.
Integrity	Maintenance and assurance of the accuracy and consistency of data provided by the system.
Precision	Degree of exactness with which context is collected.
Accountability	Determine whether the source of the data can be trusted.
Granularity	Degree of detail with which context is collected.
Time period	Time interval between two readings of context.
Sensor state	Physical state sensor.
Access level	Information about the rights of users to access certain types of information.
Reliability	Indicates validity of context can be considered credible.
Timeliness	Indicates validity of context to use considering its freshness.

In this model, we compute the trustworthiness of a medical personnel and the context-aware model using precision, recall and F-score. To evaluate the trust model, we use the confusion matrix, which provides an overview of how accurately the model predicted the patients who trusted and those who did not trust the service based on test split data. Table 3.2 shows the summary of the model.

- Trustworthy is a positive class.
- Untrustworthy is a negative class.

Table 3.2: Confusion Matrix

	Trustworthy (actual)	**Untrustworthy (actual)**
Trustworthy (predicted)	True Positive (*tp*) • Model Output: Patient identified as trusting the medical personnel and the context-aware e-health service. • Ground Truth: Patient trusts the medical personnel and the context -aware e-health service.	False Positive (*fp*) • Model Output: Patient identified as trusting the medical personnel and the context-aware e-health service. • Ground Truth: Patient does not trust the medical personnel and the context -aware e-health service.

3.3.2 Evaluation Metrics

To evaluate the trust model for context-aware e-health service we used precision, recall and f-score. Precision in a classification problem is defined as the total number of correct positive values (*tp*) over the total number of correct positives plus the total number of incorrect positives (*fp*).

$$Precision = tp/ (tp + fp)$$

(20)

where t_p is appropriately identified and f_p is erroneously identified. Precision is also defined as the number of the maximum suggested things that are appropriate. It is the number of appropriate items nominated from suggested items to the number of items that are appropriate in the suggested (Otebolaku & Lee, 2018).

Recall in a classification problem is defined as the number of correct positives (*tp*) over the number of correct positives plus the number of incorrect negatives (*fn*).

$$Recall = tp/ (tp + fn)$$

(21)

Otebolaku & Lee (2018) describe recall as the proportion of the suggested items appropriate and favoured by the users in the existing setting to the total number of appropriate items in the reference set as shown in (21) (Otebolaku & Lee, 2018).

F-score captures the trade-off between precision and recall of a classifier model. It is joint metrics of both precision, recall, and computed as the harmonic mean between these metrics:

$$F1 = \frac{2\times Precision \times Recall}{Precision + Recall}$$

(22)

F-score is the average of precision and recall. It is a measure of the accuracy of the recommendation system in deliberation of significant and insignificant items included in the recommendation set.

3.4 Trust Model Test Cases

We performed functional tests on the proof of concept discussed in section 3.2 to verify that it functions as expected and the patients can trust the context-aware e-health system. Functional testing is defined as a type of testing which verifies that each function of the software application operates in conformance with the requirement specification. This testing mainly involves black box testing, and it is not concerned about the source code of the application.

Functional Testing involves: -

- Understanding the Software Engineering Requirements.
- Identifying test input (test data).
- Computing the expected outcomes with the selected test input values.
- Executing test cases.
- Comparison of actual and computed expected results.

We used the test cases below:

Table 3.3: Tests cases.

Test Name	**Description**	**Steps**	**Expected Results**	**Scenario Type**
Registration	Verify that the users can successfully register to use the service.	**Preconditions:** User has a smart phone or laptop. Assumptions: 1.The users have been trained on how to use the systems 2. The system is working as expected **Steps:** 1.User access the webpage using the URL provided 2. User selects the relevant tab (patient/doctor/admin). 3. User enters valid email address, name, password, and phone number to register	User Successfully registers and is redirected to the homepage to login	Positive
Login	Verify that the registered users can login to the service.	**Preconditions:** User has a smart phone or laptop. **Assumptions:** 1.The users have been trained on how to use the systems 2. The system is working as expected **Steps:** 1.User access the webpage using the URL provided 2. User selects the relevant tab (patient/doctor/admin).	User successfully logs in and is directed to access the services. Doctors can view the patients' records.	Positive

		3. User enters their email address and password. 4. Use clicks submit to login		
Request access	Verify that the doctor can successfully request access.	**Preconditions:** User has a smart phone or laptop. **Assumptions:** The user has logged in successfully. **Steps:** 1. User selects and copies the patient’s ID 2. User inputs the patient ID and requests access to either download, upload, or summarize the patients record	User is successfully granted access to the patients’ records.	Positive
Grant access	Verify that the patients can successfully grant doctors access to their records	**Preconditions:** User has a smart phone or laptop. **Assumptions:** The user has logged in successfully. **Steps:** 1.User clicks the grant access button to grant the doctor access to their records.	User successfully grants the doctor access to their records.	Positive
Revoke access	Verify the patient can successfully revoke a doctor access to their records	**Preconditions:** User has a smart phone or laptop. **Assumptions:** The user has logged in successfully. **Steps:** 1.User clicks the revoke access button to deny the doctor	User successfully revokes the doctor access to their records.	Positive

		access to their records.		
Upload Records	Verify the user can successfully upload records	**Preconditions:** User has a smart phone or laptop. **Assumptions:** The user has logged in successfully. **Steps:** 1.User selects the patient ID. 2. User uploads the records linked to a patient.	User successfully uploads records	Positive
Login	Verify that an unregistered user cannot login to the service.	**Preconditions:** User has a smart phone or laptop. **Assumptions:** 1.The users have been trained on how to use the systems 2. The system is working as expected **Steps:** 1.User access the webpage using the URL provided 2. User selects the relevant tab (patient/doctor/admin). 3. User enters their email address and password. 4. Use clicks submit to login	An unregistered user should not be able to login.	Negative
Grant access	Verify that the doctors cannot access patient records if they have not been granted access.	**Preconditions:** User has a smart phone or laptop. **Assumptions:** The user has logged in successfully. **Steps:** 1.User clicks the grant access button to	Doctor should not be able to view the patients records if they have not been	Negative

		grant the doctor access to their records.	granted access.	
Context-Aware Health Monitoring	Collect and analyse real-time health data from connected devices.	Analysis of the data from the connected devices (e.g., the heart rate, blood pressure location)	The system accurately captures and displays the health data in the user's dashboard.	Positive
Personalized Health Recommendations	The system should provide personalized health recommendations based on the user's health data.	Patients’ health data exceeds or falls below specified thresholds (e.g., high heart rate, low blood pressure).	The system generates relevant recommendations to improve the user's health status.	Positive

3.5 Trust Model Test Data

The trust model was tested with 20 users. The data from the user’s direct interaction with the medical personnel and the model are presented in table 3.4 and 3.5.

Table 3.4: Medical personnel ratings

Patient ID	Medical Personnel ID	Credibility Rating	Reliability Rating	Performance Rating
1	1	0.84	0.92	0.88
1	2	0.76	0.82	0.78
1	3	0.90	0.88	0.92
2	1	0.82	0.86	0.90
2	2	0.79	0.82	0.76
2	3	0.88	0.90	0.84
3	1	0.86	0.82	0.78
3	2	0.90	0.88	0.92
3	3	0.78	0.84	0.86
4	1	0.88	0.90	0.84
4	2	0.92	0.86	0.90
4	3	0.86	0.88	0.92
5	1	0.90	0.88	0.92
5	2	0.84	0.92	0.88
5	3	0.82	0.86	0.90
6	1	0.88	0.84	0.86
6	2	0.86	0.82	0.88
6	3	0.92	0.90	0.84
7	1	0.90	0.88	0.92
7	2	0.84	0.92	0.88
7	3	0.82	0.86	0.90
8	1	0.88	0.90	0.84
8	2	0.92	0.86	0.90
8	3	0.86	0.88	0.92
9	1	0.90	0.88	0.92
9	2	0.84	0.92	0.88
9	3	0.82	0.86	0.90
10	1	0.88	0.84	0.86
10	2	0.86	0.82	0.88
10	3	0.92	0.90	0.84

Table 3.5: User ratings for the trust model

Entity ID	Credibility	Reliability	Security	Privacy	Transparency
1	0.84	0.92	0.88	0.89	0.85
2	0.76	0.82	0.78	0.86	0.82
3	0.90	0.88	0.92	0.92	0.88
4	0.82	0.86	0.90	0.85	0.80
5	0.79	0.82	0.76	0.88	0.84
6	0.90	0.92	0.85	0.86	0.92
7	0.86	0.82	0.78	0.88	0.84
8	0.90	0.88	0.92	0.90	0.88
9	0.78	0.84	0.86	0.85	0.80
10	0.86	0.82	0.84	0.88	0.86
11	0.88	0.90	0.86	0.82	0.84
12	0.92	0.84	0.88	0.90	0.86
13	0.86	0.88	0.92	0.82	0.80
14	0.84	0.82	0.80	0.88	0.86
15	0.90	0.86	0.84	0.92	0.88
16	0.42	0.65	0.38	0.28	0.52
17	0.62	0.48	0.55	0.42	0.49

Ten different patients provided their ratings for the 3 medical personnel based on based on credibility, reliability, and performance of the medical personnel. The ratings are scaled between 0 and 1, with higher values indicating a higher level of trustworthiness in the respective aspect. To compare the trustworthiness of medical personnel based on credibility, reliability, and performance as perceived by different patients.

We computed the trustworthiness of the trust model for context aware health services based on the ratings of the 17 users. Their ratings for how trustworthy they rate the trust model is represented in table 3.5.

In this thesis, we collected ratings from ten different patients regarding the credibility, reliability, and performance of three medical personnel. These ratings were scaled between 0 and 1, where higher values indicated a higher level of trustworthiness in each respective aspect. The purpose was to compare the trustworthiness of the medical personnel based on the perceptions of different patients.

The credibility rating represents the measure of how trustworthy the patients perceive the medical personnel to be in terms of their expertise, knowledge, and professionalism. It indicates the level of trust or belief the patients have in the medical personnel's capabilities.

The reliability rating refers to the measure of how reliable the patients perceive the medical personnel to be in consistently delivering accurate and dependable healthcare services. It reflects the level of trust or confidence the patients have in the medical personnel's ability to perform consistently.

The performance rating represents an overall assessment of the medical personnel's performance as perceived by the patients. It considers various factors, including credibility, reliability, and possibly other aspects of the patient's experience. It provides an overall evaluation of the medical personnel's performance.

Each row in table 3.4 corresponds to a specific patient and medical personnel interaction. The values in the columns indicate the ratings for credibility, reliability, and performance for each interaction. For example, in the first row, Patient ID 1 interacting with Medical Personnel ID 1, the credibility rating is 0.84, the reliability rating is 0.92, and the performance rating is 0.88. These ratings are derived from the patients' direct interactions with the medical personnel based on their subjective experiences.

The range of 0-1 is commonly used in trust calculations as a normalized or standardized measure. It allows for easier interpretation and comparison of trust values across different contexts and datasets. A rating of 0 represents no trust or complete distrust, while a rating of 1 represents full trust or complete trustworthiness. This standardized range provides a clear and intuitive understanding of the trust values, with values closer to 1 indicating higher levels of trust. In the context of this thesis, the ratings for credibility, reliability, and performance were scaled to the range of 0 -1 to represent the level of trust in each aspect. By using this range, the equation can calculate the overall direct trust value within the same standardized framework, enabling comparison and analysis of trust levels among different interactions and medical personnel.

CHAPTER FOUR

RESULTS AND DISCUSSION

In this section, we present and discuss the results. The trust model proof of concept explained in section 3.2 demonstrates the patients and medical personnel adoption of context-aware e-health services once they were guaranteed their information was secure therefore, they could trust the service.

4.1 Results

To compute the trust values based on the test data we have presented in table 4 we computed the trust values as illustrated below:

Table 4.1: Trust model ratings.

Entity ID	Credibility	Reliability	Security	Privacy	Transparency	Trust Rating	Normalized Trust Rating
1	0.84	0.92	0.88	0.89	0.85	3.021	0.916
2	0.76	0.82	0.78	0.86	0.82	2.702	0.707
3	0.90	0.88	0.92	0.92	0.88	3.342	1.000
4	0.82	0.86	0.90	0.85	0.80	2.980	0.885
5	0.79	0.82	0.76	0.88	0.84	2.754	0.754
6	0.90	0.92	0.85	0.86	0.92	3.137	0.936
7	0.86	0.82	0.78	0.88	0.84	2.897	0.819
8	0.90	0.88	0.92	0.90	0.88	3.306	0.985
9	0.78	0.84	0.86	0.85	0.80	2.826	0.774
10	0.86	0.82	0.84	0.88	0.86	3.005	0.899
11	0.88	0.90	0.86	0.82	0.84	3.300	0.982
12	0.92	0.84	0.88	0.90	0.86	3.400	1.000
13	0.86	0.88	0.92	0.82	0.80	3.260	0.970
14	0.84	0.82	0.80	0.88	0.86	3.220	0.959
15	0.90	0.86	0.84	0.92	0.88	3.400	1.000
16	0.42	0.65	0.38	0.28	0.52	2.250	0.454
17	0.62	0.48	0.55	0.42	0.49	2.160	0.378

We used the direct trust computation formula we presented in (13) to compute trust rating of the trust model for context-aware e-health services based on credibility, reliability, privacy, and transparency.

$$Trust\ ratings = \alpha * (C + R + S) + \beta * (P + T)$$

We assigned the weightages as below:

α = 0.6

β = 0.4

Credibility, reliability, and security (α).

are fundamental factors in establishing trust in the context-aware e-service. These factors directly impact the perception of trustworthiness and dependability. Giving higher weight to these factors reflects the significance of these aspects in the overall trust rating.

Privacy and transparency (β).

Privacy and transparency are critical factors in establishing trust, particularly in contexts where personal data or sensitive information is involved like in the case of health. Placing importance on privacy and transparency highlights the value placed on protecting user information and ensuring transparency in operations. Although slightly lower in weight compared to α, β still carries a substantial weight to acknowledge the significance of privacy and transparency in the trust rating.

Below is the computation of the trust ratings using direct trust computation formula illustrated in (13): -

For Entity 1:

$$Trust\ Rating = \alpha * (C + R + S) + \beta * (P + T)$$

= 0.6 * (0.84 + 0.92 + 0.88) + 0.4 * (0.89 + 0.85)

= 3.021

$$Normalized\ Trust\ Rating = \frac{(Trust\ Rating - Min\ Trust\ Rating)}{(Max\ Trust\ Rating - Min\ Trust\ Rating)}$$

= (3.021 - 2.702) / (3.342 - 2.702)

= 0.916

For Entity 2:

$$\text{Trust Rating} = \alpha * (C + R + S) + \beta * (P + T)$$

$$= 0.6 * (0.76 + 0.82 + 0.78) + 0.4 * (0.86 + 0.82)$$

$$= 2.702$$

Normalized Trust Rating = (Trust Rating - Min Trust Rating) / (Max Trust Rating - Min Trust Rating)

$$= (2.702 - 2.702) / (3.342 - 2.702)$$

$$= 0.707$$

For Entity 3:

$$Trust\ Rating\ =\ \alpha\ *\ (C\ +\ R\ +\ S)\ +\ \beta\ *\ (P\ +\ T)$$

$$= 0.6 * (0.90 + 0.88 + 0.92) + 0.4 * (0.92 + 0.88)$$

$$= 3.342$$

$$Normalized\ Trust\ Rating = \frac{(Trust\ Rating\ -\ Min\ Trust\ Rating)}{(Max\ Trust\ Rating\ -\ Min\ Trust\ Rating)}$$

$$= (3.342 - 2.702) / (3.342 - 2.702)$$

$$= 1.000$$

The calculated trust ratings for entity 1, 2, and 3 are 3.021, 2.702, and 3.342, respectively. The Normalized Trust Ratings are 0.916, 0.707, and 1.000, respectively, after normalizing the values to be between 0 and 1. We computed the trust ratings for the other 17 users using the formulas explained above.

Transparency presents the level of transparency in the medical personnel and context-aware system's operations and decision-making processes. The patients categorize their experience high, medium, or low, based on the availability and clarity of information provided by the system and the medical personnel. Security reflects the security measures implemented to protect patient data and ensure the confidentiality and integrity of the medical personnel and context-aware system, established on the robustness of security practices in place.

Privacy hints to the extent to which the medical personnel and the context-aware system protect the patient medical based on adherence to privacy regulations and patient consent practices. Lastly reliability represents the reliability, availability and dependability of the medical personnel and the context-aware system in delivering accurate and timely services. This we base system uptime, accuracy of recommendations, and responsiveness of the medical personnel.

To evaluate the trustworthiness of our trust model for context aware e-health services we evaluate its performance using precision, recall, and F-score as illustrated in code 4 in the appendices.

The code imports necessary libraries and modules: `*numpy*` for numerical operations, `*train_test_split*` for splitting the data, `*LinearRegression*` for the trust model, and `*precision_score*`, `*recall_score*`, and `*f1_score*` for calculating evaluation metrics.

Step 1 prepares the data by defining the input features (`*features*`) and the corresponding trust ratings (`*trust_ratings*`). The features are represented as a 2D array, where each row represents a sample, and each column represents a specific feature. The features are as presented in table 3.5, they include credibility, reliability, privacy, transparency, and security. The trust ratings are represented as a 1D array.

Step 2 splits the data into training and testing sets using the `*train_test_split*` function. The `*test_size*` parameter specifies the proportion of the data allocated for testing, which is set to 20% in this case. The `*random_state*` parameter ensures reproducibility of the split.

Step 4 selects a linear regression model by creating an instance of the `*LinearRegression*` class and assigning it to the variable `model`.

Step 5 trains the linear regression model by calling the `fit` method on the `model` object, passing the training data (`*X_train*` and `*y_train`)* as arguments.

Step 6 sets a threshold value for classification, which is assigned to the variable `threshold`. This threshold is used to convert the predicted trust ratings into binary labels.

Step 7 makes predictions on the testing data by calling the `*predict*` method on the `*model*` object and passing the testing features (`*X_test*`) as input. The predicted trust ratings are compared to the threshold, and the result is converted into binary labels (0 or 1) using the `*astype*(int)` function.

Step 8 calculates the precision, recall, and F-score by calling the respective functions (`*precision_score*`, `*recall_score*`, and `*f1_score*`) and passing the true binary labels (`*y_test_bin*`) and the predicted binary labels (`*y_pred*`) as arguments.

Finally, it prints the calculated precision, recall, and F-score.

The precision represents the proportion of correctly predicted positive cases (high trust ratings) among all the predicted positive cases. The recall represents the proportion of correctly predicted positive cases among all the actual positive cases. The F-score is the harmonic means of precision and recall, providing a balanced measure of the model's performance.

By printing these metrics, we assess the performance of the trust model in predicting trust ratings, specifically evaluating how well it identifies positive cases (high trust ratings) based on the chosen threshold.

Comparing the precision, recall, and F-score of our trust model with the scores existing trust models for example with the Context-Aware Trust-Based Personalized Services model" proposed by Otebolaku & Lee (2018) discussed in section 2.4.2 their precision value was 0.8, recall: 0.57 and F-score: 0.67. In terms of precision, our trust model outperforms their as we have achieved perfect precision on 1. In terms of recall, our trust model significantly outperforms the framework, indicating that it has a better ability to correctly identify trustworthy instances. Lastly, the F-score, which considers both precision and recall, shows that out trust model performs better than the framework.

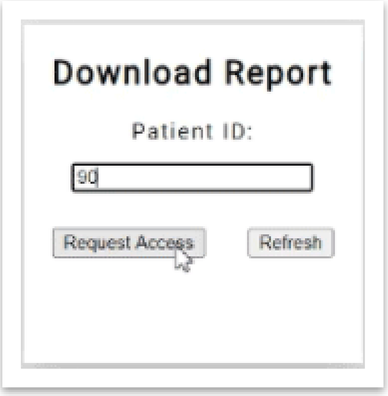
Overall, based on the results and comparison, our trust model has better performance in terms of precision, recall and F-score.

Table 4.2: Tests cases results explanation

Test Name	Test Scenario	Result
Registration	System functionality Test	In this test scenario the users were able to successfully register once they keyed in a valid email address, unique username and password that met the minimum set requirements.
Login	System functionality Test	Only registered users can login to the system on condition they provide a valid combination of login credentials.
Request access	System functionality and Trust test	Doctors who have successfully registered and are considered as trusted either directly or indirectly by the patients are the only ones who can request access to the patients records successfully.
Grant access	System functionality and Trust test	Patients can only grant access to doctors who are trusted. The model abstracts the trust computation from the customer.
Revoke access	System functionality and Trust test	Patients revoke access to doctors whom they distrust or were not satisfied with their service, they also provide feedback which is used to compute indirect trust.
Upload Records	System functionality	Doctors can successfully upload the patient’s laboratory results; doctors note among other documents
Updating and Deletion of records	Immutability	Changes made to record to are appended as new records and no record is deleted.
Monitoring System	System Functionality	The system continuously monitors patients' health status and triggers alerts in case of abnormal patterns or emergencies. Help is dispatched based on the patients’ location.
Access Log	System Functionality	Access logs are maintained, recording all instances of user access and activity for auditing purposes
Authentication	System Functionality	Users are required to authenticate themselves using valid login credentials to access the system.
Audit Trail	System Functionality	An audit trail is generated, capturing and storing all system activities for later review and analysis.
Trust Evaluation	Trust test	The trust model accurately evaluates the trustworthiness of authorized users based on direct and indirect trust factors.

Performance	System performance	The system demonstrates efficient performance, handling multiple user requests and data processing in a timely manner.
Data Encryption	System Functionality	Patient contextual and health information is encrypted, ensuring data confidentiality and security.
Access	System Functionality	Access permissions are properly enforced, preventing unauthorized users from accessing sensitive patient information.
Usability	System Functionality	Users find the trust model and system features easy to understand and navigate, resulting in a positive user experience.
Concurrency	System Functionality	The system handles concurrent user interactions without data conflicts or performance degradation.

For the context aware e-health service system to adapt to changes in context. Different users should have different access rights; patients' access is restricted to only one's record. Upon login the doctor request access as illustrated in figure 4.1 to view a patient's data.

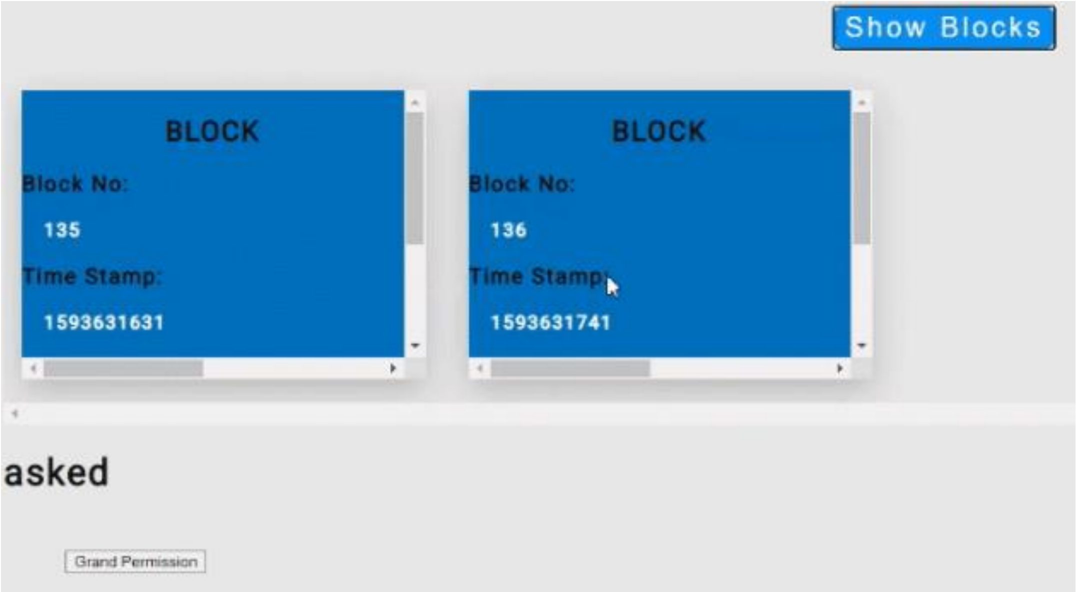


Download Report

Patient ID: 90

Figure 4.1: Doctor requests access to the patient's records.

On the patient's login screen, they see the notification to grant the doctor access to their records as illustrated in figure 4.1.



Block No:
135
Time Stamp:
1593631631

Block No:
136
Time Stamp:
1593631741

Figure 4.2: Patient granting the doctor access to their records.

Trust, the trust model is secure from unauthorized access, use and disclosure of patient’s information. The patients are guaranteed that only authorised personnel can access their information. The integrity of the data is also maintained as any modification done on the data is appended as a new block and data cannot be deleted due to the immutable nature of blockchain. The patients can choose a privacy policy they trust, and it satisfies their current need.

Authentication, before access the system the doctor and the patients shall have to sign in with valid credentials .When a patient has an attack that requires the assistance of a medical personnel or to be taken to a hospital, a sensor will be triggered that will alert the medical personnel near the patient and the hospital of the patient’s current medical condition, their exact location and the activity they were conducting during or before the attack. Once the patient has been fully assisted that is the patient’s condition has been managed or he/she has been taken to hospital their context.

Adaptability the model should be able to adapt the context of the users and function effectively.

4.2 Discussion

Trust in Context-Aware e-health services is paramount; without it the users will be less likely adopt the service. To ensure we increase the use of these services we implement a trust model that maintains integrity, privacy, and confidentiality of the users' personal data. The precision, recall and F-score values in section 4.1 clearly stipulate that the trust model evaluated in this thesis upholds users trust and the model proves the trustworthiness of the service.

Section 4.1 presents the results of a trust model for context-aware e-health services. The trust values were computed based on the test data presented in table 3.4 and 3.5. The trust ratings were calculated using a formula that considered credibility, reliability, security, privacy, and transparency. The weightages for these factors were assigned as $\alpha = 0.6$ and $\beta = 0.4$.

The computed trust ratings and normalized trust ratings for several entities were presented in table 4.1. The trust ratings were calculated for each entity by combining the respective factors with the assigned weightages. Normalized trust ratings were obtained by normalizing the trust ratings to be between 0 and 1. Section 4.1 explains the significance of each factor in establishing trust, such as credibility, reliability, security, privacy, and transparency. It mentions that transparency reflects the level of transparency in operations, while security represents the measures to protect patient data. Privacy indicates the extent to which patient medical information is protected, and reliability refers to the dependability of the system in delivering accurate and timely services.

Additionally, we present the python code snippet that evaluates the trustworthiness of the trust model using precision, recall, and F-score. The code uses a linear regression model and splits the data into training and testing sets. The performance metrics are calculated based on the predicted trust ratings and the corresponding true labels. Comparing the precision, recall, and F-score of the trust model with the context aware trust based personalized services model shows that our trust model performs better in terms of precision, recall, and F-score. The context-aware trust model proposed by Otebolaku and Lee (2018) did not consider whether consumption context is trustworthy or not. The user preferences were retrieved without consideration for characterizations by context and trust. Thus, recommendations were generated based only on the preference values. When the number of values were increased in the traditional models the accuracy level decreased. On the other hand, the Reputation Experience and Knowledge (REK) Trust Evaluation Model evaluated trustworthiness based on three factors: reputation, experience, and knowledge. They computed the trust values using direct and indirect values without considering the context and did not evaluate the precision, recall and f-score of their model trustworthiness as it compares to other models, as we have done in this model.

Lastly, table 4.1 explains the results of specific test cases related to system functionality, such as registration and login tests.

Overall, the thesis section 4 discusses the computation of trust values, the evaluation of the trust model's performance, and compares it with two other model, highlighting its superior performance.

CHAPTER FIVE

CONCLUSION AND FUTURE WORK

In this thesis, a proof-of-concept trust model for context aware e-health service is implemented, it facilitates maintaining data privacy and promoting trust for context-aware e-health services. The main objective of this thesis is to formulate a trust model that guarantees users privacy when using context-aware e-health services. The model incorporates existing trust models; these models are Reputation, Experience & Knowledge (REK) Trust Evaluation Model, Trust-Based Context-Aware Recommender Systems and Trust modelling computation. The context used in this model is *who* and *where,* whereby *who* is the patients, the medical personnel trying to access the patient's data, and *where* is the location of the patient in case of an emergency, the medical personnel requesting access and the emergency services team to be dispatched. The model adopted the concept of direct and indirect trust to compute the trustworthiness of the medical personnel by computing the medical personnel's trust degree. Direct trust is achieved from the patients experience with the medical personnel while indirect trust is derived from recommendations of other patients. The medical personnel are considered trustworthy if their trust value is greater than or equal to 0.5. To maintain the integrity of the data, the model integrates to an Ethereum blockchain solution. The patients and medical personnel register by providing their personal data. The patient's data from context aware applications is uploaded automatically and a random ounce used to encrypt the files, and a secret is stored in blockchain. The patient provides access to the medical personnel who is then able to see and fetch the patient's address and data. To achieve our main objective, we drilled it down into three specific objectives namely: examine trust concerns affecting context-aware e-health services, investigate existing trust models to construct groundwork for the formulation of the trust model, formulate a trust model for derived from existing trust models and blockchain, lastly investigate the efficiency of the trust model in three above in preserving trust. In chapter one we examined trust concerns affecting context-aware e-health services. These trust concerns include privacy, integrity, and confidentiality of the model throughout the thesis we extensively explain how we address this concerns using blockchain, access control, trust evaluation and authentication. In chapter two we investigate existing trust models to construct groundwork for the formulation of the trust model. The trust models investigated include the REK trust model, trust degree model, context-aware trust model, computational trust model, trust-based context-aware recommender systems, context-based trust management model and blockchain based access control framework. After the evaluation of this models, we were able to refine and formulate our trust model for context-aware e-health services as we have described in chapter three of this thesis. Lastly in chapter three and four we conducted experiments and validated the trustworthiness of our model this enabled us to determine the effectiveness of the model. We computed the trust values assigned to our medical personnel and measured the effectiveness of the model using precision, recall and F-score metrics. Apart from using metrics we also evaluated the proof-of concept system using various test cases in section 3.5 and discussed the test results in section 4.1. These test cases investigated the functional capabilities and the trustworthiness of the model. The functional test cases were to determine if the service performs as expected and the trustworthiness test was to confirm that the service and especially the medical personnel can be trusted. A key contribution of this model is the incorporation of blockchain to ensure data integrity, this feature lacks in trust models we evaluated. Although the model is effective in ensuring only trusted medical personnel and authenticated patients can access the service, we have evaluated its effectiveness only in the context-aware e-health sector we did not extend it to other domains. We also limited our context to who and where because of time and resources. For future work we can develop mechanisms to dynamically adapt the trust model based on evolving contexts and changing user preferences. This can involve real-time updates and adjustments to trust evaluations based on contextual changes and user feedback.

REFERENCES

Almenárez-Mendoza, F., Marín-López, A., Campo, C., & García, C. (2006). PTM: A pervasive trust management model for dynamic open environments. *IEEE International Conference on Pervasive Computing and Communications Workshops* . Pisa: IEEE International .

Altinisik, E., Nuhoglu, S., Cobanoglu, C., Sengul, M., Eryildiz, N., & Ergur, A. (2022). The Patient Perspective of Telemedicine in the Context of COVID-19 Pandemic. *Bulletin of Science, Technology & Society*, 39–53.

Aneka, K., Jeremy, S., & Laura, R. (2020). The COVID-19 pandemic: new concerns and connections between eHealth and digital inequalities. *Journal of Information, Communication and Ethics in Society*.

Ayuku, B., Okeyo, G., Mindila, A., & Chemwa, W. (2021). A Trust Model for Context-Aware E-Health Services. *iCatse International Conference on IT Convergence and Security (ICITCS2021)* (pp. 177-189). Springer.

Baker, D. W. (2020). Trust in Health Care in the Time of COVID-19. *JAMA*, 2373-2375.

Barasa, E., Rogo, K., Mwaura, N., & Chuma, J. (2018). Kenya National Hospital Insurance Fund Reforms: Implications and Lessons for Universal Health Coverage. *Health systems and reform*, 346–361.

Bernadette, A., Anthony, K., Ngaira, D., & Pepela, W. (2019). *Enhancing Health Information System for Evidence based decision making in the Health Sector.* Nairobi: The Health Sector Monitoring and Evaluation Unit - Ministry of Health, Kenya. Retrieved from: https://www.health.go.ke/wp-content/uploads/2019/01/HIS-POLICY-BRIEF-.pdf

Chew, E., Teo, S. H., Tang, W. E., Ng, D. W., Koh, G. C., & Teo, V. H. (2023). Trust and Uncertainty in the Implementation of a Pilot Remote Blood Pressure Monitoring Program in Primary Care: Qualitative Study of Patient and Health Care Professional Views. *JMIR human factors*.

Dey, A. k. (2001). Understanding and Using Context. *Pers. Ubiquitous Comput*, 4-7.

Fadelli, I. (2019). PAL: A wearable system for context-aware health and cognition support.

Gelogo, Y. E., & Kim, H.-K. (2015). Integration of Wearable Monitoring Device and Android Smartphone Apps for u-Healthcare Monitoring System.

Gubert, L. C., da Costa, C. A., & Righi, R. d. (2020). Context awareness in healthcare: a systematic literature review. *Universal Access in the Information Society*, 245-259.

Hasselgren, A., Rensaa, J.-A. H., Kralevska, K., Gligoroski, D., & Faxvaag, A. (2021). Blockchain for Increased Trust in Virtual Health Care: Proof-of-Concept Study. *Journal of Medical Internet Research*, 23-30.

Integrated Health Services . (2023). Retrieved from World Health Organization: https://www.who.int/teams/integrated-health-services/about

Katarzyna Krot, I. R. (2021). How Public Trust in Health Care Can Shape Patient Overconsumption in Health Systems? The Missing Links. *International journal of environmental research and public health*, 3860.

Kim, S. H., Lee, S., & Lee, K. (2018). Context-Aware Mobile Health for Diabetes Management. *Healthcare Informatics Research*, 165-172.

Krukow , K., Nielsen, M., & Saassone, V. (2008). Trust models in ubiquitous computing.

Kwereba, J., & Shah, K. (2022). *Mobile Clinics: An Innovative Model Of Health Service Delivery*. Nairobi: Africa Helath Business.

M'Hamed, A., Zerkouk, M., Husseini, A. E., & Messabih, B. (2013). Towards a Context Aware Modeling of Trust and Access Control Based on the User Behavior and Capabilities. *International Conference on Smart Homes and Health Telematics.*

Ministy of Health, & Ministry of Public Health Sanitation. (2012). *Kenya Health Policy.* Nairobi.

Mousa, A., Bentahar, J., & Alam, O. (2021). Multi-dimensional trust for context-aware services computing. *Expert Systems with Applications*, 114592.

Narayanan, A. (2016). *Bitcoin and Cryptocurrency Technologies.*

Negin, R., Rahmani, A. M., & Mohsenzadeh, M. (2009). A Context-based Trust Management Model for Pervasive Computing System. *International Journal of Computer Science and Information Security*.

Obosi, J. O. (2019). Decentralized Governance in the Management of Urban Health Care Systems in Developing Countries. *Open Journal of Political Science*, 189-202.

Odhiambo, E. M. (2015). *A framework For Implementation of E-Health in Kenya Public Hospitals (Thesis).* Nairobi: Strathmore University.

Onyancha, & et.al, H. (2020). *Kenya Community Health Strategy 2020 - 2025.* Nairobi: Ministry of Health.

Otebolaku, A., & Lee, G. M. (2018). A Framework for Exploiting Internet of Things for Context-Aware Trust-Based Personalized Services. Mobile Information Systems. *Mobile Information Systems*, 1-24.

Ouaddah, A. (2017). A blockchain based access control framework for the security and privacy of IoT with strong anonymity unlinkability and intractability guarantees.

Paganelli, F., Spinicci, E., & Giuli, D. (2008). ERMHAN: A Context-Aware Service Platform to Support Continuous Care Networks for Home-Based Assistance. *International Journal of Telemedicine and Applications*, *13*.

Santhiyagu, J., Kumar, B. R., & Prabhu, G. G. (2017). Context aware mobile computing: A survey. *International Journal of Academic Research and Development*, 131-132.

Shankari, B., Saravanagru, R. A., & Thangavelu, A. (2011). Context Aware Healthcare Application. *International Journal of Computer Applications*, 7–12.

Siddiqui, M. H., S. S., U. M., & Sheikh, R. I. (2020). Context-aware healthcare systems: A review of literature and future directions. *Journal of Ambient Intelligence and Humanized Computing*, 771-789.

Tan, Z., Wang, X., & Wang, X. (2016). A Novel Iterative and Dynamic Trust Computing Model for Large Scaled P2P Networks. *Hindawi Publishing Corporation*.

Tedros Adhanom Ghebreyesus, J. Y. (2019, October 10). *Delivering quality health services: a global imperative for universal*. Retrieved from WHO: https://www.who.int/publications/i/item/9789241513906

Tortorella, R. A., & Kinshuk. (2017). A mobile context-aware medical training system for the reduction of pathogen transmission.

Truong, N. B., Um, T.-W., Zhou, B., & Lee, G. M. (2017). From Personal Experience to Global Reputation for Trust Evaluation in the Social Internet of Things. *IEEE Global Communication (GLOBECOM).* Singapore.

Vahiny, S., Ankur, G., Najam, U. H., Shabaz, Mohammad, D., & Ofori, I. (2022). Blockchain in Secure Healthcare Systems: State of the Art, Limitations, and Future Directions. *Security and Communication Networks*, 1-15.

Wan, T. C., Chieng, H. C., & Ho, J. W. (2018). Context-Aware Computing Applications in Health Care. *A Review. Journal of Medical Systems*, 42-54.

Wigmore, I. (2016, May). *techtarget.com*. Retrieved from WhatIs.com: https://whatis.techtarget.com/definition/context-awareness

World Health Organization, & World Bank Group. (2018). *Delivering quality health services : A global imperative for universal health coverage.* Genève: The World Bank. Retrieved from https://www.worldbank.org/en/topic/universalhealthcoverage/publication/delivering-quality-health-services-a-global-imperative-for-universal-health-coverage.

Zalo, M. (2020, August 20). *The Emerging Practice of Telemedicine and the Law: Kenya's Stance.* Retrieved from strathmore.edu: https://cipit.strathmore.edu/the-emerging-practice-of-telemedicine-and-the-law-kenyas-stance/

APPENDICES

Appendix I: Code for Extracting device details

```
private String getDeviceDetails(String userAgent) {
    String deviceDetails = UNKNOWN;
    Client = parser.parse(userAgent);
    if (Objects.nonNull(client)) {
        deviceDetails = client.userAgent.family
                                  + " " + client.userAgent.major + "."
```

Appendix II: Code for Extracting User IP

We use the code 3 to extract the users IP address.

```
private String extractIp(HttpServletRequest request) {

    String clientIp;

    String clientXForwardedForIp = request

      .getHeader("x-forwarded-for");

    if (nonNull(clientXForwardedForIp)) {
```

Appendix III: Code for Getting user location.

Once we have their IP address, we can get the location of the user using code 4:

```
private String getIpLocation(String ip) {

    String location = UNKNOWN;

    InetAddress ipAddress = InetAddress.getByName(ip);

    CityResponse = databaseReader

      .city(ipAddress);
```

Appendix IV: Code for: Trust Model evaluation

```
import numpy as np
from sklearn.model_selection import train_test_split
from sklearn.linear_model import LinearRegression
from sklearn.metrics import precision_score, recall_score, f1_score

# Step 1: Prepare the data
features = np.array([
    [0.84, 0.92, 0.88, 0.89, 0.85],
    [0.76, 0.82, 0.78, 0.86, 0.82],
    [0.90, 0.88, 0.92, 0.92, 0.88],
    [0.82, 0.86, 0.90, 0.85, 0.80],
    [0.79, 0.82, 0.76, 0.88, 0.84],
    [0.90, 0.92, 0.85, 0.86, 0.92],
    [0.86, 0.82, 0.78, 0.88, 0.84],
    [0.90, 0.88, 0.92, 0.90, 0.88],
    [0.78, 0.84, 0.86, 0.85, 0.80],
    [0.86, 0.82, 0.84, 0.88, 0.86],
    [0.88, 0.90, 0.86, 0.82, 0.84],
    [0.92, 0.84, 0.88, 0.90, 0.86],
    [0.86, 0.88, 0.92, 0.82, 0.80],
    [0.84, 0.82, 0.80, 0.88, 0.86],
    [0.90, 0.86, 0.84, 0.92, 0.88],
    [0.42, 0.65, 0.38, 0.28, 0.52],
    [0.62, 0.48, 0.55, 0.42, 0.49]
])

trust_ratings = np.array([3.021, 2.702, 3.342, 2.980, 2.754, 3.137,
2.897, 3.306, 2.826, 3.005, 3.300, 3.400, 3.260, 3.220, 3.400, 2.250,
2.160])

# Step 2: Split the data
X_train, X_test, y_train, y_test = train_test_split(features,
trust_ratings, test_size=0.2, random_state=42)
```

```
# Step 3: Select a regression model
model = LinearRegression()

# Step 4: Train the model
model.fit(X_train, y_train)

# Step 5: Set the threshold for classification
threshold = 0.8

# Step 6: Make predictions and convert to binary labels based on threshold
y_pred = (model.predict(X_test) >= threshold).astype(int)
y_test_bin = (y_test >= threshold).astype(int)

# Step 7: Calculate precision, recall, and F-score
precision = precision_score(y_test_bin, y_pred)
recall = recall_score(y_test_bin, y_pred)
fscore = f1_score(y_test_bin, y_pred)

print("Precision:", precision)
print("Recall:", recall)
print("F-score:", fscore)
```

Appendix V: Publications During MSc Period

Ayuku, B., Okeyo, G., Mindila, A., & Chemwa, W. (2021). A Trust Model for Context-Aware E-Health Services. *iCatse International Conference on IT Convergence and Security (ICITCS2021)* (pp. 177-189). Springer.