PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
Ministry of Higher Education and Scientific Research
Mohamed Khider University – BISKRA

Faculty of Exact Sciences, Natural Sciences and Life

Computer Science Department

N° d'ordre : RTIC25/M2/2022

Thesis

Presented to obtain the academic master's degree in

Computer Science

Option: Networks and Technologies of Information and Telecommunications (RTIC)

Trust in Healthcare Domain

By:

TABAL SIRINE

Defended on ..../..../……., in front the jury composed of :

BELOUNNAR SALIHA	President
HAMIDA Ammar	
NAIDJI ILYES	Examiner

Academic year 2021-2022

Acknowledgements

First of all, we have to say thanks to Allah that I have been and I am good enough physically and mentally to study and reach this place, peace upon our prophet Mohammed. And I wish I will meet my died mother and my father for helping me in this path.

I would also like to thank my project supervisor Dr. Hamida Ammar for guiding, giving the helping hand and being a good listener to me, without her supervising I wouldn't do that project to the fullest.

Finally, I would like to acknowledge my family and friends who supported me during my time here at the university.

Table of contents

List of figures

List of tables

General Introduction

In nowadays, we are facing a huge use in trust in wireless sensor networks in this world. Wire-less Sensor Networks enjoy great benefits due to their low-cost, small-scale factor, smart sensor nodes.

A Wireless Sensor Network (WSN) consists of sensor nodes deployed over a geographical area for monitoring physical phenomena like temperature, humidity, vibrations, seismic events, and so on. Those nodes can communicate with each other or directly to the sink. Each sensor has four essential parts which are “sensing unit”, “processing unit”, “transceiver unit” and “the power unit” although we can find some kind of sensors that have other optional units such as the mobilizer.
We can use it in healthcare domain to improve the QOS of the healthcare domain.

However, trust in health care has declined during the past half-century. Many factors are thought to contribute to the declining trust in clinicians and organized medicine, including the rise of managed care and related financial incentives, highly publicized conflicts of interest between clinicians and pharma and device manufacturers, limited time for communication, fragmentation of the patient-clinician relationship, and consumerism.

From the best ways to conserve the trust in healthcare of the messages between the nodes. So, if we choose a good solution of trust, we can provide a good trust health system between systems.

The structure of this thesis is as following:

Chapter 1: This chapter explains generally the mobile platform and trust in it, its classification ...etc. Between all of these, we talked also about trust factor’s, the mobile platform architectures.

Chapter 2: In this chapter we’ll talk about trust in healthcare and its major factors also the possible ways to make it way efficient to implement.

Chapter 3: at this stage we will talk about our trust solution and how to implement it and realize it and how to make the binominal distributed system possible.

Chapter 4: At the end will present in this last chapter the simulation tools, network model and the results of the simulation.

Chapter one

Trust in mobile platform

1.1 Introduction

Trust plays a crucial role in our social life to facilitate coordination and cooperation for mutual benefits. The concept of trust has been studied in disciplines ranging from economics to psychology, from sociology to medicine, and to information science. It is hard to say what trust exactly is because it is a multidimensional, multidisciplinary and multifaceted concept. We can find various definitions of trust in the literature. Common to these definitions are the notions of confidence, belief, faith, hope, expectation, dependence, and reliance on the goodness, strength, reliability, integrity, ability, or characters of a person or thing. Generally, a trust relationship involves two parties: a trustor and a trustee. The trustor is the person or entity that holds confidence, belief, faith, hope, expectation, dependence, and reliance on the properties of another person or thing, which is the object of trust – the trustee. With the rapid growth of global digital computing and networking technologies, trust becomes an important aspect of the design, establishment and maintenance of a secure computing system and a mobile system.

This chapter introduces the basic knowledge of trust, trust modeling and trust management. We review some basic technologies of trust management in mobile platforms, which include trust evaluation on mobile applications, mobile trusted computing platform, trust management of mobile software components, and mobile malware detection. Further discussions on open research issues and future research trends on mobile platforms trust management are also provided. Finally, we conclude the chapter in the last section.

1.2 Mobile platform

Mobile platform as a service (*mPaaS*) is a specialized type of *PaaS* designed to provide an integrated development environment (*IDE*), deployment platform, lifecycle management and analytics for mobile/web applications [1].

Enterprises often use *mPaaS* to create custom applications for both internal and customer-facing use. This capacity can help support a BYOD environment and

productivity applications without requiring mobile application developers for support for mobile devices.

Like most *PaaS* offerings, *mPaaS* isn't a single thing but rather a suite or ecosystem of related tools designed to provide a wide assortment of features and functionalities that can vastly accelerate mobile application development, testing, deployment, management and updating/patching.

MPaaS is designed to be quick and easy; often eliminating much of the traditional time-consuming processes involved in software development projects such as mobile application development. Thus, *mPaaS* typically requires no coding skills. An *mPaaS* integrated development environment usually features an object-oriented drag-and-drop interface to simplify development of *HTML5* or native applications with direct access to a device's sensors, GPS, accelerometer, camera, microphone and other functions. *MPaaS* often supports multiple mobile operating systems.

Delivered over the web through a browser, *mPaaS* might support public cloud, private cloud and on-premises storage. Web applications can be created and then connected to back ends with a few lines of code. *MPaaS* is generally a leased cloud service with pricing per month that varies according to the number of devices and supported features.

1.3 Mobile architecture

Mobile applications can be classified into mainly three categories :

- Browser based mobile web applications : These are pure web applications that are designed using responsive web design techniques that can cater to a variety of devices and form factors [2].
- Native mobile applications : These applications are built for specific mobile platforms , such as iOS, Android, that can fully leverage the device capability. Normally native mobile applications are built using *SDKs* provided by mobile platforms.

- Hybrid applications : These applications can be developed using web technologies such as JavaScript and can also partially leverage the device capabilities using a web to native layers.

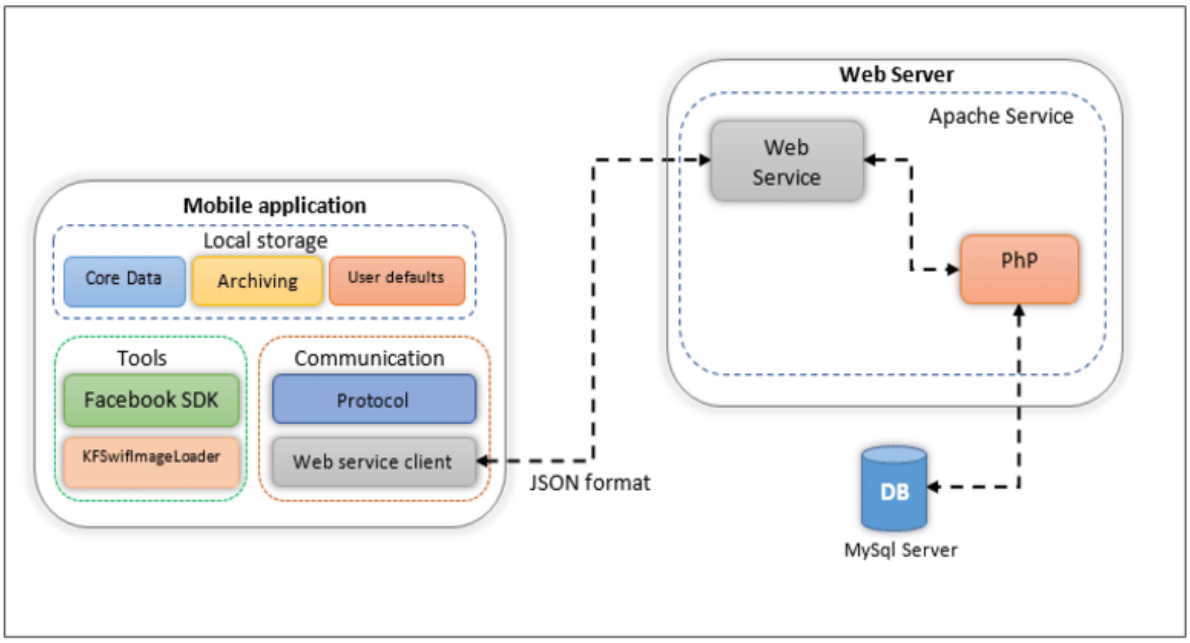

Figure 1 : Mobile architecture [3].

1.3.1 Architecture of a native mobile application

Native mobile application fully utilizes the device capability. Figure 2 and Figure 3 depict architectures for *iOS* and Android native applications :

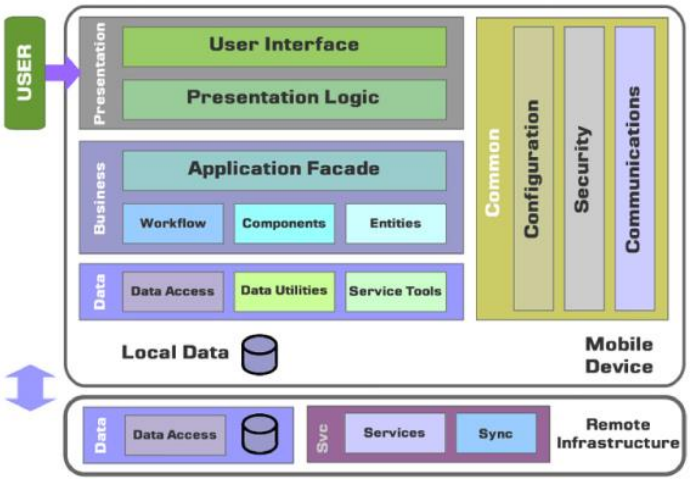

Figure 2 : iOS based native Mobile application.

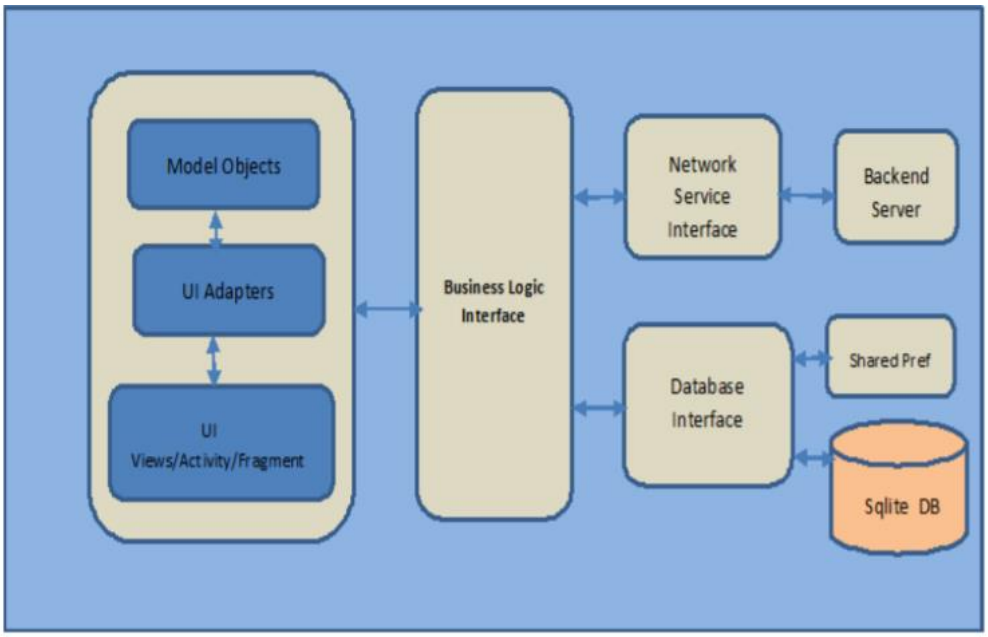

Figure 3 : Architecture of Android based native Mobile App.

1.3.2 Architecture of a hybrid mobile application

Hybrid application targets different mobile Operating system with a very thin application shell with a web view. One-time application development is needed with the publication to various mobile application stores. Hybrid applications are very popular in-developing Single Page Application responsive applications for Tablets and Smart Phones. The key components of the hybrid application are given in Figure 4. The Mobile application development using hybrid application development has :

- benefits:
  - Usability: Ability to use device-specific
- features to improve usability
  - Maintainability: Easy maintenance of codes and ease of future enhancements
  - Extensibility: Support for multiple platforms
  - Device Diversity: No additional effort for supporting new devices
  - Portability: to various mobile platforms
  - Faster time to market : through quicker deployment to mobile application stores.

We can have specific mobile services which consolidate the required back-end services and provides optimized data for the mobile application.

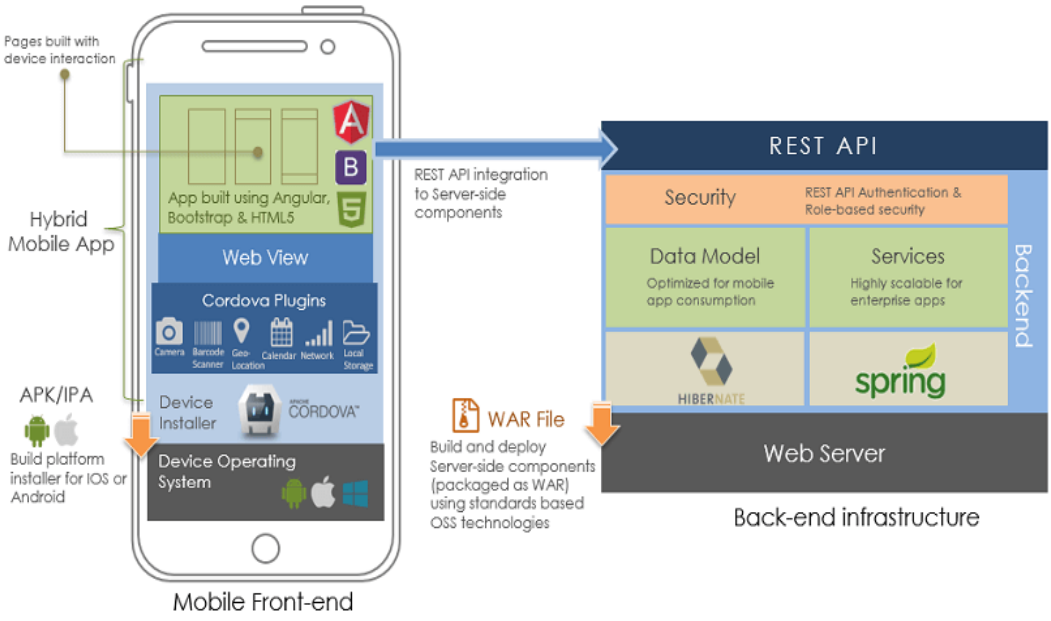

Figure 4 : Architecture of a hybrid Mobile App.

1.3.3 Architecture of a mobile web application

Mobile web applications are mainly developed using responsive design. *It provides* provides flexible and responsive layouts that automatically adjust themselves for various devices and form factors which include the following techniques: Fluid design contains the page size in relative units. Flexible images and media flexible images would automatically scale based on the screen resolution. CSS3 media queries would provide flexible layouts and use various devices dependent CSS style rules. Figure 5 shows the responsive layout displayed over multiple devices.

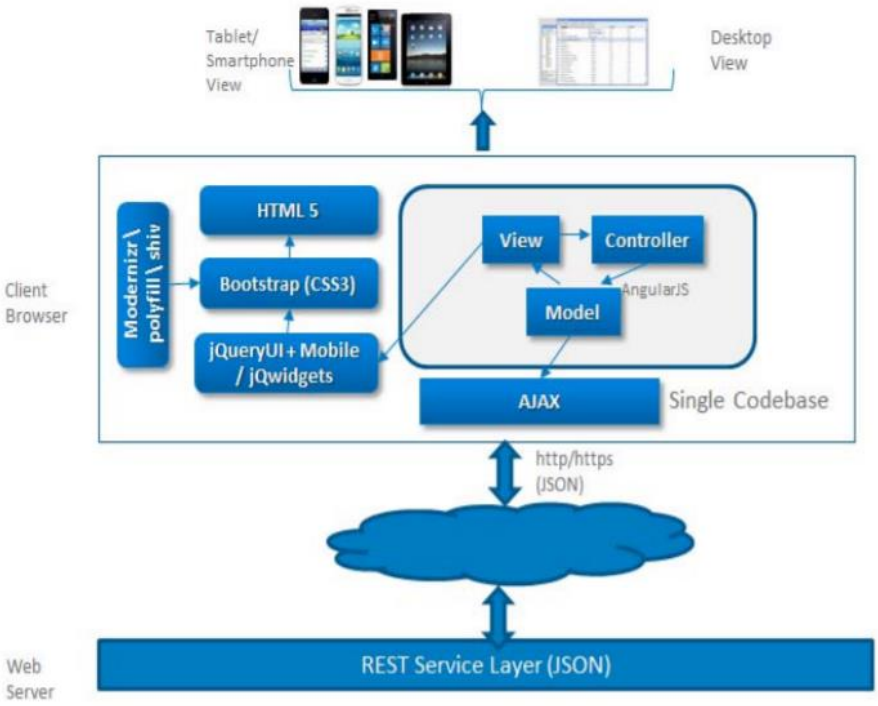

Figure 5 : Mobile web application using RWD.

1.4 Fields of mobile application

Currently, mobile application development has taken a turn to the future. With the advancements in technology mobile applications is becoming one of the biggest and important aspects of development. Mobile phones are right now the lifeline for a lot of people across the globe. Hence it is important that applications are developed in a way that will help the numerous mobile users. Here are some of the trends in mobile application development [4].

1.4.1 Augmented and virtual reality applications

Augmented reality and virtual reality are the future of mobile application development. It has been a revolutionary tool in the field of entertainment. Games like *Pokemon go* have captured the market and have opened horizons for a lot of similar augmented reality applications. Virtual reality too has been very useful for a vast majority of businesses. Building these applications is the current market trend and will certainly be on the top of the year end.

1.4.2 Artificial intelligence

The whole world is slowly moving towards artificial intelligence. Even mobile operating system are slowly integrating artificial intelligence to help the user with their day to day lives. *Siri*, *Prisma*, *Google Now* are just some of the artificial intelligence applications currently in the market and they are growing at an exponential pace. Artificial intelligence is the future and mobile artificial intelligence is a huge trend in 2017.

1.4.3 Cloud-based mobile applications

Cloud-based mobile applications have been on the rise since a couple of years. A lot of applications are now fetching data directly from the cloud in order to take *minimum space* in the *internal memory* of the smart phone. These are very important advancements as users can now use huge mobile applications without the worrying about data storage and thus makes it easier for them overall.

1.4.4 Location-based services

With the rise of the internet and availability of *GPS* in the mobile phone's location-based services have been on the rise. Providing location-based services is a huge trend currently as the users can be given real-time information. Apart from that, it can be used in various fields like navigation, travel, retail, and security. Beacon technology has also become increasingly popular and in 2017 it has become a trend worth following.

1.4.5 Application security

With the whole world slowly going online *cyber security* is a very important aspect of mobile application development. With users saving sensitive data on their mobiles it has become imperative to make sure security in the applications is top notch. In 2017 has seen a rise in security features in most applications and this trend will continue for the future.

1.4.6 Internet of things

With the fast advancing technology, it has become more and more important to save time in the day-to-day chores and use that time for meaningful tasks and thus Internet of

things has gained a lot of momentum. By connecting basic appliances with the internet one can use their whole home from their mobiles. The ability to integrate these appliances to exchange data offers great opportunities for the future.

1.4.7 Wearable technology

Wearable technology has been on the rise in the past two years with products like apple watch firmly established in the market wearable technology offers enormous opportunities in various fields like healthcare and sports. Mobile applications are being linked with wearable technology to provide seamless integration for the user.

1.4.8 Enterprise mobile applications

Enterprise mobile applications are a trend as they give us the freedom to connect with multiple people and help to manage and optimizing business processes. Being able to communicate to coworkers and employees through mobile devices while managing the work is something very important in the current market.

1.5 Trust, Trust modeling, and Trust issues

According to [5], [6][7], *trust* in computing is modeled after human relationships and as such is strongly associated with security; that is, generically the concept of *trust* , and security, may be applied to other areas, for example, a party may "*trust*" another party to deliver secure quality service, in which case *trust* becomes a measure of the "*security*" of service-availability. Authors in [8] classified *trust* into *objective* and *subjective trust*. *Objective trust* is concerned with the impressions directly between two parties; *subjective trust* involves the impressions obtained from third parties.

1.5.1 Trust

A *trust* is a fiduciary relationship in which one party, known as a *trustor*, gives another party, the *trustee*, the right to hold title to property or assets for the benefit of a third party, the beneficiary. *Trusts* are established to provide legal protection for the *trustor's* assets, to make sure those assets are distributed according to the wishes of the *trustor*, and to save

time, reduce paper work and, in some cases, avoid or reduce inheritance or estate taxes. In finance, a *trust* can also be a type of closed-end fund built as a public limited company [9].

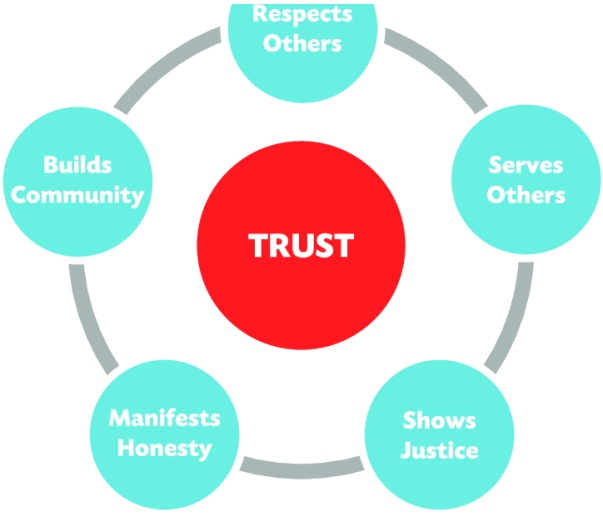

Figure 6 : Trust model [10].

1.5.2 Trust modeling

The concept of *trust* and/or *trust management* has received considerable attention in engineering research communities as *trust* is perceived as the basis for decision making in many contexts and the motivation for maintaining long-term relationships based on cooperation and collaboration. Even if substantial research effort has been dedicated to addressing *trust-based mechanisms* or *trust metrics* (or computation) in diverse contexts, prior work has not clearly solved the issue of how to model and quantify *trust* with sufficient detail and context-based Adequacy. The issue of *trust* quantification has become more complicated as we have the need to derive *trust* from complex, composite networks that may involve four distinct layers of communication protocols, information exchange, social interactions, and cognitive motivations. In addition, the diverse application domains require different aspects of *trust* for decision-making such as emotional, logical, and relational *trust*. This survey aims to outline the foundations of *trust* models for applications in these contexts in terms of the concept of *trust*, *trust* assessment, *trust* constructs, *trust* scales, *trust* properties, *trust* formulation, and applications of *trust*. We discuss how different components of *trust* can be mapped to different layers of a complex, composite

network; applicability of *trust* metrics and models; research challenges; and future work directions [11].

1.5.3 Trust issues and solution

In the face of *trust* we will face many difficulty's and many challenges there for they will slow that process as we see :

We have discussed a variety of applications using the concept of *trust* in diverse do mains. Although the challenges of *trust* research may be unique depending on a domain, this section identifies and discusses the common design challenges and corresponding suggestions in developing *trust* models as follows:

- Identification of key *trust* dimensions. In any context, *trust* can be the basis for decision making closely related to achieving a system/application goal. Since dimensions of *trust* are numerous, it is not trivial to select key components of *trust* to maximize decision performance. Reflecting the notion of context dependency in the nature of *trust*, *trust* system designers should investigate the requirements of entities and/or information that can be directly related to achieving given goals of systems.
- Optimal balance of multiple objectives based on situational *trust*. T*rust assessment* is affected by many different factors particularly related to utility and risk analysis under the dynamics of a situation. Although trust can be estimated based on objective criteria, regardless of the level of objective trust.

1.6 Conclusion

In this chapter we see what is a mobile platform and what is a mobile architecture, we also took a deep dive in the fields of applications in the mobile world and the uses of theme in many ways. We also saw Trust, Trust Modeling, and Trust Management, and we define each one of them.

In the next chapter we will see deeply the conception of trust and also the healthcare domain and the relationship between each other.

Chapter Tow

Trust and Healthcare

2.1 Introduction

The concept of trust and/or trust management has received considerable attention in engineering research communities as trust is perceived as the basis for decision making in many contexts and the motivation for maintaining long-term relationships based on cooperation and collaboration. Even if substantial research effort has been dedicated to addressing trust-based mechanisms or trust metrics (or computation) in diverse contexts, prior work has not clearly solved the issue of how to model and quantify trust with sufficient detail and context-based adequateness. The issue of trust quantification has become more complicated as we have the need to derive trust from complex, composite networks that may involve four distinct layers of communication protocols, information exchange, social interactions, and cognitive motivations. In addition, the diverse application domains require different aspects of trust for decision making such as emotional, logical, and relational trust. This survey aims to outline the foundations of trust models for applications in these contexts in terms of the concept of trust, trust assessment, trust constructs, trust scales, trust properties, trust formulation, and applications of trust. We discuss how different components of trust can be mapped to different layers of a complex, composite network; applicability of trust metrics and models; research challenges; and future work directions.

In this chapter we will see the trust management and trust in health care domain and what's the problem that we will face and what is the solution that has been achieved.

2.2 Healthcare

Health care is a fundamental human good because it affects our opportunity to pursue life goals, reduces our pain and suffering, helps prevent premature loss of life, and provides information needed to plan for our lives. Society has an obligation to make access to an adequate level of care available to all its members, regardless of ability to pay [12].

Physicians regularly confront the effects of lack of access to adequate care and have a corresponding responsibility to contribute their expertise to societal decisions about what health care services should be included in a minimum package of care for all.

Individually and collectively as a profession, physicians should advocate for fair, informed decision making about basic health care that :

- Is transparent.
- Strives to include input from all stakeholders, including the public, throughout the process.
- Protects the most vulnerable patients and populations, with special attention to historically disadvantaged groups.
- Considers best available scientific data about the efficacy and safety of health care services.
- Seeks to improve health outcomes to the greatest extent possible, in keeping with principles of wise stewardship.
- Monitors for variations in care that cannot be explained on medical grounds to ensure that the defined threshold of basic care does not have discriminatory impact.
- Provides for ongoing review and adjustment in consideration of innovation in medical science and practice to ensure continued, broad public support for the defined threshold of basic care.

2.2.1 How to improve healthcare

As we come to the end of another fun-filled year in healthcare, so many conversations have been started about things we need to do, about ways we need to change, about how we can possibly do so much better.

We've been functioning in a system not truly of our making, a healthcare system that in the end doesn't do its best for everybody, and we have seen these divides highlighted and widening throughout this year like almost no other time before.

Almost without exception, we all have in mind an idealized healthcare system that works for everybody, every time. In our heart of hearts, we know what this would look like.

None of us would wish the healthcare system we have on our worst enemies, and we all wish for a healthcare system that would do for everybody as we think it should for those closest to us -- for our loved ones, friends, colleagues, and community.

We have to create a system that lets everybody have equal access to the best care, the right care at the right time, and figure out how to make this system blinded to someone's ability to pay.

True, in a capitalist system, there will always be haves and have-nots, and there will always be those who wish to pay more for premium services. But if we make the basics the best we possibly can, if no one gets denied what they truly need, if no one ever needs to choose medications over food or rent, then we will probably have gone a long way towards making things better.

We need to expand access, we need to build up the primary care foundational workforce that drives the healthcare system, we need to pay a living wage across all medical specialties (so that our brightest minds don't opt out of a career that is seen as less prestigious because of the lackluster image that has been foisted upon it), and to all members of the healthcare team.

Figure 7 : A Solution for Health care.

We need everybody in this system working towards a common goal, taking care of our patients and making sure that all of those working in healthcare are taken care of as well. In every way. Right now, in this country and around the world, things look pretty rough.

It seems that nobody can agree on anything, and that any time anybody has an idea, there is an upwelling of ideological opposition that ends up with no winners, and a toxic environment that discourages discussion and the exchange of ideas, cooperation, or finding effective solutions [13].

2.3 Trust management

The understanding of the trust approach in it's requirement and also it's relationship with the healthcare domain, we will start with start by defining the assets of the trust management and its proprieties as we see in follow :

2.3.1 Definition

Due to the nature of WSN deployment being prone to the surrounding environment and suffering from other types of attacks in addition to the attacks found in traditional networks, other security measurements different from the traditional approaches must be in place to improve the security of the network. The trust establishment between nodes is a must to evaluate the trustworthiness of other nodes, as the survival of a WSN is dependent upon the cooperative and trusting nature of its nodes [14].

Security and trust are two tightly interdependent concepts and because of this interdependence, these terms are used interchangeably when defining a secure system. However, security is different from trust and the key difference is that, it is more complex and the overhead is high. Trust has been the focus of researchers for a long time, from the social sciences, where trust between humans has been studied to the effects of trust in economic transactions [15-16]. Although intuitively easy to comprehend, the notion of trust has not been formally defined. Unlike, for example, reliability, which was originally a measure of how long a machine can be trustworthy, and came to be rigorously defined as a probability, trust is yet to adopt a formal definition [14].

2.3.2 Trust proprieties

Trust is a very complicated concept that is influenced by many measurable and non-measurable properties. It is highly related to security since ensuring system security and user safety is a necessity to gain trust. However, trust is more than security. It relates not only security, but also many other factors, such as *goodness*, *strength*, *reliability*, *availability*, *ability*, or other characters of an entity. The concept of *trust* covers a bigger scope than security, thus it is more complicated and difficult to establish, ensure and maintain, in short manage *trust* than *security* [18].

- *Trustee's* objective properties, such as a trustee's security and dependability. Particularly, reputation is a public assessment of the trustee regarding its earlier behaviors and performance.
- *Trustee's* subjective properties, such as trustee honesty, benevolence and goodness.
- *Trustor's* subjective properties, such as *trustor* disposition and willingness to trust
- Trustor's objective properties, such as the criteria or policies specified by the trustor for a trust decision
- Context that the trust relationship resides in, such as the purpose of trust, the environment of trust (e.g., time, location, activity, devices being used, their operational mode, etc.), and the risk of trust. It specifies any information that can be used to characterize the background or situation of the involved entities. Context is a very important factor influencing trust. It specifies the situation where trust exists. Dey [18] defined the ability of a computing system to identify and adapt to its context as context-awareness. Notably, the influencing properties of trust could be different or paid different attention by a trustor in different situations and contexts.

There are many trust proprieties: Global trust, Composite trust… [13].

2.3.3 Trust management computation

The volatile growth of the internet and globalization that influences every facet of life are fueled by the rapid acceleration of computing/communication technologies. Although security is a major concern, we must also protect ourselves from false/misleading information provided by some information/service providers. Traditional security mechanisms cannot protect against this type of threat. Trust management mechanisms on the other hand can provide protection [19]

2.3.3.1 Trust composition

This refers to the components that are considered in trust computation and it involves two major modules namely: quality of service (QoS) trust and social trust [20]. *QoS* refers to the expectation of an IoT entity to provide superior quality in its functionalities. *QoS trust* utilizes some trust properties, such as competence, reliability, task completion capability, and cooperativeness, to measure the value of trust

2.3.3.2 Trust propagation

Trust propagation refers to the way of propagating trust information to other entities. Under this form of propagation [6], two main schemes can be identified:

- Distributed trust refers to IoT entities autonomously propagating trust and observations to other IoT entities they interact with or encounter without the necessity for a centralized entity [22].
- Centralized trust requires the presence of centralized entities. It can exist as either a virtual trust service or a physical cloud that is implemented by IoT devices [22].

2.3.3.3 Trust aggregation

This refers to the most appropriate method of aggregating trust information, which is then evaluated by the entity itself (*direct evaluation*) or by other entities (*indirect evaluation*) [8]. This component aggregates information using weights, which might be static or dynamic. The static is calculated in accordance with the entity attributes. The

original trust on both communication parties is built on both sides' trust attributes. To make proper dynamic trust decisions, trust management must rely on context information when assigning weights to each property [23]. In the literature, there are various models of trust aggregation including the belief theory, fuzzy logic, Bayesian inference, weighted sum, and regression analysis [21].

2.3.3.4 Trust update

This component decides when to update the values of trust. The updating of the trust information occurs periodically (*time-driven*) by applying a trust aggregation or after a transaction or event affects the QoS (*event-driven*) [22].

2.3.3.5 Trust formation

This refers to whether trust computation is based on either one trust attribute (single-trust) or the use of multiple attributes (multi-trust). Besides, these components are chiefly concerned with what weights are put on QoS and social trust attributes from trust [21].

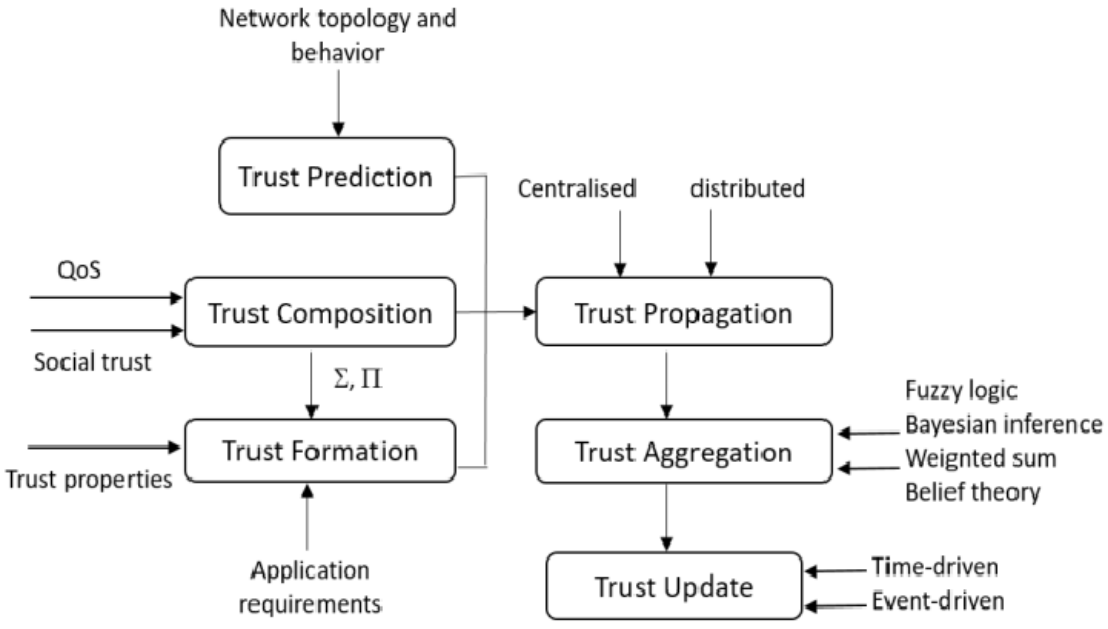

Figure 8: Trust management computation [22].

2.4 Trust in healthcare system

The continuous development of the Internet and the construction of new computing infrastructures are improving opportunities for the provision of e-health [24]. E-health is the use of information and communication technologies to acquire, store, share or transfer healthcare-related information. Moreover, it supports providing healthcare services to users. The main application areas of e-Health include the following: Electronic Health Records (EHRs) [25-26], ubiquitous & pervasive health [22], telemedicine & telecare services [27], and decision support systems [24]. With the advancement in technology, EHR systems, with the goals of improving patient care and outcomes, enable HCPs to monitor health status online and store information derived from medical examination in EHRs, which may include personal information, laboratory results, medical treatments, diagnoses, medications, immunization status, and even some sound and image data. EHR aggregates patient medical information originating from multiple independent HCPs located in the same city, country or across the country border.

2.5 Attacks on trust healthcare

Following are some possible attacks in trust healthcare [25]:

- Bad-mouthing Attack: This attack occurs when a dishonest entity tries to hurt the reputation of one or more entities by assigning unfairly low ratings to them.
- Collusion Attack: In this attack, a group of entities work collectively to either boost each other’s reputation or conspire against one or more entities in the network.
- Ballot stuffing Attack: To falsely raise reputations service providers engage in many fake dealings.
- Whitewashing Attack: Sometime when an entity gets a bad reputation, he/she may leave the system and try tore-register under a completely different identity.
- Denial of Service Attack: This attack engages resources in meaningless activities and jams traffic to affect the availability of the reputation system

2.6 Requirements for the TRSS in the healthcare domain

Designing efficient TRSs in the healthcare domain clearly raises research issues at several levels. The requirements and challenges identified in this section will serve as a reference model for measuring the performance and features of existing TRSs.

- **Adaptive Behavior**: TRSs rely on feedback provided by others, thus avoiding or reducing the influence of unfair ratings in reputation systems, which constitute a fundamental problem. Unfair behavior may be explained by a variety of reasons, including personality/habit, business gains, irrepressible, victim exploitation and randomness. The reputation system can only be safeguarded against malicious.
- **Fair Treatment of New Users:** Determining initial reputation score for new entities is a challenge in reputation systems. If the new entities are assigned a very low default reputation value, they may never be selected and may not get a chance to improve their reputation. For example, in the P2P environment, in which the group of peers works collaboratively in the medical consultation, or research, a peer might be reluctant to obtain services from the peer with a low reputation value. However, assigning a high default reputation score will provide an unfair advantage to new entities who are still unknown to the system. Initially, when a new entity joins the system, the construction of a trust evaluation based on little or no information can be completed by gathering information from direct and indirect sources. The TRS should define a mechanism that can represent the uncertainty associated with a new entity without penalizing them or providing an unfair advantage. TRS must distinguish between entities with unknown quality and with poor long-term performance. For this purpose, service consumers should be encouraged to provide ratings. Otherwise, the TRSs will face the problem of free riders [28]. Consumers are more willing to provide feedback about a service provider if they are given an incentive.

- **Context/Criteria Compatibility:** Context/criteria knowledge is a critical requirement for TRSs, especially when calculating trust. Chen et al. [29] describe context as the set of environment friendly circumstances and settings that governs an entity behavior or in which the event that occurred is of interest to the user. Some of the requirements that should be addressed by a context-aware TRS in the healthcare domain include :
    - Allowing the service consumer to select the information that characterizes the context,
    - Tagging the trust information according to the context,
    - Performing a context-aware reputation computation by categorizing the context and using a specific reputation computation technique based on the type of context,
    - Adapting the trustworthiness computation and assessment according to the context,
    - Performing an implicit context reconfiguration,
    - Performing autonomously.
- **Privacy and Confidentiality :** TRSs should guarantee privacy both to the entity owing the reputation and the entities providing the recommendations. In the healthcare domain, one important requirement for TRS is rating secrecy, that is, the service consumer identity information is kept secret to avoid retaliation and privacy violation. The TRSs should ensure that participating entities do not retrieve identification information about each other. Designing a mechanism for TRSs that achieves both trust and anonymity is challenging. Revenge rating is an issue, especially in TRSs developed for the healthcare domain, where a service provider (e.g., doctor), by acting as a service consumer (e.g., patient), may take revenge by spoiling the reputation of another service provider. For example, a heart physician as a service consumer may give bad ratings to an oncologist as a service provider, who consequently ma spoil the reputation of that specific heart physician as a service consumer

- **Changing Identity :** A user who registers himself/herself with several forged identities at the TRS allows him/her to forge or control a large amount of entities and acts on behalf of them (Sybil attack). If a user has a bad reputation, it would be in his interest to change his identity so that he can start as a new user. If a service consumer is allowed to have multiple identities, it may disrupt the accuracy of the TRS computation by sending false data collusively or by sending multiple reputations for a single task. Having multiple identities also threatens the privacy of the user. A sybil attacker with external knowledge can exploit the received recommendations to infer the private interests of users [30]. To discourage sybil attack, one simple solution can be to ask for some information at the time of registration, such as the device International Mobile Equipment Identity (IMEI) number, and restrict each device to the maximum registration of one account. Other solutions include (i) penalizing the user by imposing a computational cost on identity creation and (ii) averaging all the recommendations received by identities with an IP address in the same zone. Due to the mobility feature in a mobile network, detection and handling of sybil defence is quite different compared with online networks. There is a need for sybil-resilient schemes that prevent adversaries from distorting reputation scores.
- **Reliability:** Reliability is concerned with the number and quality of information resources used to calculate reputation scores. Experience, knowledge, and credibility are important elements and must be considered while computing reputation. A greater number of reliable sources used to calculate the trustworthiness of an entity will allow computing the reputation reliably. Incomplete information leads to inaccurate information and, in turn, affects the computation of the reputations.

In this table we will see TRS requirements for mitigating different attacks.

Attack	Adaptive behavior	Context/Criteria Compatibility	Changing identities	Privacy and Confidentiality
Traitor attack	X			

Misbehavior		X	X	
Denial of service attack				X
Newcomer attack				X

Table 1 : attacks on trust healthcare .

2.7 Binomial Distribution-based Trust Management Scheme for Healthcare-oriented Wireless Sensor Network

This trust management scheme is base a lot of Bernoulli trials, Bernoulli trials is a random experiment with exactly two possible outcomes which are success and failure in which the probability of success is the same every time the experiment is conducted. so the interaction between the nodes is addressed as the success or failure of each Bernoulli trials, we extract the trust value and reputation of the node is take from the probability distribution function of the binomial distribution, and this reputation is updated continuously between nodes until obtain the new trust value, so this method more suitable and has low computational complexity for this types of networks like HWSN.

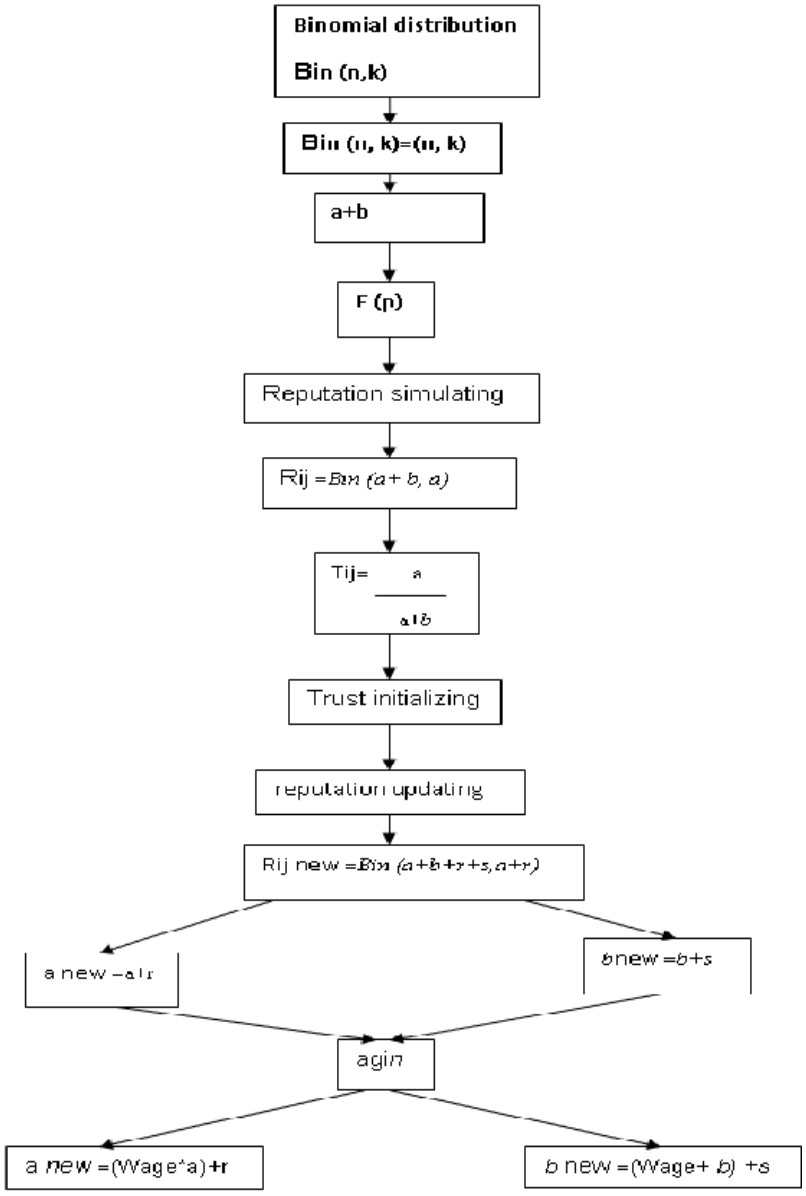

Figure 9 : BDTMS flowchart [33].

Bin(n, k) it is the binomial distribution which is represent the probability of *k* success in *n* experiments.

$$Bin(n,k) = C(\mathrm{n,\ k})\, p^k (1-p)^{n-k}$$

This expression represent the binomial distribution which the *p* is the probability of success and the *C(n, k)* represent as the formula as follow :

$$C(n,k) = \frac{n!}{k!\,(n-k)!}$$

$a+b$: when interaction start between two nodes , there are two cases which binomial distribution (cooperation , non-cooperation) , so , a represent the number of cooperation and *b* represent the number of non-cooperation.

In this research they assume that the probability of a which cooperation is *p*, for that, we can calculate the probability distribution of node reputation *p* using binomial distribution by the function

$$F(p) = Bin(a+b, a)\frac{(a+b)!}{a!\,b!}p^a(1-p)^b$$

- **Reputation simulating :** R_{ij} express the reputation of node I to node j. the maximum value of the previous function *f(p)* which is the probability distribution represent the greatest probability of *p* so $p = a\ (a+b)$ here , there are two values of *p* , the first is $p= 1$ and it is the maximum value , the second is $p = 0$ and it is the minimum value , so the trust of node I to node j is expressed as : $Tij=a\ (a+b)$.
- **Trust initializing :** this step is important for the interaction , so define the body nodes as the same initial trust value, they assume that the nodes trust value is 0.5 so from the previous formula find that and obviously shown that the trust value is 0.5 for the both a and b.so this point shows a difference at the initialization , if the values of *a* and *b* smalls this mean that there are a few interactions , so they obtained trust value are not enough in the same time if the values of a and b are large that mean there are a big number of interactions, therefore , select the appropriate a and b value.
- **Reputation updating :** $\mathrm{R}_{\mathrm{ij}}^{\mathrm{new}} = \mathrm{Bin}(\mathrm{a}+\mathrm{b}+\mathrm{r}+\mathrm{s}, \mathrm{a}+\mathrm{r})$ this function represent the latest reputation between nodes where the *r* represent the number of cooperation and the *s* represent the number of non-cooperation , and the current number of interactions is $(a + b + r + s)$.
- **Aging :** the factor Wage represents the aging weight. That factor is responsible for ensuring that all nodes are always cooperating together.
- **Indirect information :** the indirect information is when a node receives a trust evaluation about other node from its neighbor, in this case we cannot completely

believe the reputation information which is transferred by other nodes so for used that information we need to evaluate the reputation of the node so this is the new reputation (a^{new}_j, b^{new}_j) is:

$$\begin{cases} a_j^{new} = a_j + \dfrac{a_k}{b_k + a_k} \cdot a_j^k \\ b_j^{new} = b_j + \dfrac{a_k}{b_k + a_k} \cdot b_j^k \end{cases}$$

$$\begin{cases} a_j^{new} = a_j + \dfrac{a_k}{b_k + a_k} \cdot a_j^k \\ b_j^{new} = b_j + \dfrac{a_k}{b_k + a_k} \cdot b_j^k \end{cases}$$

In this expression, the F_d represent the detection flag, so if it value is 0, we said that the detected node is malicious if it value is not then it is a normal node. Where we can define the interval between the highest trust value $T_h(i)$ and the next highest trust value $T_h(i+1)$, $Tl(i)$ is the lowest trust value in a detection period.

This presented approach in is the only approach that treated the On-Off attack pattern, considered as an insider attack. For that, it exploited the propagation, the aggregation and the update modules. Otherwise, it using only the indirect trust.

2.8 Conclusion

In this chapter we give an overview about the trust management and its attacks in trust in healthcare also We have evoked in this chapter the various solutions to avoid as much as possible the attacks with the malicious behaviors in order to destroy the network. After comparing these solutions, we conclude that we need to provide a solution to improve the healthcare domain as we will see in the next chapter.

Chapter Three

Conception

3.1 Introduction

Trust is a salient feature in the context of healthcare, which is characterized by *uncertainty* and an *element of risk*. Trust is considered important because it indirectly influences the *quality of healthcare* based on patient *satisfaction*, *adherence* and the *continuity* of its relationship with healthcare professionals and *promotion* of an accurate and *timely diagnosis*. The *degree of trust* represents the opinion of patients about healthcare professionals and their willingness (based on their evaluation) to recommend a healthcare professional. So in this chapter we will give solution trust based intrusion detection and clustering considering the indirect trust and history trust.

3.2 Description of global conception

In this specific healthcare system that is defined in wireless sensor nodes detect each device in our healthcare system, in every sensor node, our proposed system should calculate the trust of each node using trust properties which are *direct trust* and *indirect trust* and *history trust*, every property of them has many factors like *data* trust, *communication* trust and *energy* trust, once we calculate the trust we should compare it by the trust threshold value and if the result is less than the threshold value that mean there is a malicious node, after we eliminate those bad nodes are detached from the network.

For *HWSN*, the trust management scheme involves the trust initialization, reputation distribution, trust/reputation information collection, modeling, transferring, the derivation of trust, trust decisions, and so on. Generally, the trust management scheme can be divided into the following four parts: collection, modeling, transferring and decision.

- Collection : refers to collecting node behaviors and trust/reputation information by interaction between nodes.
- Modeling : refers to representing the relationship between the reputation and trust.
- Transferring : involves the indirect reputation transfer and the trust value transfer.

- Decision : involves two aspects, the selection of the next hopping node and the punishment for those nodes of the low trust value.

After we eliminate those malevolent nodes, the rest of honest nodes were segregated into small clusters, every cluster of them chose a *cluster head* (CH) which act like a leader of that cluster, we use the multi-objective firefly algorithm (MOFA) to choose the cluster head, after that we will use the Binomial distribution-based trust management system to verify which is which bad nodes and trying to steal the sensitive data and which one belongs to our system.

The following figure shows the architecture of our system:

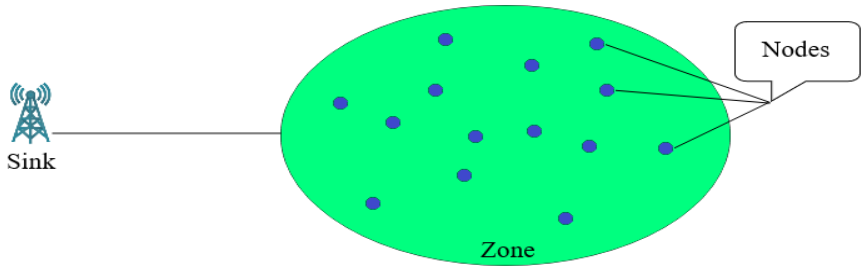

Figure 10 : Architecture of our trust based system .

3.3 Detail's description

In this part we will discuss in details our solution to improve trust in healthcare domain by using the binomial distribution managed system:

3.3.1 Honest sensor nodes

The honest sensor nodes are the type of node who will perform only it tasks like sensing data and sending it like temperature and wind speed, and it will not perform other malicious activities like modifying the type of data that we captured.

The schema below shows how we figure the honest sensor node:

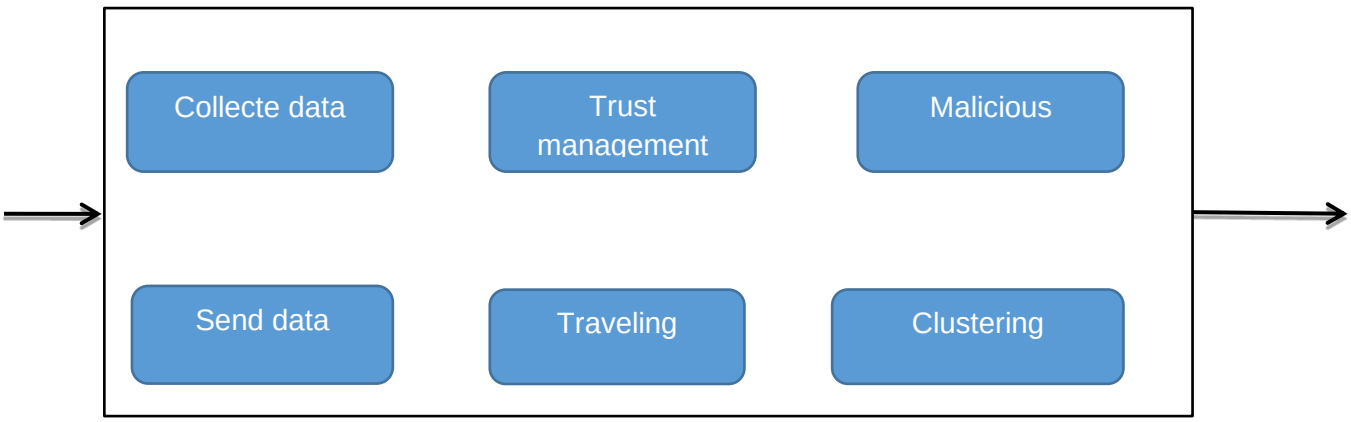

Figure 11: Honest node tasks

3.3.2 Malicious sensor nodes

In the beginning, the *malicious node* is like the rest of the nodes so that it performs the tasks required of it naturally without any hesitation in providing services as soon as possible, but after a period of time it starts doing strange things such as delaying or sending wrong information to other elements as well. This node can give negative opinions about honest nodes and as well as he can present positive opinions about malicious elements to cooperate with them on abnormal behavior that can cause serious consequences.

In another sense, Attacks can occur at any layer such as physical, link, network, transport, and application etc. Most of these routing protocols are not designed to have security mechanisms and it makes it even easier for an attacker to break the security for example, attacks at the physical layer of the network include jamming of radio signal, tampering with physical devices [34].

The malicious sensor node works as follow:

- Send false information to other elements as well
- This node can give negative views about the sincere contract F = -F
- And can also provide positive views on malicious items F = + F

3.3.3 Sink node

The *sink node* is very important in the wireless body area network because it *control* the sensor node and their behaviors all the time. It responsible to *collect data* from the sensor node and it can detect the attacker from it value of trust.

3.4 Detailed conception

In this part we will discuss in details our solution to improve trust in healthcare domain.

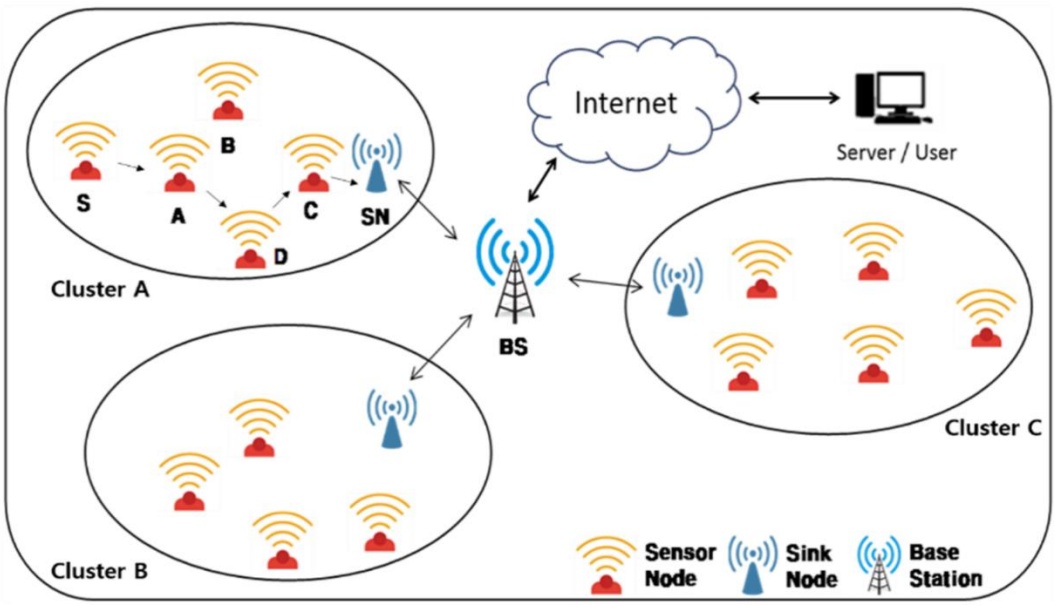

Figure 12 : Trust healthcare solution .

3.4.1 Sensor node deployments

First, we Randomly deploy sensor nodes in the network zone then we can divide it to clusters.

- **Step Partitioning:** In this step, the sink makes the partitioning of the network to clusters each cluster have its Cluster-head.
- **Step Data sensing:** after dividing each Group the sensors will automatically detect the data that we will aiming to capture.

- **Step data transmission:** In this last step, any source node that, the node will capture the data and sending to the cluster head, after that each cluster will send the data to the base station for treating.
- **Step trust calculation:** after sending the data we will calculate the trust value of each node we captured and each node to assure.
- **Step node deployments:** after each step of those each sensor node will change its position randomly and chose new cluster head based on MOFA algorithm.

Each step will be shown in the figures bellow:

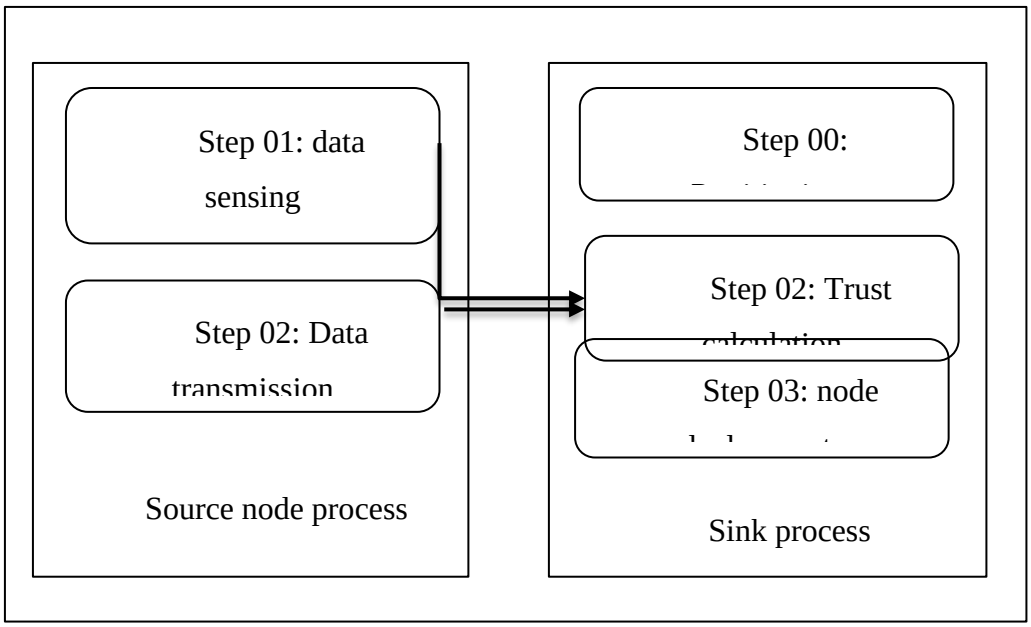

Figure 13 : Process of our conception .

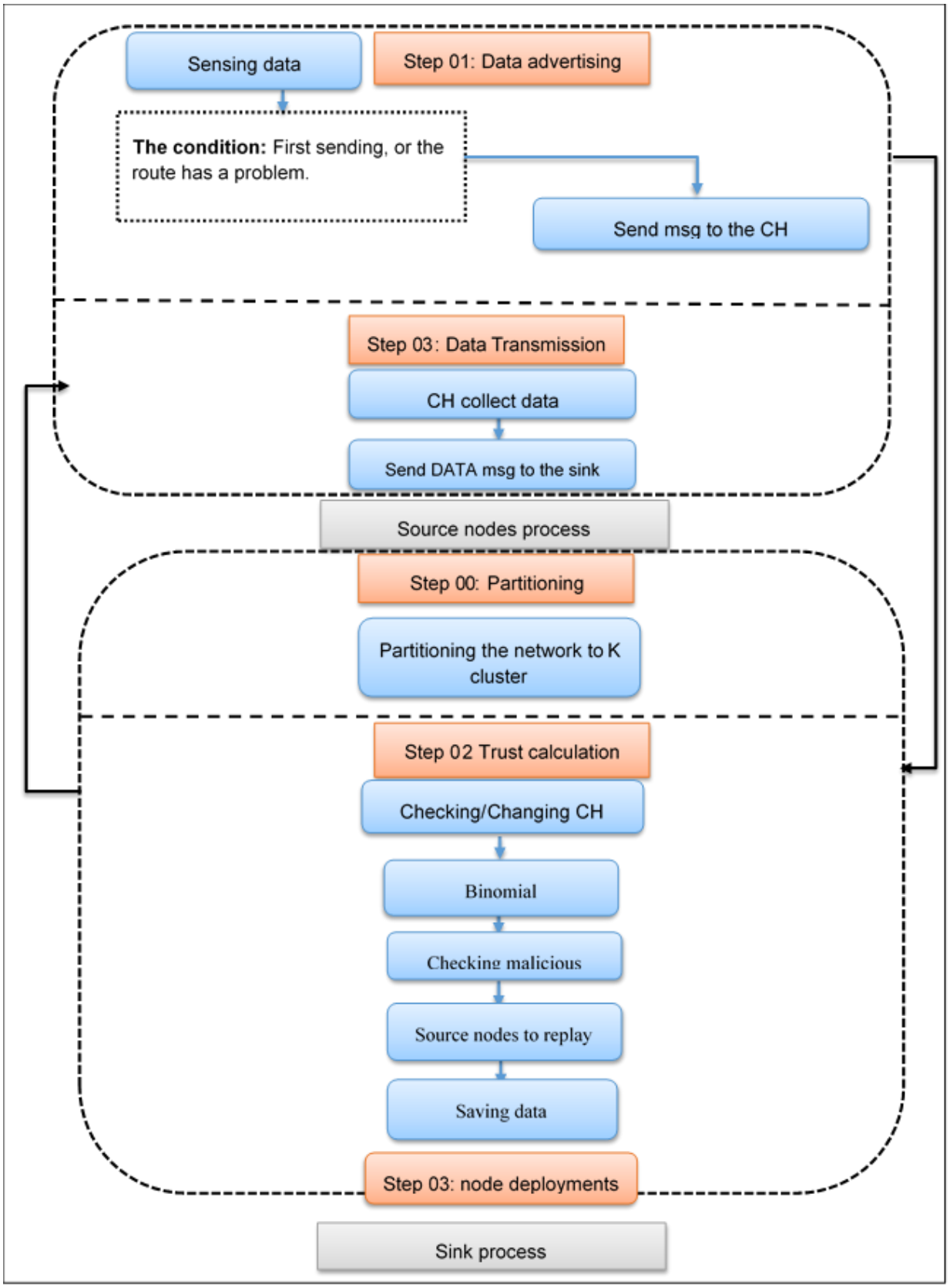

Figure 14 : Global architecture of our proposed solution.

3.4.2 Trust management

In this section, we will discuss and analyze the trust management scheme in the general sense, then propose a binomial distribution-based trust management scheme for HWSN.

- **Trust management scheme :** For HWSN, the trust management scheme involves the trust initialization, reputation distribution, trust/reputation information collection, modeling, transferring, the derivation of trust, trust decisions, and so on. Generally, the trust management scheme can be divided into the following four parts : collection, modeling, transferring and decision.
- **On-Off attack model :** The On-Off attack is an internal attack, which is very harmful. In this attack, a compromised node performs some good behaviors as a normal node or bad behaviors alternately. These behaviors appear non-stationary periodic characteristics. From the aspect of the trust management, the compromised node can obtain much higher trust value by continuously performing the good behaviors in a short period of time. Thereafter, it performs the bad behaviors during a long time intermittently, and the trust value of itself reduces slowly. When the trust value of itself drops to a certain extent, it performs the good behavior again. Hence, the trust value of itself ascends quickly, yet descends slowly.

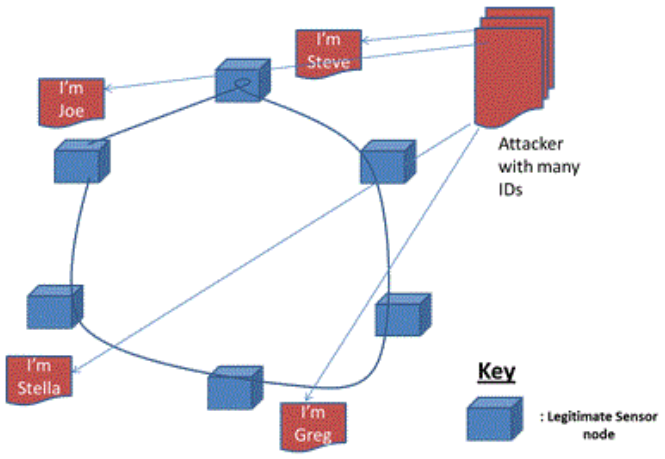

Figure 15 : Sybil attack in wireless sensor network .

- **Binomial distribution-based :** The binomial distribution is *n* repeated Bernoulli trials. In HWSN, the success or failure of the interaction between the nodes is addressed as the success or failure of each *Bernoulli trial*. Then, the probability distribution function of the binomial distribution is taken as the *reputation* of the node. The *reputation* is further updated by continuous interaction between nodes to obtain the new trust value. The binomial distribution expression has more direct descriptive on the interaction and cooperation between nodes in the network

Binomial distribution *Bin(n; k)* represents the probability of *k* successes in *n* experiments. It can be expressed as:

$$Bin(n,k) = C(n,k)p^k(1-p)^{n-k}$$

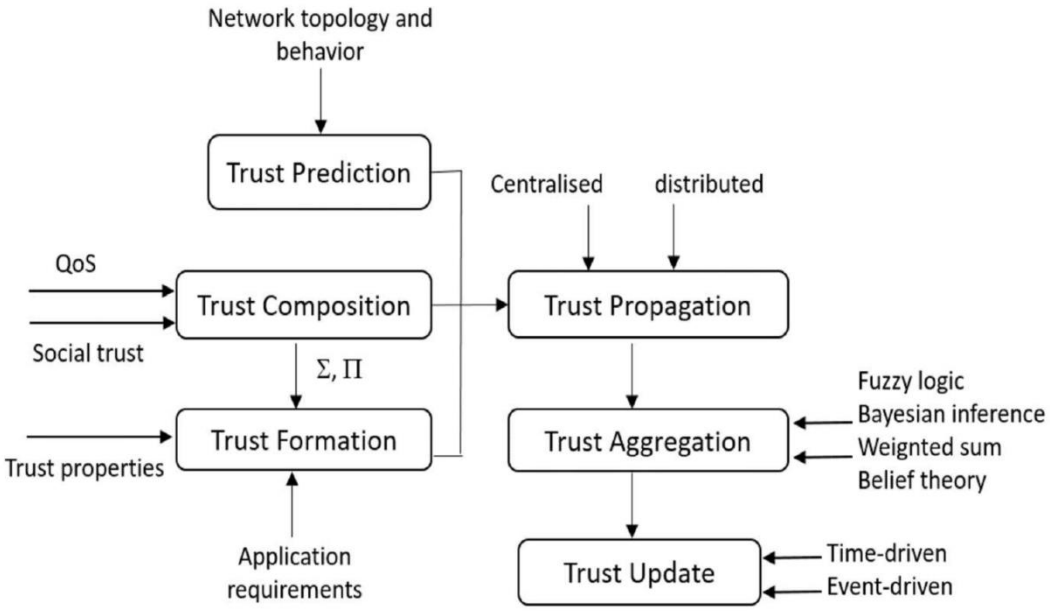

Figure 16: Trust Management Algorithm.

3.4.3 Trust initializing

By balancing these two approaches, we assume that the node's trust value is 0.5, when we let a to be equal to b (since the denominator is zero when $a = b = 0$, we assume a trust value of *0.5* for $a = b = 0$. Obviously, it can be shown from the formula that the trust value is *0.5* when both *a* and *b* are 1, as well as 100. However, there is a clear difference between

the two cases. At the initialization, if the values of *a* and *b* are small, it indicates that there are few interactions, and the obtained trust values are not accurate enough. In contrast, if the values of *a* and *b* are large, the weight of historical trust information will be increased, which will have *a* great impact on the subsequent trust evaluation. The requirement of convergence time for the trust value will increase, it may affect the normal operation of the network. Therefore, the appropriate initial *a* and *b* value should be selected.

3.4.4 Reputation updating

We assume that the node *i* has established some reputation *Rij* about node *j*. Node *i* and node *j* should further interact *(r + s)* times. *r* and *s* represent the number of cooperation and non-cooperation, respectively. Thereby, the current number of interactions is *(a + b + r + s)* times. The latest reputation *Rij* of node *j* is:

$$R_{ij}{}^{new} = Bin(a + b + r + s, a + r)$$

From the above equation, the reputation just updates two parameters:

$$a^{new} = a + r$$

$$b^{new} = b + s$$

3.4.5 Aging

The newly obtained information should be given larger weight. Hence, an aging-weighted parameter is introduced.

$$a^{new} = \left(W_{age} * a\right) + r$$

$$b^{new} = \left(W_{age} * b\right) + s$$

Where, W_{age} represents the aging weight, its range is *(0, 1)*. The aging weight is responsible for ensuring that all nodes are always cooperating together.

3.4.6 Cluster head selection

We use the firefly multi-objective algorithm (MOFA) to choose the cluster head of each cluster, the Cluster leader collects data from other sensor nodes and transmits it to the sink node.

The Firefly algorithm was developed by Yang for continuous optimization, which was later applied to structural optimization and image processing. The Firefly algorithm was based on the blinking patterns and behavior of fireflies. Essentially, The Firefly algorithm uses the following three idealized rules.

- Fireflies are unisex, so a firefly will be attracted to other fireflies, regardless of gender.
- The attractiveness of a firefly is proportional to its brightness and they both decrease with distance. Thus for any two flashing fireflies, the less brighter one will move towards the brighter one. If there is no brighter one than a particular firefly, it will move randomly.
- A firefly's attractiveness is proportional to its brightness and both decrease with distance. So, for two flashing fireflies, the less bright will move to the brighter. If there is none brighter than a particular firefly, it will move randomly.

3.4.7 Indirect information

If *a* node *i* has m neighbor nodes holding trust evaluation of node *j*, the node *i* receives the trust evaluation about the node *j* from these neighbor nodes as indirect information. We denote the indirect observation of neighbor node *x* to the node *j* as $\left(a\middle|j^{x}, b_j^{x}\right)$, and the node *i* holds the reputation of node *j* and another neighbor node k, expressed as $\left(a\middle|j \quad , b_j \right)$ and $\left(a\middle|k \quad , b_k \right)$.

This information is synthesized into a new reputation for node *j*. In the process of synthesizing reputation information of other nodes, in order to defend against the bad mouthing attacks, we cannot completely believe the reputation information transferred by other nodes. Hence, for reputation synthesis, we need to weigh the reputation of other nodes. Therefore, the new reputation $\left(a\middle|j^{new}, b_j^{new}\right)$

$$\begin{cases} a_j^{new} = a_j + \dfrac{a_k}{b_k + a_k} \cdot a_j^k \\ b_j^{new} = b_j + \dfrac{a_k}{b_k + a_k} \cdot b_j^k \end{cases}$$

$$T_{ij} = \frac{a_j^{new}}{a_j^{new} + b_j^{new}} = \frac{a_j \cdot (b_k + a_k) + a_k \cdot a_j^k}{a_j \cdot (b_k + a_k) + b_j \cdot (b_k + a_k) + 2a_k \cdot b_j^k}$$

3.4.8 Indirect information

To defend against the On-Off attack, we define a time interval between the highest trust value $T_h(i)$ and the next highest trust value $T_h(i+1)$ as a detection period $P(i)$. There is the lowest trust value $T_l(i)$ in a detection period, and this moment represents TIM. Secondly, we present a descent time $(t_d(i))$, which is a time interval from $T_h(i)$ to $T_l(i)$, as well as an ascent time $t_a(i)$ from $T(i)$ to $T_h(i+1)$. Finally, we give any trust value $T_d(i, m)$ during a descent time, and any trust value $T_a(i, n)$ during a descent time. If the following relationship is satisfied, the malicious node that launched the On-Off attack can be basically detected.

$$F_D = \begin{cases} 0 & if \ |t_d(i) - t_a(i)| < \delta \\ & and \left(\begin{array}{l} T_d(i,\ m) > \dfrac{T_h(i) - T_l(i)}{t_d(i)} \\ \ and\ T_a(i,\ n) < \dfrac{T_h(i+1) - T_l(i)}{t_a(i)} \end{array} \right) \\ & or \sum_{k=0}^{\min(t_d(i) - t_a(i))} \left(T_a(i,\ TIM + k) - T_d(i,\ TIM - k) \right) < \sigma \\ 1 & otherwise \end{cases}$$

3.5 Conclusion

In this chapter, we have been presenting our work of how ensure the trust management in healthcare domain by calculate the trust using binomial trust methods, so after all those calculations we can detect malignant nodes from honest nodes. The resulting performances will be evaluated by simulation in the next chapter.

Chapter Four

Implementation

4.1 Introduction:

In this field of networking which is a wireless body area network (WBAN), every time A new solution appears and the first thing to do is to go through stages of testing, evaluation and validation before training and work with the solution, at a conceptual level, according to the simulation model in order to save cost and time.

In this chapter we use the omnet++ simulator to evaluate our proposed approach, According to well defined criteria. The obtained results will be analyzed and interpreted.

4.2 OMNET++:

OMNeT++ 6.0 is the result of more than three years of work, and includes many essential new features that we would already have a hard time without. The present changelog summarizes all changes made during the 15+ pre-releases.[33]

We briefly summarize the changes below in each part of OMNeT++ before going into the details. [33]

The most prominent new feature is the new Python-based Analysis Tool in the IDE. The use of Python under the hood allows for arbitrarily complex computations to be performed on the data, visualizing the result in the most appropriate form chosen from a multitude of plot types, and producing publication quality output, all while using an intuitive user interface that makes straightforward tasks easy and convenient. Custom computations and custom plots are also easily accessible. [33]

Figure 17: OMNeT++ logo.

Why OMNeT ++ :

- Modeling of wired and wireless networks.
- Hardware architectures
- Modeling of communications protocol

4.3 Frameworks

4.3.1 INET framework

INET framework is an open-source model library for the *OMNeT++ simulation environment*. It provides protocols, agents and other models for researchers and students working with communication networks. INET is especially useful when designing and validating new protocols, or exploring new or exotic scenarios.

INET contains models for the Internet stack (TCP, UDP, IPv4, IPv6, OSPF, BGP, etc.), wired and wireless link layer protocols (Ethernet, PPP, IEEE 802.11, etc), support for mobility, MANET protocols, DiffServ, MPLS with LDP and RSVP-TE signalling, several application models, and many other protocols and components.

Several other simulation frameworks take INET as a base, and extend it into specific directions, such as vehicular networks, overlay/peer-to-peer networks, or LTE. [33]

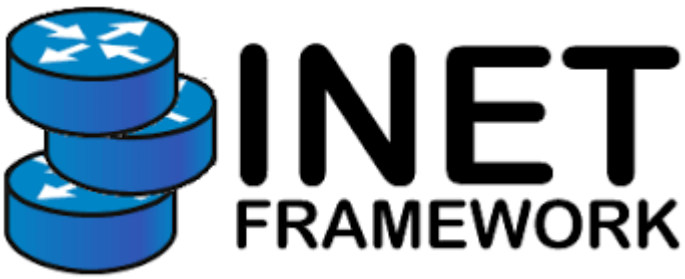

Figure 18 : INET framework.

4.3.2 NETA framework

NETwork Attacks (NETA) is a framework devised to simulate attacks in heterogeneous networks using OMNeT++ and the INET-Framework. *NETA* is aimed to be a useful tool

in the network security field. This tool could make easy to demonstrate the effectiveness of defense security techniques or solutions against network attacks as well as for comparing the capabilities of different defense techniques. [33]

Figure 19 : NETA framework .

4.4 Hardware used

For this simulation we're using a lenovo ideapad laptop with 4gb of ram an *i5;* 8genration process to bellyful our goal from this simulation.

Figure 20 : Lenovo idea pad.

4.5 Use of OMNeT++

To explain the uses of each component of the OMNeT editor we will speak about each one briefly in the sector bellow :

4.5.1 NED editor

The NED language (programmed using NED files with. NED extensions) is used to define the structure of the modules and the topology of the network. At the most basic level, we can roughly divide the contents of the NED file into two fundamental components, namely the module definition part and the network topology definition part. Modules are of two types, simple (active) and compound, which ultimately represent the structure of each node that would be part of the simulation analysis. Simple modules basically express the interface of the module (i.e. gates and parameters). Active modules are programmed in C++, and the hierarchical nesting of simple modules forms a compound module. On the other hand, a group of active modules can be encapsulated to form composite modules where hierarchical levels are not limited Compound modules typically contain definition submodules and an interconnect. The network part describes the topology/layout of any network scenario or the location of certain nodes in a simulation scenario. Other features of the NED file include inheritance (for modules, channels, etc.), metadata ratings, and package information. [34]

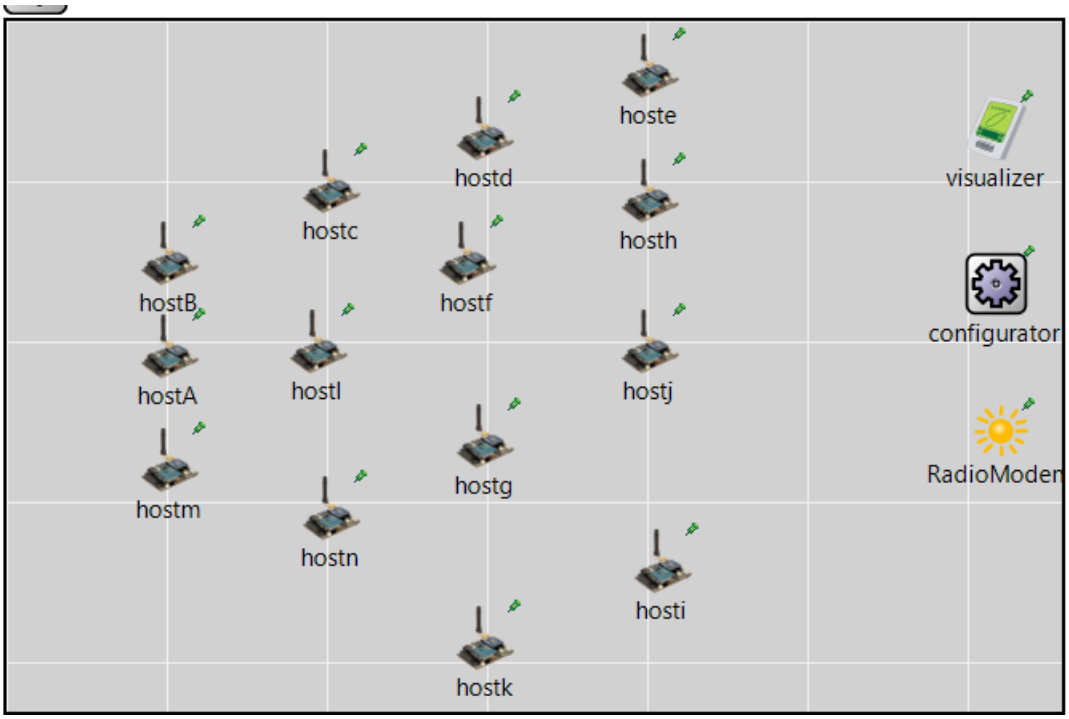

Figure 21 : NED file editor

```
{
    parameters:
        @display("bgb=659.232,431.424;bgg=100,1,grey95");
        @figure[title](type=label; pos=0,-1; anchor=sw; color=darkblue);


        @figure[rcvdPkText](type=indicatorText; pos=380,20; anchor=w; font=,18; textFormat="packets received:
        @statistic[packetReceived](source=hostB.app[0].packetReceived; record=figure(count); targetFigure=rcv

    submodules:
        visualizer: <default(firstAvailableOrEmpty("IntegratedCanvasVisualizer"))> like IIntegratedVisualizer
            @display("p=618,67;i=device/palm2");
        }
        configurator: Ipv4NetworkConfigurator {
            @display("p=618,164");
        }
        hostA: SensorNode {
            @display("p=102,203");
        }
        hostB: SensorNode {
            @display("p=102,145");
        }
        hostc: SensorNode {
            @display("p=203,100");
        }
        hostd: SensorNode {
            @display("p=299,67");
        }
        hoste: SensorNode {
            @display("p=402,28");
```

Figure 22: NED file editor source code.

4.5.2 The INI File Editor:

The INI file editor takes into account all supported configuration options and offers in several forms, organized by themes. Descriptions and default values are displayed in tooltips, which can be persisted for easier reading. The structure of the ini file (sections and their inheritance tree) is also viewed and editable by drag and drop and dialogs. Validation and content support (Ctrl+Space) is also provided if necessary. The editor supports unlimited undo/redo and automatic conversion from INI OMNeT++ 3.x files. [34]

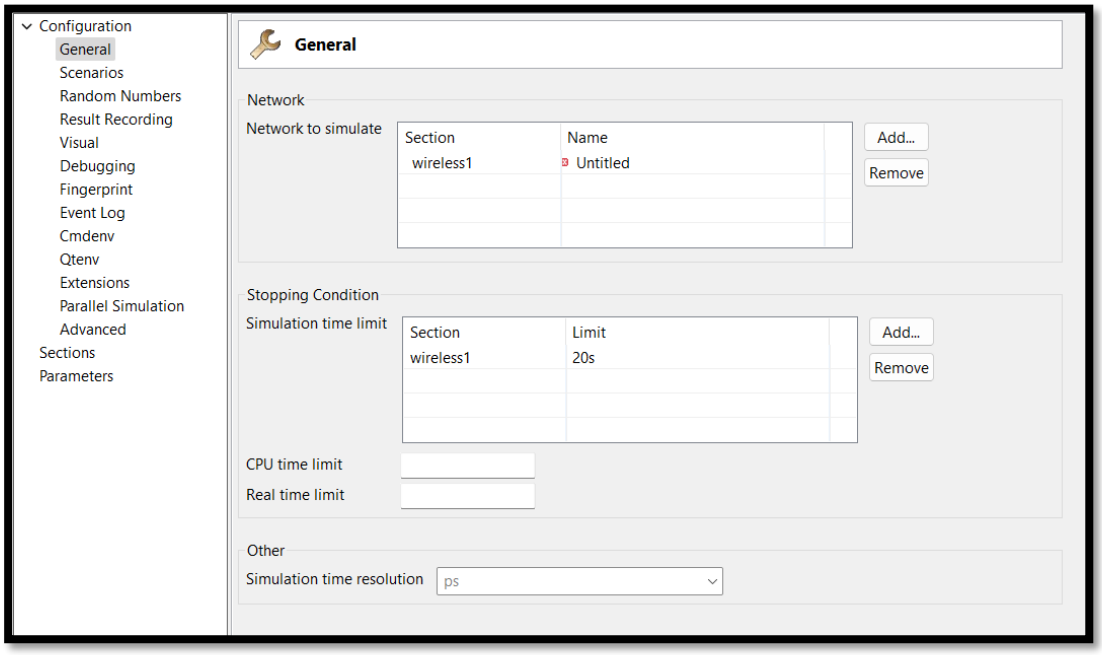

Figure 23: INI file editor .

```
*.hostA.numApps = 1
*.hostA.app[0].typename = "UdpBasicApp"
*.hostA.app[0].destAddresses = "hostB"
*.hostA.app[0].destPort = 5000
*.hostA.app[0].messageLength = 1000B
*.hostA.app[0].sendInterval = exponential(12ms)
*.hostA.app[0].packetName = "UDPData"


*.hostB.numApps = 1
*.hostB.app[0].typename = "UdpBasicApp"
*.hostB.app[0].destAddresses = "hosts"
*.hostB.app[0].destPort = 5000
*.hostB.app[0].messageLength = 1000B
*.hostB.app[0].sendInterval = exponential(12ms)
*.hostB.app[0].packetName = "UDPData"




*.hostB.numApps = 1
*.hostB.app[0].typename = "UdpSink"
*.hostB.app[0].localPort = 5000
*.hostc.numApps = 1
*.hostc.app[0].typename = "UdpSink"
*.hostc.app[0].localPort = 5000
*.hostd.numApps = 1
*.hostd.app[0].typename = "UdpBasicApp"
```

Figure 24 : INI file editor source .

4.6 Implementation steps

We will start the process of our simulation by summarizing it in the following steps:

- Configure the network set the protocols like
- Function which calculates the trust and assign it to each node
- Create Class of honest node behavior and attacker node behavior also the sink node behavior

4.7 Simulation

At this section we will discuss our simulation model, we list the details of the configuration and parameters used for the simulations performed to evaluate the performance of our proposed system.

In Beginning of each transaction for each *node confidence* in the natural force we explain earlier, if trust we computed is the most significant value of the confidence threshold value for the transaction (*0.6*) It means that the node is a trustee and the node communicates with it and adds *0.1* to the trust value of that node, else if the value of the trust we calculated is less than the trust threshold value of the transaction then we add (-*0.1*) to the trust of that node.

Regarding malicious things, we used the type of attack that indicates that the loss is a Data or modification (highly sensitive medical data) as it is provided *negative feedback* on every node involved in the transaction.

The *sink* node is responsible for checking the update of the trust, once the trust is lower Then *0.5*, the sink node detects that this node is an attacker and removes it from the network.

At last of the simulation and when the sink node eliminates all the malicious node from the network. The sink node chooses one of the nodes which has its trust value is 1. That node collects the other sensing information’s and send it to the sink node

As following are the parameters of the simulation:

Settings	value
Sensor nodes	14
malicious nodes	2
Simulation time	NA
Simulation time Variant	0.5
Threshold trust value of every transaction	0.6
Value of trust added or decrease from node in every transaction	0.1

Table 2 : Simulation settings .

4.8 Results

In this section we will present the results of our simulation in 14 nodes and 2 malicious one using 3 clusters as an example.

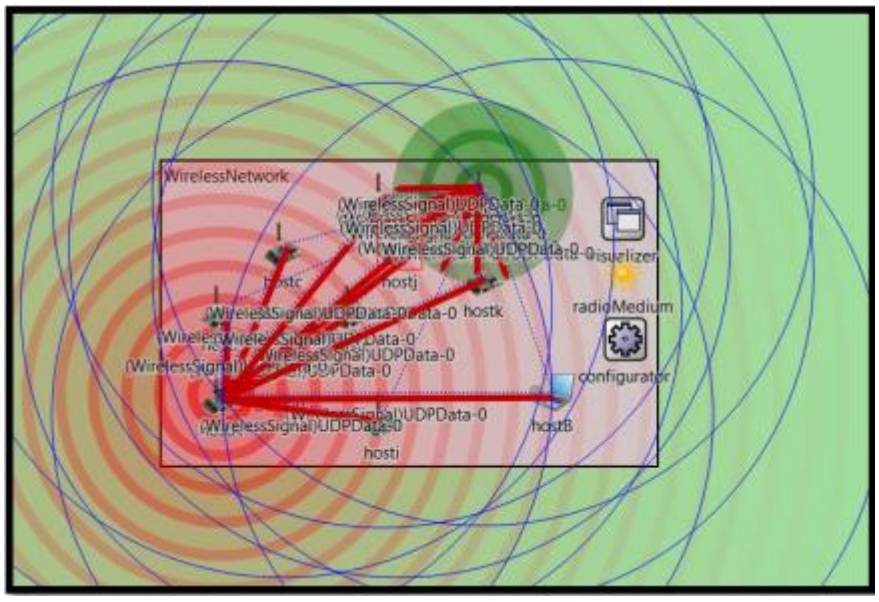

Figure 25 : simulation results.

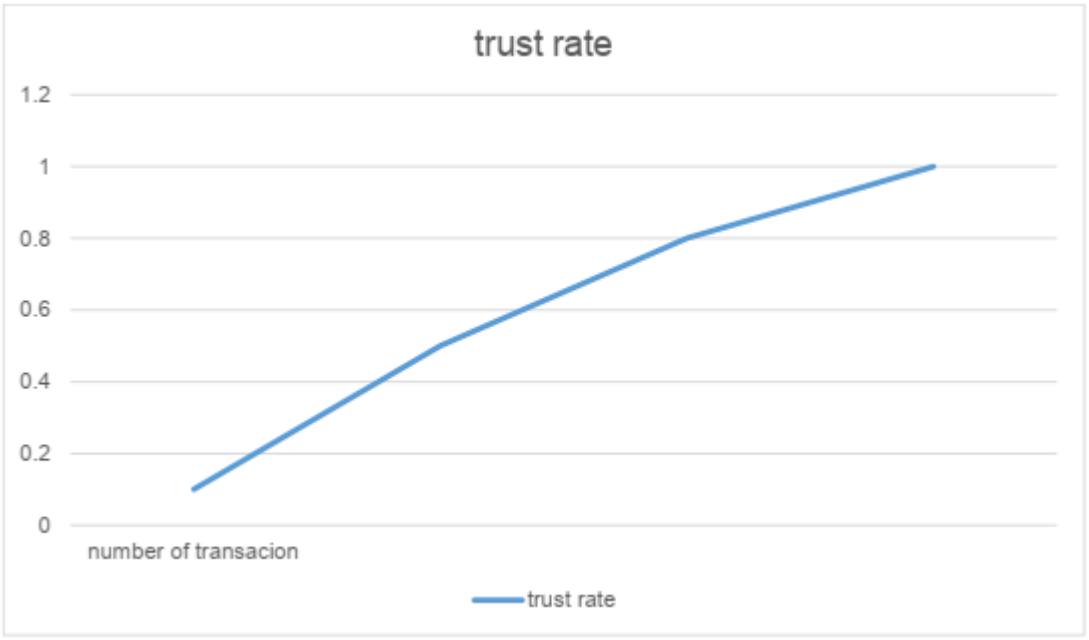

Figure 26 : Trust rate.

The trust is a value that shows to us the number of nodes THAT are trusted in our simulation network and its value is: $trust\ rate = \frac{nbr\ of\ good\ transactions}{all\ the\ transactions}$

In this regard each time we implement our trust method we make the nodes more trusted.

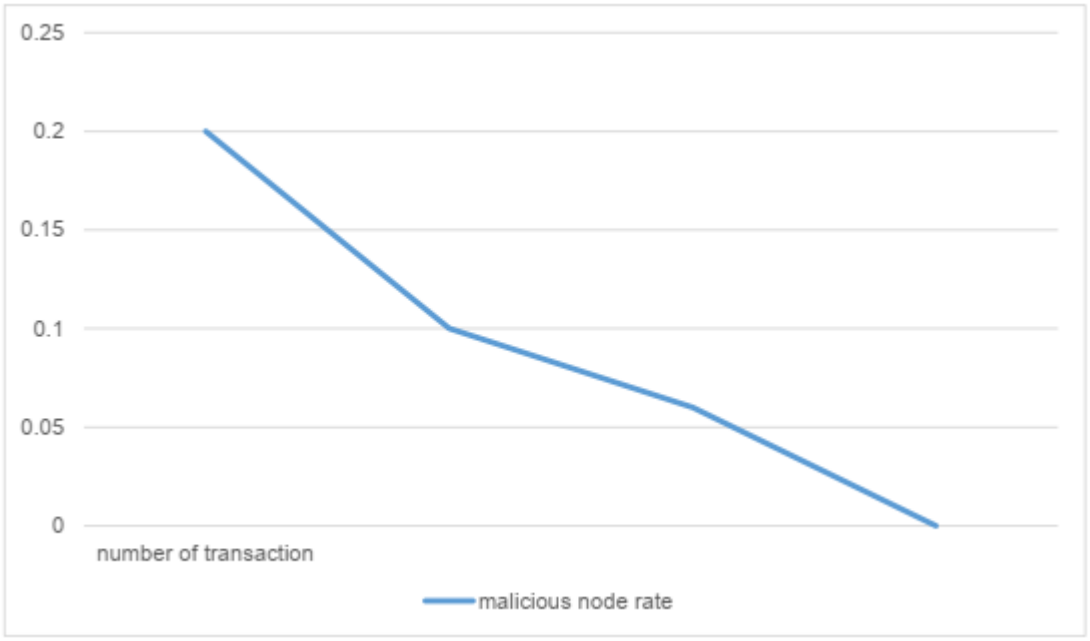

Figure 27 : Malicious node rate.

In this figure we see the rate of the malicious nodes that infected our network and who's note trusted.

For every time we applicate the trust method the number of untrusted nodes will decline and for that more trusted network

4.9 Conclusion

In this chapter, we've seen simulation tools and settings that used for the simulation, so as result of our simulation we found that our proposed trust solution and we've seen that from obtaining results from simulation such as trust rate and malicious node rate. That means we achieved our goal which a trusted network.

General conclusion

In this thesis, we saw what is mobile platforms discussed it architecture and trust in its problem in healthcare domain. To solve this problem, we proposed a new trust solution-based binominal distributed systems, we kept the main thing in this solution is the negotiation methodology and we made our research to reduce the number of malicious nodes. And that operation has been done instead of calculating the trust of each message and make a lot of calculation to the sink just to maximize network lifetime.

The trust management come a fourth to detect faulty nodes and malicious nodes in the wireless sensor network, this one is helping to solve the problem of security threats, more generally the trust management came to promote the security of networks especially sensitive networks like WSN and the mobile platform through maintaining a good level of trust in the network communication and relationships between nodes. For that in our work we based on the calculation of distributed binominal trust system between each of the nodes and getting the history of each trust node also we care for the trust and indirect trust to propose a method which can detect number of attackers in wireless sensor network like a bad mouth attack and simple attack.

In this work we use three factors, and there are other works use one or two factors, so because the wireless sensor network is very sensitive we hope in the future to use more than three factors.

Bibliography

[1] Stephen J. Bigelow, "What is MPaaS? Mobile Platform as a Service Definition," *SearchMobileComputing*.https://www.techtarget.com/searchmobilecomputing/definition/mobile-platform-as-a-service-MPaaS (accessed Jun. 09, 2022).

[2] S. K. Sivakumar and S. Srivastava, "Introduction to Mobile Architecture," 2017, Course or Learning Material, Indira Gandhi National Open University (IGNOU); Accessed: Jun. 09, 2022. [Online]. Available: http://oasis.col.org/handle/11599/2834

[3] C. Silva Villafuerte, R. M. Toasa G, J. Guevara Gordillo, H. Martinez, and J. Vargas, "Mobile Application to Encourage Local Tourism with Context-Aware Computing," 2018, pp. 796–803. doi: 10.1007/978-3-319-73450-7_75.

[4] "Top trends in the field of Mobile App Development," *WebClues Infotech*, Jun. 20, 2017. https://www.webcluesinfotech.com/top-trends-field-mobile-app-development/ (accessed Jun. 10, 2022).

[5] K. M. Khan and Q. Malluhi, "Establishing Trust in Cloud Computing," *IT Prof.*, vol. 12, no. 5, pp. 20–27, Sep. 2010, doi: 10.1109/MITP.2010.128.

[6] A. Nagarajan and V. Varadharajan, "Dynamic trust enhanced security model for trusted platform based services," *Future Gener. Comp Syst*, vol. 27, pp. 564–573, May 2011, doi: 10.1016/j.future.2010.10.008.

[7] E. D. Canedo, R. de Sousa Junior, R. Carvalho, and R. Albuquerque, "Trust Measurements Yeld Distributed Decision Support in Cloud Computing," *Int. J. Cyber-Secur. Digit. Forensics IJCSDF*, vol. 1, p. 140, Jan. 2012.

[8] B. K. Thomas Beth, Malte Borcherding, "Valuation of Trust in Open Networks," *Third Eur. Symp. Res. Comput. Secur. ESORICS 94*, vol. 3, no. 2, pp. 3–18, 1994.

[9] Julia Kagan "What Is a Trust?," *Investopedia*. https://www.investopedia.com/terms/t/trust.asp (accessed Jun. 10, 2022).

[10] "Creative Commons — Attribution-NonCommercial-NoDerivs 3.0 Unported — CC BY-NC-ND 3.0." https://creativecommons.org/licenses/by-nc-nd/3.0/ (accessed Jun. 10, 2022).

[11] J.-H. Cho, K. Chan, and S. Adali, “A Survey on Trust Modeling,” *ACM Comput. Surv.*, vol. 48, pp. 1–40, Oct. 2015, doi: 10.1145/2815595.

[12] “Defining Basic Health Care | American Medical Association.” https://www.ama-assn.org/delivering-care/ethics/defining-basic-health-care (accessed Jun. 10, 2022).

[13] Fred N. Pelzman, MD “Opinion | A Solution for Healthcare, and Everything Else?,” Dec. 27, 2021. https://www.medpagetoday.com/opinion/patientcenteredmedicalhome/96382 (accessed Jun. 10, 2022).

[14] V. R. S. Dhulipala and K. Narasimman, “Trust management technique in wireless sensor networks: challenges and issues for reliable communication: a review,” *CSI Trans. ICT*, vol. 5, Apr. 2017, doi: 10.1007/s40012-017-0169-5.

[15] A. Pirzada and C. Mcdonald, “Establishing Trust In Pure Ad-hoc Networks,” *Proc. 27th Australas. Conf. Comput. Sci. - Vol. 26 Darlinghurst Aust. Aust.*, Feb. 2004.

[16] D. H. Mcknight and N. L. Chervany, “The Meanings of Trust,” 1996.

[17] S. Ba and P. Pavlou, “Evidence OF the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior,” *MIS Q.*, vol. 26, pp. 243–268, Sep. 2002, doi: 10.2307/4132332.

[18] P. Zhang and A. Vasilakos, “A Survey on Trust Management for Internet of Things,” *J. Netw. Comput. Appl.*, vol. 42, Jun. 2014, doi: 10.1016/j.jnca.2014.01.014.

[19] “International Journal of Trust Management in Computing and Communications (IJTMCC) " Editor-in-Chief: Dr. Dorgham. ISSN print 2048-8378. Publishers - linking academia, business and industry through research.” https://www.inderscience.com/jhome.php?jcode=ijtmcc (accessed Jun. 10, 2022).

[20] Alghofaili Y, Rassam MA. A Trust Management Model for IoT Devices and Services Based on the Multi-Criteria Decision-Making Approach and Deep Long Short-Term Memory Technique. S*ensors (Basel).* 2022 Jan 14;22(2):634. doi: 10.3390/s22020634. PMID: 35062594; PMCID: PMC8777818.

[21] Warsun Najib, Selo Sulistyo, Widyawan, “Survey on Trust Calculation Methods in Internet of Things". Procedia Computer Science,Volume 161,2019,Pages 1300-1307,ISSN 1877-0509, https://doi.org/10.1016/j.procs.2019.11.245.

[22] Arbia Riahi Sfar, Enrico Natalizio, Yacine Challal, Zied Chtourou, "A roadmap for security challenges in the Internet of Things - ScienceDirect." Digital Communications and Networks, Volume 4, Issue 2,2018,Pages 118-137,ISSN 2352-8648,https://doi.org/10.1016/j.dcan.2017.04.003.

[23] A. I. A. Ahmed, S. H. Ab Hamid, A. Gani, S. khan, and M. K. Khan, "Trust and reputation for Internet of Things: Fundamentals, taxonomy, and open research challenges," *J. Netw. Comput. Appl.*, vol. 145, p. 102409, Nov. 2019, doi: 10.1016/j.jnca.2019.102409.

[24] J. P. Harrison and A. Lee, "The role of e-Health in the changng health care environment," *Nurs. Econ.*, vol. 24, no. 6, pp. 283–288, 279; quiz 289, Dec. 2006.

[25] Bandar Alhaqbani, Audun Josang, and Colin Fidge "A Medical Data Reliability Assessment Model." Journal of Theoretical and Applied Electronic Commerce Research, Volume 4, Issue 2, August 2009,Pages 64-78,ISSN 0718-1876, http://dx.doi.org/10.4067/S0718-18762009000200006

[26] J. L. Fernández-Alemán, I. C. Señor, P. Á. O. Lozoya, and A. Toval, "Security and privacy in electronic health records: a systematic literature review," *J. Biomed. Inform.*, vol. 46, no. 3, pp. 541–562, Jun. 2013, doi: 10.1016/j.jbi.2012.12.003.

[27] I. Brown and A. Adams, "The ethical challenges of ubiquitous healthcare," *Int. Rev. Inf. Ethics*, vol. 8, pp. 53–60, Jan. 2008, doi: 10.29173/irie98.

[28] HoffmanKevin, ZageDavid, and Nita-RotaruCristina, "A survey of attack and defense techniques for reputation systems," *ACM Comput. Surv. CSUR*, Dec. 2009, doi: 10.1145/1592451.1592452.

[29] C. M. Burkle and M. T. Keegan, "Popularity of internet physician rating sites and their apparent influence on patients' choices of physicians," *BMC Health Serv. Res.*, vol. 15, p. 416, Sep. 2015, doi: 10.1186/s12913-015-1099-2.

[30] Félix Gómez Mármol and Gregorio Martínez Pérez. *"Security threats scenarios in trust and reputation models for distributed systems." Computers & Security, Volume 28, Issue 7, 2009, Pages 545-556, ISSN 0167-4048,* https://doi.org/10.1016/j.cose.2009.05.005.

[31] LAANANI IBTISSAM, "Trust management in wireless body area network," Master RTIC, Mohamed Khider University – BISKRA, BISKRA, 2021.

[32] A. Ali and F. A. Khan, “Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications,” *EURASIP J. Wirel. Commun. Netw.*, vol. 2013, no. 1, p. 216, Aug. 2013, doi: 10.1186/1687-1499-2013-216.

[33] omnet++ team, What is OMNeT++?, https://omnetpp.org/intro/, access at 18/06/2022

[34] Jeanne Kelly, A Guide to NED: A New On-Line Computer Editor, ARPA ORDER NO.: 189-1 7Pl 0 Information Processing Techniques