I.J. Wireless and Microwave Technologies, **2022, 5, 21-35**
Published Online on October 8, 2022 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2022.05.03

Trust Modelling and Management for IoT Healthcare

Abdul Rauf
Kulliyyah of ICT, International Islamic University, Kuala Lumpur, Malaysia
E-mail: abdul.rauf@live.iium.edu.my

Riaz Ahmed Shaikh
Computer Science Department, King Abdulaziz University, Jeddah, Saudi Arabia
E-mail: rashaikh@kau.edu.sa

Asadullah Shah
Kulliyyah of ICT, International Islamic University, Kuala Lumpur, Malaysia
E-mail: asadullah@iium.edu.my

Received: 15 April 2022; Revised: 04 May 2022; Accepted: 25 May 2022; Published: 08 October 2022

Abstract: The IoT wave is on rise and it is considered as the biggest world changing computing ecosystem after the invention of Internet where the meaning of lifestyle is expected to be changed. IoT is now diffusing pervasively in most areas of life like smart home, smart cities, smart irrigation, smart healthcare etc. The concerned industry is trying to reap maximum benefits from this regime without putting extra efforts or investing much to make the related infrastructure secure and trustworthy. IoT end device, a.k.a smart object, is one component of this ecosystem, responsible to interact with the physical environment and gather the data, along with communication technologies, processing capabilities like fog or cloud computing and applications to interact with the device (s). It is possibility that such devices can be faulty, compromised or misbehaving because of internal or external factors like hardware malfunctioning or cyber-attacks. In this situation the data gathered and transferred by such devices can be disaster and challenging in decision making specifically in an area where the human life is involved like IoT healthcare. We have proposed a mathematical model to estimate the trust of such devices. Trust on IoT devices and gathered data from such trusted devices will boost the confidence of end users on this new computing regime; especially in healthcare environment. The estimated trust status (trusted, uncertain, and untrustworthy) will be saved in a database or CSV file with a timestamp to be used as reputation by healthcare applications. Patients are assigned their SOI based on their specific diagnoses and procedures performed during their medical encounter. Similarly, for a patient with heart diseases or having hypertension can be considered in extreme category with a value of $\gamma = 1$ if there is some deviation of readings.

Index Terms: IoT healthcare, Trust management, Smart healthcare.

1. Introduction

The Internet of Things (IoT) is basically an idea which conceives a connected set of anyone, anything, anytime, anyplace, any service, and any network. “The basic idea is that IoT will connect objects around us (electronic, electrical, non-electrical) to provide seamless communication and contextual services provided by them. Development of RFID tags, sensors, actuators, mobile phones make it possible to materialize IoT which interact and co-operate each other to make the service better and accessible anytime, from anywhere.” [1] Everyday objects include not only the electronic devices we encounter or the products of higher technological development such as vehicles and equipment but things that we do not ordinarily think of as electronic at all - such as food and clothing. These devices collect the data from their environment, communicate with each other or transfer it to the clouds for analytics, making decisions and taking actions.

The connectivity among things or smart objects is mostly achieved through different wireless communication technologies (WiFi, 3G, 4G, 802.15.x) and supporting protocols which are employed pervasively for smart monitoring and control applications [2]. This arrangement opens a new era of intelligent applications and huge number of smart services that can bring substantial impact on human lives and boost economic growth [3]. Assisted healthcare, smart homes, smart cities, smart transportation, smart grids, smart irrigation, security and surveillance are a few known examples to name.

Assisted Healthcare or simply IoT Healthcare is one of the attractive application areas for the IoT [4]. The IoT healthcare has the potential to be applied in different scenarios like remote health monitoring, fitness programs, curing chronic diseases, and elderly care. Hence, different types of medical equipment, embedded with sensors and communication capabilities can be viewed as smart devices or objects which constitute a core part of the IoT Healthcare. The medical services based on IoT healthcare are expected to provide high quality services at reduced cost. Such services with use of artificial intelligence and knowledge base will increase the quality of life and improve the users' experience [5].

However, IoT is also facing the challenges of security and privacy [6]. These security issues become even worst and challenging in case of IoT healthcare. J. Radcliffe, during Black Hat event in 2011, demonstrated a shockingly feasible scenario that how he was able to remotely controls the insulin management digital unit which was being used for his diabetes treatment [7]. With this evidence, Radcliffe assumes many serious threats, including the ability of the adversary to change the amount of insulin delivered by the pump to the patient. Although this would require proximity to the device (100 to 200 feet for the wireless transceiver used on this insulin pump), it would only take seconds to reprogram its functionality, which could potentially result in patient hospitalization or even casualty. Similarly, a compromised smart pacemaker can put the patient into misfortune. Incorrect data transfer from an IoT device can be misleading for health practitioner.

In this paper, we continue our research work, proposed in [8] where we identified trust parameters and suggested a conceptual model for trust evaluation of IoT devices. This paper further elaborates the trust parameters and related mathematical equations. Also, explain, the final trust estimation of an IoT device. This trust estimation will help to trust the data before making a critical decision. The exiting methodologies met several shortcomings in terms of reliability, less trust level, security and computational complexities. To tackle these issues, we proposed a novel trust modeling and management for IoT healthcare. The major research objectives are summarized as follows:

- Initially, we identify four parameters reliability, availability, response time and identity from existing literature to be used for direct trust estimation.
- The estimated trust status (trusted, uncertain, and untrusted) will be stored in a database or CSV file with timestamp to be used as reputation by the healthcare applications.
- The Severity of illness (SOI) is defined as the extent of organ system derangement or physiologic decompensation for a patient.

The remaining paper is organized as follows. Section two explains trust and trust management. Section three highlights the related work from literature. Section four reveals proposed mathematical model and section five gives theoretical analysis and evaluation of the model using different scenarios in IoT healthcare. Section six, ends the paper with concluding remarks and future research work.

2. Trust and Trust Management

Trust management has a vital role in IoT for reliable data analysis based on which several services can be offered with more confidence and helps to acquire end user's trust. It provides a level of satisfaction to tackle the perceptions of doubt and risk in user acceptance and consumption of IoT services and applications. However, trust is not a simple concept when we deal with reliability, integrity, security, privacy and other similar characteristics of data, devices or networks. In order to get the better insight of Trust, we review some definitions in existing literature.

2.1 Defining Trust

An earlier definition of trust was proposed by D. Gambetta, focuses on reliability trust [9]. The author states that "Trust is the subjective probability by which an individual, A, expects that another individual, B, performs a given action on which its welfare depends". The definition is based on two factors, the dependency of one party on the other while the act of the other party is some sort of fuzzy until and unless the action is completed. This definition does not talk about the alternative to party, B, if there are some good evidences to trust on another entity which can perform the same desired action.

Another definition was presented by McKnight, D. H. in [10]. According to him trust is the level to which one party is ready to depend on something or somebody in a given circumstances with a feeling of relative security, even though negative consequences are possible. Here the dependency is coming up with feeling of security but fair of risk is still there. Mayer, R. C [11] describes trust in a more rich way, he expresses it as the readiness of a party to be exposed to the action of another party based on the belief that the other will accomplish a specific action significant to the first party, even though the first party may not have ability to monitor or control the other party.

2.2 Defining Trust Management

Trust Management is an approach to utilize certain set of practical procedures, tools, and rules to highlight the role of trust in decision mechanisms. Etalle et al. [12] defines this concept as "Trust Management is an approach to making decisions about interacting with something or someone we do not completely know, establishing whether we should

proceed with the interaction or not". It focuses on trust establishing, updating, and revoking through the study of security policies, credentials, and trust relationships.

The concept of trust is influenced by many parameters. It is highly associated with security since ensuring security and privacy of system as well as of user is required to gain trust of consumers. Trust, somehow, has bigger scope than security as it is not only based on security, but also affected by many other factors (e.g. reputation, performance, reliability, availability, ability etc.). Thus, trust is more complicated and challenging to establish, ensure and maintain than security [11].

In smart environments, IoT devices may take numerous readings like temperature, humidity, fire, pressure measurements, heart-beat readings, Oxygen breathing measurements etc. to help decision making and immediate reaction. This ascertains the importance of trust worthiness of the involved device(s) to make the right assessment and highlights the interaction between entities by trusting what they report and acting accordingly. Then, establishing and managing trust in a huge number of objects in heterogeneous and large-scaled environments is a considerable challenge for researchers and manufacturers.

3. Related Work

Gligor and Wing [14] proposed a trust model based on computational trust and behavioral trust in computer networks and humans' social networks respectively. They suggested a modest communication model of entities and channels. In this model the entities can be network hosts, network applications or humans. For human users, behavioral trust uses a game-theoretical approach. The reliability of the received information is evaluated based on peer reviews or reputation of the sender entity. Trust can be achieved by verifying whether the sender can be trusted, e.g., by second opinions. In some situations, the second opinion might never arrive, and receiver might have to use the received information without validating it which may cause risks during decision making phase.

Dong Chen et al. [15] suggest and validate a trust and reputation model based on fuzzy theory for IoT or Cyber Physical Systems (CPS). The trust is established using direct observations and indirect reputations values. The direct observations are made using different network efficiency parameters like End-to-end packet forwarding ratio (EPFR), energy consumption (AEC), and packet delivery ratio (PDR). The model does not consider the social relationships of the service requestors in SOA.

Gu et al. [12] describe trust management control based on architectural modeling of IoT by using fuzzy set theory. They decomposed the IoT architecture in three main layers (sensor, core and application layers) and argued that the trust must be evaluated at each layer for specific reasons and must share this trust among each layer for more trustworthy environment. In this model the final authority to react against collected information is performed by service requester based on cumulative trust and requester's policy. The paper does not provide comparison with other proposed models.

A conceptual model [13] is proposed by A. Arabsorkhi et al. based on human's way of trusting other humans in everyday social life. In this model the trust is evaluated based on stored experience and a threshold value of predefined trust. The model was not verified by using some simulation tool or taking example of some application scenario.

Atzori et al. [14] introduced a new concept of trust for IoT based on social relationships, called Social IoT (SIoT). It describes the social relationships among IoT objects like human beings have their social and community networks. The idea was carried forward to develop a subjective model for trust management in SIoT [15]. The model works on direct experience and indirect observation (e.g. reputation: recommendation by common friends). Bao and Chen [16] [17] worked on similar idea of trust in SIoT. They proposed a trust management protocol for highly dynamic IoT environment considering both social trust and QoS trust metrics. They used multiple trust properties like honesty, cooperativeness, community-interest and recommendation for each participating node. Both direct observations and indirect recommendations are considered while updating the trust values.

Leister and Schulz [22] proposed a trust model that considers all the main entities of an IoT ecosystem e.g. humans, devices and communication technologies. They described trust in a different way and defined policies which can be used to determine if something is trustworthy or not. The model calculates the trust values before and after interaction with another entity and use these values to judge that how much the other party is trustworthy.

Køien, G. M. [18] analyzed and identified different characteristics of trust in software, hardware, devices and services in IoT environment. He tried to give reasons for the acceptance of IoT devices and smart objects based on humans' conduct of trust. The author studied the trust in IoT environment very deeply and concluded that it may not be possible to attain 100% trust in this ecosystem because of the involvement of multiple components and entities. Even then, humans may not be able to evade using IoT devices in future.

Xu et al. [19] have proposed an autonomic agent trust model to ensure the reliability and credibility of IoT environment. This model helps to reduce the security related concerns in this highly dynamic environment. However, to build the credibility protection model for IoT systems, agents and agent platforms must be implemented on all nodes which may raise issues related to scalability and heterogeneity of this system.

The mechanism for trust establishment and management can also be vulnerable like other security practices. Sun et al. [25] examined the vulnerabilities in trust establishment methods and proposed defense techniques against attacks in

these networks. However, their focus was mainly wireless ad-hoc and sensor networks. Table 1. Displays a summary of above related work.

Table 1. Comparison of literature analysis

Research	Computational Approach	Cooperative / Behavioral approach	Fuzzy Set Theory	Social Networking	Direct Observation	Reputation /Peer Reviews
[20]	✓	✓		✓		✓
[21]	✓		✓		✓	✓
[12]			✓		✓	✓
[13]		✓		✓		✓
[14]		✓		✓	✓	
[15]		✓		✓	✓	✓
[16][17]		✓		✓	✓	✓
[22]	✓	✓			✓	✓
[18]		✓				

4. Proposed Model

Figure 1 explains the proposed trust management model. In our proposed model, we firstly identified four parameters reliability, availability, response time and identity from existing literature to be used for direct trust estimation (Table 2, provides a comparison of different management schemes used and related trust parameters). These parameters are defined and represented mathematically in the following section and finally will be used to estimate the overall trust of the concerned device. The estimated trust status (trusted, uncertain, and untrusted) will be stored in a database or CSV file with timestamp to be used as reputation by the healthcare applications.

Table 2. Comparison of Trust Schemes with parameters

Research	Adopted trust approach	Trust Parameters
[23]	Community of Interest IoT	Reliability, reputation
[13]	Social IoT (SIoT)	Trust threshold
[17]	SIoT, QoS	honesty, cooperativeness, and community interest
[21]	QoS	Identity, End-to-end packet forwarding ratio (EPFR), Energy Consumption and packet delivery ratio (PDR)
[15]	SIoT	Own experience, peer recommendations
[16]	Community of Interest IoT, SIoT	honesty, cooperativeness, and community-interest, peer recommendation
[12]	Architecture modeling of loT, QoS	Sensor layer: energy consumption, efficiency of perception Core/Network Layer: bandwidth, service price, routing efficiency Application layer: processing data, storage, and human-computer interface

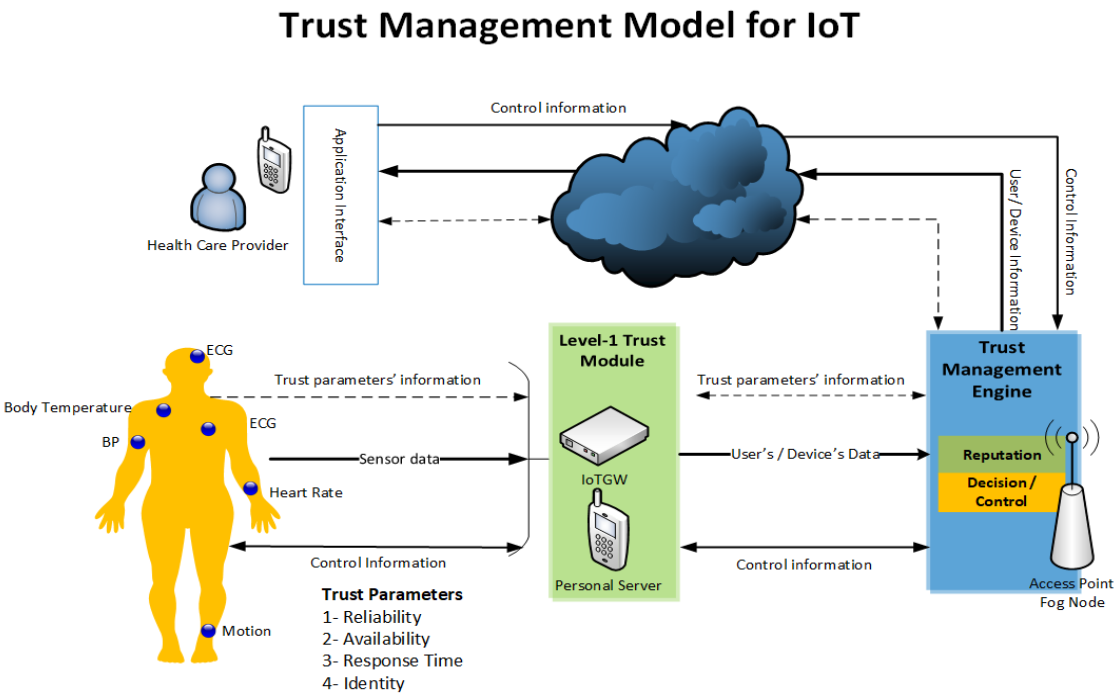

Fig. 1. Proposed Trust Management Model

4.1 Trust Parameters' Definition & Estimation

In this section, we are discussing the trust parameters such as reliability, Availability, Identity, Response time and Trust estimation.

(i) Reliability:

In assisted health care environment, IoT device is considered reliable if it is disseminating the data at configured frequency and within given standard reading range. The reliability (Re) of a device (d) at time (t) is calculated in the following manner.

$$\mathrm{Re}_{d,t} = \frac{F_v + R_v}{2} \tag{1}$$

F_v represents the tolerance level of deviation against configured frequency based on the nature of application. If the frequency is as per configuration, then F_v = 1. For any increase or decrease of frequency, F_v will be decreased by β as shown in Equation below.

$$F_v = \begin{cases} 1 & if \quad frequency\ is\ as\ per\ configuration \\ 1-\beta & Otherwise \end{cases} \tag{2}$$

Where, β is a tuning factor and its value depends upon the severity level of application. There are three types of network applications (James D. McCabe) and we can set this β accordingly.

Table 3. Values for β tuning factor

Type of Application	β value
Mission-critical	1.0
Real-Time	0.75
Rate-Critical	0.50
Others	0.25

For mission-critical applications like healthcare, its value can be set to 1. For example, if a healthcare IoT device is set to disseminate reading ten times per minute and due to some malfunctioning or attack, it is producing reading five times or 15 times. We may apply β as one which results in F_v = 0. Otherwise, if the reading is as per configuration, β will be 0 and F_v = 1

R_v Characterizes the tolerance level of deviation against configured reading based on severity of illness (SOI). If the reading is in the pre-defined normal range as per medical science or a range to show disease, then R_v = 1. Beyond the range, its value decreases by γ (γ is a tuning factor) as shown in Equation below.

$$R_v = \begin{cases} 1 & if \quad reading\ is\ as\ per\ configuration \\ 1-\gamma & Otherwise \end{cases} \tag{3}$$

The value of γ can be set between zero and one depending on the severity of illness (SOI). The Severity of illness (SOI) is defined as the extent of organ system derangement or physiologic decompensation for a patient. It gives a medical classification into minor, moderate, major, and extreme [24]. Patients are assigned their SOI based on their specific diagnoses and procedures performed during their medical encounter.

Table 4. Values for γ tuning factor

Severity of illness (SOI)	γ value
Extreme	1.0
Major	0.75
Moderate	0.50
Minor	0.25

For example, normal human body temperature is the typical temperature range found in humans. The normal human body temperature range is typically stated as 36.5–**37.5** ℃ (97.7–**99.5** ℉). Any increase in temperature because of fever, it may go to around 105/106 ℉ but beyond this value, it shows that there is something wrong with the measuring device**.** Similarly, any reading below 80 ℉ will also indicate some issue. Such kind of case can be considered under the moderate category of SOI and value of **γ** can be set to 0.50. Similarly, for a patient with heart diseases or having hypertension can be considered in extreme category with a value of **γ** = 1 if there is some deviation of readings.

(ii) Availability:

The device will be considered fully available if the number of received TCP keep-alive (in case of HTTP) or DTLS heartbeat extension packets (in case of CoAP) are same as sent. Here it is assumed that there is no network congestion and network resources in terms of bandwidth are available. The availability (Av) of a device (d) at time (t) is calculated in the following manner.

$$Av_{d,t} = \begin{cases} 1 & P_{rev} == P_{tran} \\ \dfrac{P_{rev}}{P_{tran} + \left(P_{tran} - P_{rev}\right)} & P_{rev} < P_{tran} \\ 0 & Else \end{cases} \tag{4}$$

$$Av_{d,t} = \begin{cases} Available & Av_{d,t} == 1 \\ Partially\ \ available & 0 < Av_{d,t} < 0 \\ Not\ available & Av_{d,t} = 0 \end{cases} \tag{5}$$

Where, P_{rev} represents the total number of received packets, P_{tran} represents the total number of transmitted packets. Set the value of $Av_{d,t} = 1$ for available, 0.5 for partially available and zero for unavailable device in final trust estimation.

Fig. 2 shows the behavior of a device against availability parameter. When we do not get any response from device under consideration, it is declared as unavailable. In case response to some of the sent packets is received, the device is considered as partially available. However, if we get the same number of packets as sent the device is declared as available and can be trusted in terms of availability

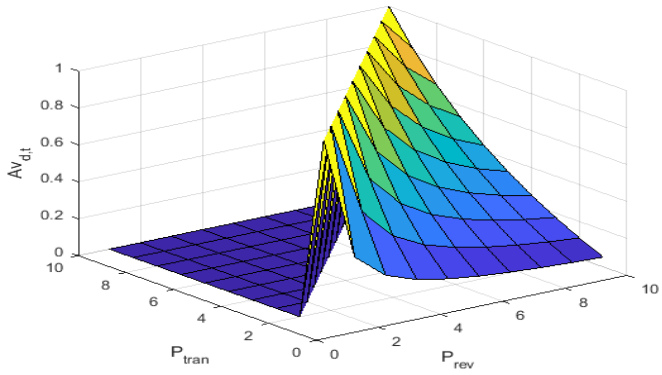

Fig. 2. Availability of a device

(iii) Response Time:

We define response time as the time elapsed during the client requests using an application layer protocol HTTP/HTTPS/CoAP to receive or send some information and the client receives the server's reply / acknowledgement against this request

$$Rt_{d,t} = \begin{cases} 0 & if \quad \dfrac{RT}{RT_{\max}} > 1 \\ 1 & Otherwise \end{cases} \tag{6}$$

RT is the response time and RT_{max} is the maximum acceptable response time which can be defined based on application type and it will describe the tolerance level in terms of time that the application can accept against any request. If the value of $\boldsymbol{Rt_{d,t}}$ is greater than one, it is considered as un-responsive and is assigned with a value zero. Otherwise, assigned with a value of one to be used in final trust calculation.

(iv) Identity:

Identity proves that the device is genuine and legitimate. It is assumed that an identity management system and authentication mechanism is already in place for an IoT device. The identity (Id) of a device (d) at time (t) is validated by implemented authentication mechanism and can have value zero or one.

$$Id_{d,t} = [0,1] \tag{7}$$

If the identity of the device is proved based on the implemented authentication mechanism, then the value of this parameter will be set to one otherwise zero

(v) Estimating the Trust:

We have derived the following mathematical equation to estimate the Trust of a device (d) at any given time (t).

$$T_{d,t} = Id_{d,t} \times \left[\frac{\boldsymbol{Re_{d,t}} + \boldsymbol{Av_{d,t}} + \boldsymbol{Rt_{d,t}}}{3}\right] \tag{8}$$

The equation depicts that the device identity is of prime importance and must be proved. After calculating the trust value of device (d) at time t ($T_{d,t}$), the model will quantize the trust value into three states as follows.

$$Mp(T_{d,t}) = \begin{cases} Trusted & 0.85 \le T_{d,t} \le 1 \\ Uncertain & 0.5 \le T_{d,t} < 0.85 \\ Untrusted & 0 \le T_{d,t} < 0.5 \end{cases} \tag{9}$$

By using the values from equations one to six. The final trust of the device is computed using equation (7). The device is assigned with one of the trust values based on above results as to be stored in reputation file or database table

$$\begin{aligned} Trusted &= 1 \\ Uncertain &= 0.5 \\ Untrusted &= 0 \end{aligned} \tag{10}$$

4.2 Reputation Calculation

Trust value related to a device **d** at any time **t** is stored in a database table or a CSV file along with timestamps. Whenever, application receives data from device "**d"**, before processing the data and taking decision based on this data, it first calls "Trust Management Engine" to know the reputation of the device and hence the received data. Trust engine works as:

1. Fetch the latest n trust readings (where trusted=1, uncertain = 0.5 and untrusted = 0) based on timestamp associated with the device d
2. Use the following equation (8) to calculate the reputation
3.

$$\text{Re}\, p_{d,t} = \alpha\left(Trust\ Value_{latest}\right) + \left(1-\alpha\right) \left(\sum_{i=1}^{n-1} \frac{Trust\ values_{except latest}}{m-1}\right) \tag{11}$$

$$\begin{aligned} &0.85 \le \text{Re}\, p_{d,t} \le 1 \Rightarrow Trusted \\ &0.5 \le \text{Re}\, p_{d,t} < 0.85 \Rightarrow Uncertain \\ &0 \le \text{Re}\, p_{d,t} < 0.5 \Rightarrow Untrusted \end{aligned} \tag{12}$$

The above equation represents an Exponential Moving Average (EMA) which is a type of moving average (MA) that places a greater weight and significance on the most recent data points. The exponential moving average is also referred to as the exponentially weighted moving average. An exponentially weighted moving average reacts more significantly to recent values under consideration [25]. The exponential moving average is calculated by multiplying past moving average of (n-1) trust values by one "smoothing factor" which is **(1 – α)**, then multiplying latest trust value by another "smoothing factor" which is $\boldsymbol{\alpha}$ and adding the two. The two "smoothing factors" combined always equal 1.00 [26].

5. Analysis and Evaluation

5.1 Theoretical Analysis of the Model

Proposition 01: The value of Reliability ($Re_{d,t}$) will always remain in the range of zero and one.

Proof:

Case 1: In a best possible scenario, the device is disseminating the data as per configured frequency and readings are in predefined range. We can set $\beta = 0$ and $\boldsymbol{\gamma} = 0$ [27]. By putting these values in Equation 2 and 3, we get $F_v = 1$ and $R_v = 1$. substituting these values in Equation 1, we get the following result:

$$Re_{d,t} = \frac{1+1}{2} = 1 \tag{13}$$

Case 2: In case the device is sending the data as configured frequency, but the reading is not correct keeping in view SOI as "extreme". Again $\beta = 0$ but $\boldsymbol{\gamma} = 1$ (Refer to table 4). By putting these values in equation 2 and 3, result in Fv =1 and R_v = 0. Substituting the values of Fv and R_v in Equation 1, will generate the following result:

$$Re_{d,t} = \frac{1+0}{2} = 0.50 \tag{14}$$

Case 3: The device is transferring the data as configured frequency, but the reading is not correct keeping in view disease in "major" category. Now $\beta = 0$ but $\boldsymbol{\gamma} = 0.75$ (Refer to Table 4) [28]. By using these values in equation 2 and 3, we get Fv =1 and R_v = 0.25. Substituting the values of Fv and R_v in Equation 1, will generate the following result.

$$Re_{d,t} = \frac{1+0.25}{2} = 0.625 \tag{15}$$

Case 4: The device is sending the data as configured frequency, but the reading is not correct keeping in view disease in "moderate" category. Now $\beta = 0$ but $\boldsymbol{\gamma} = 0.50$. By entering these values in equation 2 and 3, we get Fv =1 and R_v = 0.50. Putting the values of Fv and R_v in Equation 1, the value of $Re_{d,t}$ is:

$$Re_{d,t} = \frac{1+0.50}{2} = 0.75 \tag{16}$$

Case 5: The device is disseminating the data as configured frequency, but the reading is not correct keeping in view disease in "minor" category. Hence $\beta = 0$ but $\boldsymbol{\gamma} = 0.25$. By using these values in equation 2 and 3, we get Fv =1 and R_v = 0.75. After entering the values of Fv and R_v in Equation 1, we get the following result:

$$Re_{d,t} = \frac{1 + 0.75}{2} = 0.875 \tag{17}$$

Case 6: The device under consideration is not producing the data as configured frequency for a mission-critical application. However, the reading is in predefined range [29]. By using the values of $\beta = 1$ and $\boldsymbol{\gamma} = 0$ in equation 2 and 3 respectively, we get:

$$Re_{d,t} = \frac{0 + 1}{2} = 0.50 \tag{18}$$

Case 7: The device is not emitting the data as per configuration for mission-critical application neither the reading is in predefined ranges for "extreme" SOI. In this situation $\beta = 1$ and $\boldsymbol{\gamma} = 1$. Hence, we get Fv = 0 and R_v = 0 by using equation 2 and 3.

$$Re_{d,t} = \frac{0 + 0}{2} = 0 \tag{19}$$

Case 8: The device is not producing the data as per configured frequency for mission-critical application neither the reading is in predefined ranges for "major" type of disease. In this situation $\beta = 1$ and $\boldsymbol{\gamma} = 0.75$. Hence, we get Fv = 0 and R_v = 0.25 by using equation 2 and 3.

$$Re_{d,t} = \frac{0 + 0.25}{2} = 0.125 \tag{20}$$

Case 9: The device is not sending the data at a rate as expected for mission-critical application. Also, the reading is not in predefined ranges for "moderate" SOI. In this situation $\beta = 1$ and $\boldsymbol{\gamma} = 0.50$. Hence, we get Fv = 0 and R_v = 0.50 by using equation 2 and 3.

$$Re_{d,t} = \frac{0 + 0.50}{2} = 0.25 \tag{21}$$

Case 10: The device is not disseminating the data at configured frequency for mission-critical application and the reading produced by the device is also not in predefined ranges for "minor" SOI. In this situation $\beta = 1$ and $\boldsymbol{\gamma} = 0.25$. so, we get Fv = 0 and R_v = 0.75 by using equation 2 and 3.

$$Re_{d,t} = \frac{0 + 0.75}{2} = 0.375 \tag{22}$$

By investigating all possible scenarios for a mission-critical application like assisted healthcare, it is concluded that the value of $Re_{d,t}$ will always remain between zero and one.

Table 5. Reliability scenario summary

Scenario	$\boldsymbol{Fv}$	$\boldsymbol{R_v}$	$\boldsymbol{Re_{d,t}}$
Case 1	1	1	1
Case 2	1	0	0.5
Case 3	1	0.25	0.625
Case 4	1	0.5	0.75
Case 5	1	0.75	0.875
Case 6	0	1	0.5
Case 7	0	0	0
Case 8	0	0.25	0.125
Case 9	0	0.50	0.25
Case 10	0	0.75	0.375

Proposition 02: The device availability (available, partially available and un-available) is considered based on the values of $Av_{d,t}$ where values range between zero and one.

Proof:

Case 1: In the best-case scenario, when P_{rev} are same as P_{tran}. If it is assumed that n number of packets were sent to the device under consideration and r number of packets were received where $= r$. By using the eq (4)

$$Av_{d,t} = \frac{n}{n+(n-n)} = 1 \quad (23)$$

Case 2: There are some packet drops because of device exploits. If n packets are sent and r packets are received in a way that $r < n$

$$Av_{d,t} = \frac{r}{n+(n-r)} < 1 \quad (24)$$

Case 3: In the worst-case scenario, when n packets are sent, and no packet is received back i.e. $r = 0$

$$Av_{d,t} = \frac{0}{n+(n-0)} = 0 \quad (25)$$

Case 4: In rare case scenario, when n packets are sent, and r packets are received in a way that $r > n$ which shows malfunctioning of the device & declared as un-available

$$Av_{d,t} = \frac{r}{n+(n-r)} > 1 \text{ or undefined } (\infty) \quad (26)$$

Proposition 03: The device is considered responsive if the value of $Rt_{d,t} < 1$ where the maximum acceptable response time is configurable based on nature of the application.

Proof:

Assumption: It is assumed that RT is independent of any congestion and delay caused by network traffic. For theoretical analysis of the proposed model, we assume the following maximum acceptable response time values corresponding to each application type:

Table 6. Values of maximum acceptable time

Type of Application	RT_{max} (ms)
Mission-critical	10
Real-Time	15
Rate-Critical	20
Others	< 100

Case 1: For a mission-critical application like assisted healthcare the RT_{max} is set to 10 ms. In case when RT is greater than RT_{max} , putting values in equation (5)

$$Rt_{d,t} = \frac{RT}{RT_{max}} > 1 \Rightarrow \text{not acceptable and value of } Rt_{d,t} \text{ will be set to zero} \quad (27)$$

Case 2: When RT is same as RT_{max} or even lower than RT_{max}. Using equation (5), we can conclude:

$$Rt_{d,t} = \frac{RT}{RT_{max}} \leq 1 \Rightarrow \text{acceptable and value of } Rt_{d,t} \text{ will be set to one in final trust estimation} \quad (28)$$

Proposition 04: Trust value of a device is always in the range from zero to one.

Proof:

Case 1: The identity of the device is not proved as per implemented authentication mechanism. However, the device is reliable in any respect, available and response time is in acceptable range.

$$T_{d,t} = 0 \times \left[\frac{1+1+1}{3}\right] = 0 \Rightarrow \text{untrusted} \quad (29)$$

By using the Trust estimation equation, the values of $T_{d,t} = 0$. Hence, we conclude that the device is un-trustworthy even though if it is reliable, available and response time is in acceptable range.

Case 2: The device identity is proved, reliability is as per case 1 (refer to table 4), device is available and response time is acceptable. By using trust estimation equation:

$$T_{d,t} = 1 \times \left[\frac{1+1+1}{3}\right] = 1 \Rightarrow \text{trusted} \quad (30)$$

Case 3: The device identity is proved by existing authentication mechanism, reliability is as per case 2 (refer to table 4), the device is available, and RT is acceptable. By using equation (7):

$$T_{d,t} = 1 \times \left[\frac{0.5+1+1}{3}\right] = 0.83 \Rightarrow \text{uncertain} \quad (31)$$

Case 4: The device identity is verified, reliability is as per case 3 (refer to table 4), the device is available, and *RT* is acceptable. By using equation (7):

$$T_{d,t} = 1 \times \left[\frac{0.625+1+1}{3}\right] = 0.87 \Rightarrow \text{trusted} \quad (32)$$

Case 5: The device identity is proved by existing authentication procedure, reliability is as per case 4 (refer to table 4), the device is available, and *RT* is acceptable. By using equation (7):

$$T_{d,t} = 1 \times \left[\frac{0.75+1+1}{3}\right] = 0.91 \Rightarrow \text{trusted} \quad (33)$$

Case 6: The device identity is evidenced, reliability is as per case 5 (refer to table 4), the device is available, and *RT* is acceptable. By using equation (7):

$$T_{d,t} = 1 \times \left[\frac{0.875+1+1}{3}\right] = 0.95 \Rightarrow \text{trusted} \quad (34)$$

Case 7: The device identity is proved by existing authentication procedure, reliability is as per case 6 (refer to table 4), the device is available, and *RT* is acceptable. By using equation (7):

$$T_{d,t} = 1 \times \left[\frac{0.50+1+1}{3}\right] = 0.83 \Rightarrow \text{uncertain} \quad (35)$$

Case 8: The device identity is verified by in place authentication mechanism, reliability is as per case 7 (refer to table 4), the device is available, and *RT* is acceptable. By using equation (7):

$$T_{d,t} = 1 \times \left[\frac{0+1+1}{3}\right] = 0.66 \Rightarrow \text{untrusted} \quad (36)$$

Case 9: The device identity is evidenced, reliability is as per case 8 (refer to table 4), the device is available, and *RT* is acceptable. By using equation (7):

$$T_{d,t} = 1 \times \left[\frac{0.125+1+1}{3}\right] = 0.70 \Rightarrow \text{untrusted} \quad (37)$$

Case 10: The device identity is verified by existing authentication mechanism, reliability is as per case 9 (refer to table 4), the device is available, and *RT* is acceptable. By using equation (7):

$$T_{d,t} = 1 \times \left[\frac{0.25+1+1}{3}\right] = 0.75 \Rightarrow \text{untrusted} \quad (38)$$

Case 11: The device identity is proved by existing authentication procedure, reliability is as per case 10 (refer to table 4), the device is available, and *RT* is acceptable. By using equation (7):

$$T_{d,t} = 1 \times \left[\frac{0.375+1+1}{3}\right] = 0.79 \Rightarrow \text{uncertain} \quad (39)$$

Case 12: The device identity is proved by existing authentication procedure, the device is reliable as per case 1 (refer to table 4), the device is unavailable, and *RT* is acceptable. By using equation (7):

$$T_{d,t} = 1 \times \left[\frac{1+0+1}{3}\right] = 0.66 \Rightarrow \text{uncertain} \quad (40)$$

Case 13: The device identity is proved, reliability is as per case 1 (refer to table 4), the device is partially available, and *RT* is acceptable. By using equation (7):

$$T_{d,t} = 1 \times \left[\frac{1+0.5+1}{3}\right] = 0.83 \Rightarrow \text{uncertain} \quad (41)$$

Case 14: The device identity is verified, reliability is as per case 1 (refer to table 4), the device is available, and *RT* is not acceptable. By using equation (7):

$$T_{d,t} = 1 \times \left[\frac{1+1+0}{3}\right] = 0.66 \Rightarrow \text{uncertain} \quad (42)$$

Some of the cases are not mentioned deliberately where the identity of the device is not proved and hence the related trust value is zero to represent the device as un-trusted. The above scenarios can be plotted in a line graph (Fig. 3) to represent the impact of different parameters on trust estimation of a device.

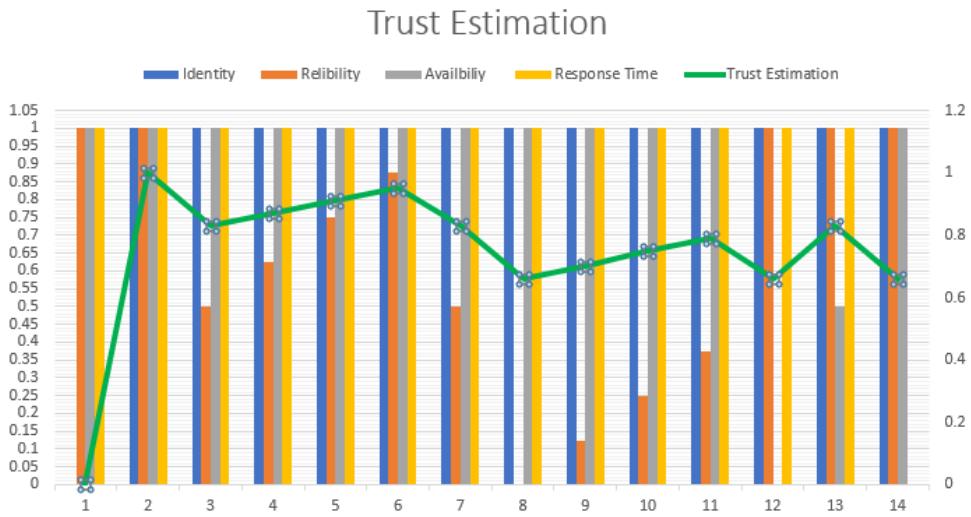

Fig. 3. Impact of trust parameters on trust estimation

Proposition 05: Reputation value of a device is always in the range from zero to one.

Proof:

For simplicity, we are considering latest five readings from stored trust values of a device "d" to calculate its reputation using equation (8)

Table 7. Case 1

Time stamp	Device Identity	Trust Status	Trust value
00:00:10	D1	Trusted	1
00:00:20	D1	trusted	1
00:00:30	D1	Trusted	1
00:00:40	D1	Uncertain	0.5
00:00:50	D1	untrusted	0

$$Rep_{d,t} = 0.6 \text{ x } (0) + 0.4 \text{ x } \left(\frac{1+1+1+0.5}{4}\right) = 0.35 \Rightarrow \text{untrusted} \quad (43)$$

Table 8. Case 2

Time stamp	Device Identity	Trust Status	Trust value
00:00:10	D1	untrusted	0
00:00:20	D1	untrusted	0
00:00:30	D1	uncertain	0.5
00:00:40	D1	uncertain	0.5
00:00:50	D1	trusted	1

$$Rep_{d,t} = 0.6 \text{ x } (1) + 0.4 \text{ x } \left(\frac{0+0+0.5+0.5}{4}\right) = 0.70 \Rightarrow \text{uncertain} \quad (44)$$

Table 9. Case 3

Time stamp	Device Identity	Trust Status	Trust value
00:00:10	D1	untrusted	0
00:00:20	D1	untrusted	0
00:00:30	D1	uncertain	0.5
00:00:40	D1	trusted	1
00:00:50	D1	trusted	1

$$Rep_{d,t} = 0.6 \text{ x } (1) + 0.4 \text{ x } \left(\frac{0+0+0.5+1}{4}\right) = 0.75 \Rightarrow \text{uncertain} \quad (45)$$

$$Rep_{d,t} = 0.6 \text{ x } (1) + 0.4 \text{ x } (\frac{1+0.5+0.5+1}{4}) = 0.90 \Rightarrow \text{trusted} \quad (46)$$

Table 10. Case 5

Time stamp	Device Identity	Trust Status	Trust value
00:00:10	D1	uncertain	0.5
00:00:20	D1	uncertain	0.5
00:00:30	D1	uncertain	0.5
00:00:40	D1	trusted	1
00:00:50	D1	trusted	1

$$Rep_{d,t} = 0.6 \text{ x } (1) + 0.4 \text{ x } (\frac{0.5+0.5+0.5+1}{4}) = 0.85 \Rightarrow \text{trusted} \quad (47)$$

Table 11. Case 6

Time stamp	Device Identity	Trust Status	Trust value
00:00:10	D1	trusted	1
00:00:20	D1	trusted	1
00:00:30	D1	trusted	1
00:00:40	D1	trusted	1
00:00:50	D1	uncertain	0.5

$$Rep_{d,t} = 0.6 \text{ x } (0.5) + 0.4 \text{ x } (\frac{1+1+1+1}{4}) = 0.70 \Rightarrow \text{uncertain} \quad (48)$$

Table 12. Case 7

Time stamp	Device Identity	Trust Status	Trust value
00:00:10	D1	uncertain	0.5
00:00:20	D1	uncertain	0.5
00:00:30	D1	uncertain	0.5
00:00:40	D1	uncertain	0.5
00:00:50	D1	uncertain	0.5

$$Rep_{d,t} = 0.6 \text{ x } (0.5) + 0.4 \text{ x } (\frac{0.5+0.5+0.5+0.5}{4}) = 0.50 \Rightarrow \text{uncertain} \quad (49)$$

All above cases show that the reputation of a device "d" remains in range from zero to one to reflect its status as trusted, uncertain and untrusted at the time of reputation calculation.

6. Conclusion and Future Work

The use of smart devices, IoT devices, is increasing tremendously with the passage of time in all walk of life. The usage of IoT in healthcare is also getting momentum but at the same time, it is a big concern that the data being gathered and transmitted by untrusted IoT devices to be used by healthcare applications and practitioners may be disaster. In this paper, we have proposed and evaluated a mathematical model to estimate the trust of IoT devices. The proposed model is supposed to be quite accurate and efficient in constrained environment. The accuracy and efficiency evaluation of the proposed model is part of our future research work. Further, the Domain Adaptive Risk-based Trust management model needs proof to check how vigorous the model is against possible attacks, especially the attacks which may affect the estimation of trust or in other words affecting the parameters which are proposed in estimating the trust of under consideration scenario. Being resilient is crucial for a security model, especially concerning about attack resistance because the purpose of the model is to protect the object from various possible vulnerabilities and attacks. It is planned to create related simulation in Cooja, a Contiki based simulator for constrained IoT devices, to test different scenarios as explained above and evaluate the performance, accuracy and resilience of the depicted model. Afterwards, same scenarios will be tested on real testbed using Raspberry Pi 3 B+ and some useful sensors being used in healthcare system.

References

[1] Minerva, R., Biru, A., & Rotondi, D. (2015). Towards a definition of the Internet of Things (IoT). IEEE Internet Initiative, 1(1), 1-86.

[2] Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer networks, 54(15), 2787-2805.

[3] Li, J., Huang, Z., & Wang, X. (2011, May). Notice of Retraction: Countermeasure research about developing Internet of Things economy: A case of Hangzhou city. In 2011 International Conference on E-Business and E-Government (ICEE) (pp. 1-5). IEEE.

[4] Pang, Z. (2013). Technologies and Architectures of the Internet-of-Things (IoT) for Health and Well-being (Doctoral dissertation, KTH Royal Institute of Technology).

[5] Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The internet of things for health care: a comprehensive survey. IEEE access, 3, 678-708.
[6] Das, M. L. (2015, February). Privacy and security challenges in internet of things. In International Conference on Distributed Computing and Internet Technology (pp. 33-48). Springer, Cham.
[7] Radcliffe, J. (2011, August). Hacking medical devices for fun and insulin: Breaking the human SCADA system. In Black Hat Conference presentation slides (Vol. 2011).
[8] Rauf, A., Shaikh, R. A., & Shah, A. (2018, February). Security and privacy for IoT and fog computing paradigm. In 2018 15th Learning and Technology Conference (L&T) (pp. 96-101). IEEE.
[9] Gambetta, D. (2000). Can we trust trust. Trust: Making and breaking cooperative relations, 13, 213-237.
[10] McKnight, D. H., & Chervany, N. L. (1996). The meanings of trust.
[11] Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. Journal of network and computer applications, 42, 120-134.
[12] Gu, L., Wang, J., & Sun, B. (2014). Trust management mechanism for Internet of Things. *China Communications*, *11*(2), 148-156.
[13] Arabsorkhi, A., Haghighi, M. S., & Ghorbanloo, R. (2016, September). A conceptual trust model for the Internet of Things interactions. In *2016 8th International Symposium on Telecommunications (IST)* (pp. 89-93). IEEE.
[14] Atzori, L., Iera, A., & Morabito, G. (2011). Siot: Giving a social structure to the internet of things. *IEEE communications letters*, *15*(11), 1193-1195.
[15] Nitti, M., Girau, R., Atzori, L., Iera, A., & Morabito, G. (2012, September). A subjective model for trustworthiness evaluation in the social internet of things. In *2012 IEEE 23rd international symposium on personal, indoor and mobile radio communications-(PIMRC)* (pp. 18-23). IEEE.
[16] Bao, F., & Chen, I. R. (2012, September). Dynamic trust management for internet of things applications. In *Proceedings of the 2012 international workshop on Self-aware internet of things* (pp. 1-6).
[17] Bao, F., & Chen, R. (2012, June). Trust management for the internet of things and its application to service composition. In *2012 IEEE international symposium on a world of wireless, mobile and multimedia networks (WoWMoM)* (pp. 1-6). IEEE.
[18] Køien, G. M. (2011). Reflections on trust in devices: an informal survey of human trust in an internet-of-things context. *Wireless personal communications*, *61*(3), 495-510.
[19] Xu, X., Bessis, N., & Cao, J. (2013). An autonomic agent trust model for IoT systems. *Procedia Computer Science*, *21*, 107-113.
[20] Gligor, V., & Wing, J. M. (2011, March). Towards a theory of trust in networks of humans and computers. In *International workshop on Security Protocols* (pp. 223-242). Springer, Berlin, Heidelberg.
[21] Chen, D., Chang, G., Sun, D., Li, J., Jia, J., & Wang, X. (2011). TRM-IoT: A trust management model based on fuzzy reputation for internet of things. *Computer Science and Information Systems*, *8*(4), 1207-1228.
[22] Leister, W., & Schulz, T. (2012, May). Ideas for a Trust Indicator in the Internet of Things. In *The First International Conference on Smart Systems, Devices and Technologies*. Oslo: SMART Press.
[23] Al-Hamadi, H., & Chen, R. (2016, October). Trust-based decision making for environmental health community of interest IOT systems. In *2016 IEEE 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)* (pp. 1-6). IEEE.
[24] Horn, S. D., Horn, R. A., & Sharkey, P. D. (1984). The Severity of Illness Index as a severity adjustment to diagnosis-related groups. *Health Care Financing Review*, *1984*(Suppl), 33.
[25] https://www.investopedia.com/ask/answers/difference-between-simple-exponential-moving-average, 05/05/2019 [Online]
[26] https://www.schwab.com/active-trader/insights/content/trend-your-friend-using-moving-averages, 07/05/2019 [Online]
[27] Rehiman, KA Rafidha, and S. Veni. "A trust management model for sensor enabled mobile devices in IoT." In 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), pp. 807-810. IEEE, 2017.
[28] Wang, Bo, Mingchu Li, Xing Jin, and Cheng Guo. "A reliable IoT edge computing trust management mechanism for smart cities." IEEE Access 8 (2020): 46373-46399.
[29] Radwan, Neyara, and Maged Farouk. "The Growth of Internet of Things (IoT) In The Management of Healthcare Issues and Healthcare Policy Development." International Journal of Technology, Innovation and Management (IJTIM) 1, no. 1 (2021): 69-84.

Authors' Profiles

Abdul Rauf received a B.Sc. degree in mathematics from Punjab University, Pakistan, and a Master's degree in Computer Sciences from Quaid-e-Azam University, Islamabad, Pakistan in 1997. After his master's degree, he worked for almost twelve years in a pioneer ISP in Pakistan in different technical positions. He possesses a number of relevant technical certifications from well-renowned industry giants. He is currently a Ph.D. candidate in the faculty of Information and Communication Technology (KICT), IIUM, Malaysia. His research interests include privacy, security, and trust management in different types of networks, especially in IoT.

Riaz Ahmed Shaikh is an Associate Professor at the CS Dept. in the King Abdulaziz University, Jeddah, Saudi Arabia. He obtained his Ph.D. from Computer Engineering Dept., of Kyung Hee University, Korea, 2009, and his M.S. in IT from the National University of Science and Technology, Pakistan, 2005. His research interest includes Wireless Sensor Networks, Security, Vehicular Networks, Internet of Things, Privacy, and Trust management. He is a professional member of the ACM and EC-Council

Prof. Dr. Asadullah Shah is working at Kulliyyah of ICT, International Islamic University Malaysia. He did his Ph.D. from the University of Surrey UK in 1998, with a specialization in Multimedia. He started his academic carrier at the University of Sindh Jamshoro, Pakistan, in 1986 as a lecturer. Before joining IIUM, he worked as Head of Telecommunication Engineering & Management department, IoBM Karachi Sindh, Dean Faculty of Computer and Management Sciences, Isra University Hyderabad Sindh, and Head of Telecommunication Engineering and IT, Sukkur IBA, Sindh-Pakistan. He has published 275 research articles in highly reputable international and national journals in the fields of computers, communication, and IT. Also, he has published 12 books and is Chief Editor of the Journal of Information Systems and digital technologies (JISDT) of IIUM. His fields of interest are social media and behavior modeling, e-learning, and computer game-based learning for adults and school children. He has been invited as a keynote speaker, general and executive chair for multiple IEEE conferences such as ICETAS, ICIRD held every year in various parts of the world.

How to cite this paper: Abdul Rauf, Riaz Ahmed Shaikh, Asadullah Shah, " Trust Modelling and Management for IoT Healthcare", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.12, No.5, pp. 21-35, 2022. DOI:10.5815/ijwmt.2022.05.03