Journal of Graphic Era University
Vol. 5, Issue 2, 69-83, 2017
ISSN: 0975-1416 (Print), 2456-4281 (Online)

Pervasive m-Healthcare Framework for Diabetes

Madhu Sharma Gaur[1*], Bhasker Pant[2]

[1]G. L. Bajaj Institute of Technology and Management, Greater Noida, India
[1,2]Department of Information Technology
Graphic Era University, Dehradun, India
[*]Corresponding author: madhu14nov@gmail.com

(Received June 2, 2016; Accepted September 21, 2016)

Abstract
Vision of pervasive computing includes wireless communication and information processing anywhere, anytime using mobile sensor devices connected seamlessly. Pervasive environment characterized by highly dynamic, open and diverse infrastructure where resource-restricted dissimilar mobile objects have the ability of Ad-hoc network set-up, self-organization and cooperation for information exchange and distributed operation unknown by the user. In such open computing environments, traditional security schemes and encryption algorithms cannot be always applied to address the security assurance challenges. Therefore, concepts of trust and reputation evaluation emerged by researchers. In addition to that in human-centric healthcare applications, reliability and trustworthiness between communicating nodes, quality of information assessment cannot be effectively ensured through hard security concerns. Thus soft security analysis becomes an important aspect for enhancing the security assurance and degree of trust in ICT enabled application and services where information is ubiquitous. In our proposed research work, we explore existing pervasive security and trust methods to assess the challenging gap. We put forward need of soft security and proposed a trust metric for trust based security assessment with classical clustering technique for energy-efficient resource restricted trusted and secure communication. Major security attacks and impact of signal strength on security for unnoticed pervasive services also evaluated. In winding up, we present pervasive healthcare application framework especially focused to awareness and quality remote care for diabetes, to realize and validate the conceptual model with case study.

Keywords- Diabetes, Mobile Pervasive Environment, Pervasive m-Healthcare, Security Assurance, and Trust Management.

1. Introduction

In the vision of pervasive or ubiquitous computing (Weiser, 1991) development of human-centric, mobile applications being encouraged to offer services anywhere anytime. In the pervasive environment set of wireless technologies, dissimilar mobile sensor devices connected seamlessly for distributed operations relying on highly dynamic, heterogeneous decentralized, self-organized network setup unknown by user. There are various application and service had already designed and developed in the domains like business, education, healthcare, travel, entertainment and many more. Because of open, dynamic pervasive ad-hoc network setup, there are still challenges technical, economic and social challenges need to address to enhance the assurance and acceptance of such applications. In this paper, precisely present our research work and propose a trust based secure pervasive healthcare framework especially focused to awareness and quality remote care for diabetes, to realize and validate the conceptual model with case study. From the last decade, m-healthcare solutions and deliveries are becoming the major areas of concern for research and commercial advancement.

Diabetes is one of the most common non-communicable diseases in which could be controlled at significant level by community awareness, self-care and knowledge sharing between trusted users group. Viewing long-term outcome, number of patients growing from diseases first stage to critical stage or going to other secondary chronic diseases could be reduced through such initiatives. There are two major types of diabetes, Type-I, in which our body cannot produce insulin wand Type II describes when our body repel to use insulin. Type II diabetes remained undetected for many cases. Diabetic patients are rising every year. As per the estimation done in 2010, 285 million people had diabetes and the statistics increased to 381 million in the year 2013 done by International Diabetes Federation (IDF, 2013). Continuing with same it becomes 387 billion in 2014 worldwide and predicted 592 million diabetics by 2035 (Nwin et al., 2011). IDF Diabetes Atlas (International Diabetes Federation, 2014) Global estimates of the prevalence for diabetes states estimated 61.3 million people aged 20-79 years live with diabetes in India; 2011 estimates. This number is, expected to increase to 101.2 million by 2030. Extreme distressing fact is the trend of rising diabetes in quite younger age on average 10 year alarmingly high for community researchers. Problem of Diabetes in India has passed the stage to the epidemic and every day increasing number make the country DIABETES CAPITAL of the world. Now healthcare concern is not an individual concern, it becomes an exorbitantly public health problem.

As we know self-care is directly depending upon the awareness about the diseases, its post causes. Regular stimulus and support related to food, physical activity, trusted members success story sharing and experts' interventions through SMS/Alerts or Voice/Video messages for uneducated, less skilled and users in their daily life routine. These services could be provided users by connecting them through their own basic smart devices. As per the research study done (CISCO, 2010-2015), exponential growth of "Mobile-Only-Internet" user indicated. This population has been increased up to 56 folds, from 14 million to 788 million by the end of 2015 in the emerging market like India. Authors (Sridhar and Hämmäinen, 2011) also stated a survey record about mobile Internet users in India in last one year has increased from 8 million to 25 million where about 49% of Internet users use Mobile only for accessing the Internet. Although major challenges for accessing such services are first one, less, WSN Infrastructure for broadband access secondly comparatively insufficient distribution of Mobile application and services than mobile services compared to developed countries and advanced markets, thirdly Trustworthiness and assurance for acceptance and finally education and awareness. Rest of the paper is organized as in 2. Literature review, 3 Motivation, 4 describes in detail our Proposed Research, 5. Research Method, 6. Research Outcomes and finally 7. Conclusion and future work.

2. Literature Review

For WSN and Mobile Ad-Hoc Networks (MANETs), various trust management models are used to gage malicious node behavior and security countermeasures, reliability and connection availability issues. LEACH (Low Energy Adaptive Clustering Hierarchy) defined (Bao et al., 2011) as an energy-efficient based on distributed cluster formation where cluster head allows performing accumulated operations to save energy in different operations by different nodes for data transmissions. Communicating nodes communication history and experience proposed reputation based data integrity using watchdog security mechanism for detecting invalid data and compromised nodes (Liu et al., 2009; Cho et al., 2011; Bao et al., 2012; Velloso et al., 2010). Combined certificate-based and behavior-based trust models discussed by (Bao et al., 2012; Ali et al., 2012; Hsieh et al., 2007) for trust assessment in WSN. For Trust computation encryption/decryption, digital signature creation for secure delivery specified by Trusted Computing Group (TCG) defined Mobile Trusted Module (MTM) (Trusted Computing Group 2009, 2010). To ideally combine continuous authentication and intrusion detection in highly dynamic MANET has been discussed also (Bu et al., 2011). Cluster formation and Cluster head selection with the scalability and energy efficiency for node life span defined by different researchers in their work (Bao et al., 2011; Hsieh et al., 2007; Ghorbel et al., 2009; El-Haleem and Ali, 2011). A trust routing protocol describing selfishness for MANET by packet sinking defined in TRIUMF. A widely known model named PTM (Almenarez et al., 2004) proposed to evaluate indirect trust values without considering fuzzy, subjective and uncertainty. In the literature for security and energy-efficient protocols defined by community researchers (Ali et al., 2012; Yang et al., 2004) using standard clustering technique and cluster head selection is based on different parameters like connectivity, remaining battery energy, trust information of links, mobility and node ID. SS-LEACH, RLEACH also defined by Zhang et al. (2008), as a further enhanced versions of LEACH protocol to secure mobile ad-hoc environments where energy efficiency is critical. A multi path cluster head chain to communicate with base stations is used to increase the network lifetime.

Pervasive healthcare research for diabetes survey reports, articles, and peer reviewed research papers magazines and newspapers also explored to identify the need of ICT enabled smart space solutions and deliveries (Acampora et al., 2013) Deliberately explain the technology needs and infrastructure needed for ambient intelligence in the pervasive healthcare and concluded with the e activity recognition, behavioral pattern discovery, decision support systems, methods. Unified architectural model with wireless technologies and pervasive healthcare applications like fall and activity detection, location tracking, vital signs and medication intake monitoring also discussed by Alemdar and Ersoy (2010). Electronic Health Records (EHM) is another healthcare system (International Diabetes Federation, 2014) for database synchronization through RFID tag access to the entire stakeholder like patient and healthcare workers where imbedding RFID technology with dissimilar sensors devices is less achievable. Altcare and SmartCondo (Liang et al., 2012), are smart home pervasive healthcare systems proposed to monitor every single movement of the patient and storing the data in 2D or 3D pictures with patient privacy. Some of the instant challenges in pervasive m-healthcare solutions are privacy, trust, context awareness and energy-efficiency needs further exploration and research.

3. Motivation

Pervasive environment is highly dynamic, open and decentralized environment which is always susceptible for incipient security challenges. It becomes more critical if such environment is used for human-centric applications and services especially in like pervasive healthcare. For successful delivery pervasive healthcare requires technically and conceptually realistic implementable security mechanisms with privacy and trustworthiness for pitching the human behavior for acceptance.

Diabetes is one such disease, where an individual’s behavior towards disease, action plans and decisions plays an important role for the prevention and cure. People suffering from disease despite knowing the future implications, sometimes behave irrationally and take impulsive decisions. Financial liabilities are also another major stress for patients and their families in the developing countries like India. Diabetes is growing alarmingly in India (IDF, 2013). It is also identified source of other secondary long-lasting diseases and announced as fifth death leading cause in America. These are the motivating facts for proposing our trusted and secure pervasive healthcare application framework for diabetes in Indian scenario that will enhance the community awareness self-care behavior about the dieses, control the conversion of patients from initial stage to advanced stage and finally minimize the hospital stay at critical stage cure through remote diagnosis and monitoring. Reasonably such needs motivate us for proposed work below discussed challenges and opportunities lead towards the contribution for community wellbeing.

4. Proposed Research

4.1 System Model

Regardless of Pervasive environment characteristics and infrastructure glitches, trustworthiness privacy and security are few open challenges in this resource-restricted computing. Traditional security consists of Confidentiality, Integrity, Availability (CIA), deliberately designed for digital security that is insufficient to address the WSN dynamic infrastructure. Capturing, storing and managing m-healthcare records sensor or micro-sensor device seamlessly communicate between healthcare stakeholders. Despite of substantial advancement in Wireless Sensor Technology and unending research Pervasive healthcare have many security assurance issues, some of them are partially addressed many more still persisted to be addressed like-

(i) Attack, Threats, and Eavesdropping on wireless seamless channels and connections.
(ii) Malicious and compromised behavior node detection and
(iii) Security and Privacy requirements for data confidentiality, integrity and availability.
(iv) Integration of socio-technical perspective especially for community wellbeing like m-healthcare.
(v) Trusted relationship and Trustworthiness.
(vi) Context awareness.
(vii) Mobility, adaptability, dynamism.

Inspiring from the thought of (Chang et al., 2006), “Trust is synonymous to Security”, our trust based soft security mechanism broadly works in subsequent phases as a) Impetuous behavior monitoring of communicating nodes, b) identification of social and QoS trust parameters c) Designing a Trust Metric for trust measurement, and finally threats and attack detection. Literature reviewed and study of existing Trust and Security metrics had been explored to highlight the need for n-dimensional vision of Trust Management and security assurance in ubiquitous computing where analyzing trust is done from:

(i) Direct vs. Indirect Trust computation.
(ii) Hard vs. Soft Trust solutions.
(iii) Trust based soft security by monitoring dynamic behavior of communicating nodes identifying insider attacks in trustworthy environment.

We investigate the trust and security challenges and appraise the opportunities in autonomous mobile pervasive ad hoc networks to improve security assurance. Malicious node detection is monitoring of node's impulsive behavior leads malicious node detection based on immoral snooping of the communicating channels. We consider following scenarios in the monitoring intrusive/malicious behavior dynamically to design security aware framework:

(i) Node's impetuous behavior with high mobility and self-organized infrastructure, new approved routes accessible that are challenging to detect during the learning phase.

(ii) Impetuous node behavior reason to become malicious node also known as compromised and starts encouraging the permitted routes that may not be available.

(iii) Compromised behavior direct towards foreboding that is part of non-self-come about to become accessible as honest routes.

(iv) New Compromised behavior is never observed in the learning phase become part of non-self.

Trust in human notion based on the past experience and reputation is the key consideration for our research work. We present a Bio-Inspired approach using standard clustering technique and define a trust metric parameters where we observe the node behavior vulnerabilities requirements (Gaur and Pant, 2014). Concepts of trust computing based on reputation and other soft security components had been investigated and evaluate (Gaur and Pant, 2014). Security threats and insider attacks because of wireless packet transmission and impact of signal-strength attenuation has been also addressed for subjective area.

In the pervasive mobile environment, impact of signal-strength attenuation based on Received Signal Strength (RSS) models and algorithms explored to identify the signal-strength attenuation attacks (Gaur and Pant, 2015). An algorithm to dynamically detect the assailants on signal attenuation has been also presented. We formulate all-around signal strength attacks on sensor node which is able to receive the provocations only if the signal strength of the received packet is above the pre-defined threshold. It has been observed that on signal strength attenuation various types of attacks attempts to breach security as identified Sinkhole Attack identified when a pretender's aims to attract the traffic from compromised node with respect to the routing algorithms like Selective Forwarding Attacks, Sybil Attacks, Spoofing, Wormholes Mote-class and laptop-class attacks and Jamming attacks.

A combined energy efficiency trusted and secure clustering concerns with the mobility defined in our work done so far (Gaur and Pant, 2015). Where we use standard clustering technique used for energy saving. In clustering cluster head is chosen on the basis of cumulative trust computation by evaluating five social and QoS trust parameters, intimacy, integrity, energy, selfishness and reliability. The trust calculation is conducted, particularly between two neighbor nodes in a cluster. For example, to computer trust between node X and other communicating node Y at time t. We assume The trust value that node X evaluates towards node Y at time t, $T_{xy}(t)$, is represented as a real number in the range of [0, 1] where 0 indicates distrust and 1 complete trust. $T_{xy}(t)$ is computed by:

$$T_{xy}(t) = C1 * T_{xy}^{Intimacy} + C2 * T_{xy}^{Intigrity} + C3 * T_{xy}^{Mobility} + C4 * T_{xy}^{Selfishness} + C5 * T_{xy}^{\mathrm{Re}\,liability} \quad (1)$$

Here C1, C2, C3, C4 and C5 are the Costs associated with trust parameters with equal threshold of 0.2 and cumulative level of trust obtained from C1 + C2 + C3 + C4 + C5 = 1. The best trust values of C1, C2, C3, C4 and C5 are used to maximize system performance in terms of trust ranking as shown in Figure 1.

In our previous work, a scenario for monitoring nodes' impulsive behavior was presented to analyze, how node becomes compromised from initial learning phase to its destination. Trusted behavior and energy efficient combined with security assurance extension for cluster-head selection where lowest energy consumption has been observed as shown in Figure 2.

In general security setting and cluster head selections are assigned functions or locations based on the corresponding fitness factors which may not be optimal due to their compromising behavior. Similarly, route selection, mobility estimation, size of cluster and area can be also considered over the system life-time to make it optimal solution in the subjective search space. We consider that security should be evolved and adopt in such highly dynamic and heterogeneous environment. In addition to that imparting inherent security assurance at early stage of design, development and deployment in human-centric application framework also realized. In our proposed approach three fitness functions are used for comprehensive trust based security assurance with hierarchical clustering. On simulating the proposed unified approach, we observe that average energy consumption in different scenarios for packets transmission range over a time with probability of node mobility and lowest energy consumption resulted over existing similar models.

In this work, persists our previous work with pervasive m-healthcare scenario for diabetes in India to validate the approach. Currently many of the successful solutions including smart home, ubiquitous telemedicine, medical diagnosis and patient care, remote monitoring, electronic health record system to monitor specific conditions such as elderly individual monitoring are used ranging from sensors to mobile phones and intelligent health aware mobile devices managing pervasive life style.

4.2 Proposed Pervasive m-Healthcare Conceptual Framework

There are some solutions already exists and ongoing research projects and commercial application are under design and production line. Pervasive computing is characterized by highly dynamic, heterogeneous and mobile environment to human-centric solutions by ad hoc association and seamless communication. To provide better understanding of trust computation and energy efficiency with inherent security assurance extension at the early stage of designing and developing, we propose a pervasive m-healthcare applications framework.

Trusted security assurance can be a supplementary strategy for enhancing the successful service delivery for self-care or hospital care in case of chronic disease. Assuming trust in human notion and soft security concerns may enhance such solutions deployment access for community wellbeing. The work of doctors is basically tied to the physical circle of the patient instead of making digitally available the healthcare services. Thus healthcare providers, patients and family members can be seamlessly connected to frequently reveal poor adherence of both medicinal interventions and inadequate communication by remote care through pervasive m-healthcare service delivery where information is ubiquitous.

For understanding the proposed approach, we have not adopt traditional way of case study evaluation through how and why questions considering an exploratory research at this stage. We have chosen the case on demand of society wellbeing efforts needed with the technology advancements. In the developing market like India where mobile users are increasing day by day, but common ICT enabled solutions, application implementation and automation is still at foundation stage. Thus we instigate the wireless applications especially using basic smart phones for diabetes patients.

Further case illustration is not simply an example for technology mediated solution to address healthcare disparity. It will provide a charter for diabetes care with affordable overheads. Inadequate healthcare delivery structures inspiring instruments for examining pervasive healthcare challenges and opportunities and growing demand applications and services for better to present an open source pervasive healthcare application framework that persist our previous work; energy efficient trust based secure clustering, for rapidly growing diseases Diabetes in India. Pervasive healthcare application ecosystem shown in Figure 3, to present the integration of wireless technology and process flow with rules in dynamic information space in the trusted cluster in the context of research objective for trustworthiness and security assurance.

Information processing has been systematically integrated at mobile App through user friendly interface as shown in Figure 4. Disease awareness, expert's intervention or remote diagnosis will be incorporated with our everyday routine activities and objects from the m-hospital from webs application. For the effective acceptance Strong wireless sensor technology and mobile communication support with energy efficient trust based security assurance for pervasive healthcare network to create balance between system and healthcare application stakeholders.

A distributed end-to-end multi-tier trust based secure pervasive healthcare framework has been proposed for pervasive medical care as a case study, shown in Figure 5, consists of pervasive environment, mobile devices, pervasive healthcare system, Healthcare stakeholders, diseases care contents (Symptoms, precautions, experts interventions etc.) and other regulatory concerns for self-care awareness and information sharing. Initially provide quality awareness. Especially to diabetic patients using their own basic smart mobile devices through a cross platform APP a light weight for users managed by open source web application dashboard, Content Management System to store and maintain patients data and finally most complex component m-Hospital accessible with affordable financial burden.

Broadly this framework will provide mechanisms to:

(i) Support the location independent seamless integration of the physical healthcare system.
(ii) A pervasive environment to allow seamless communication, association, and coordination among similar diseases the healthcare stakeholders.
(iii) Creating a close cluster or trusted group of patients to share and exchange valued information.
(iv) To promote healthcare observance, awareness for preventive measures.

(v) Easy Interface for alerts, messages and forum discussion for trusted community and digital worlds to educate, enhance the readiness for acceptance at curable stage due to ignorance or delay in diagnosis.
(vi) Electronically recording tracking, and monitoring.
(vii) Patient's health information.
(viii) Empower the development of easily accessible mobile and medical devices.
(ix) At initial phase we focus on 3A's (Awareness, Assurance and acceptance) supported by strong trusted patients network, diseases information exchange, expert's interventions in trusted and secure pervasive environment.
(x) This framework will be a post-Clinic and post-desktop model of human device interaction using medical sensor devices like invasive or noninvasive glucometer and insulin pumps using smart phone.

Same time we also investigate the key challenges and opportunities for further phases where rich contextual information will be organized to design an application architecture and development of the application system for remote monitoring with quality diagnosis, tracking of odd conditions of nomadic chronically ill patients, independent life of elderly people or other remote workers in disaster, earthquakes, mining etc. using easily accessible and affordable laser or sensor noninvasive healthcare device, hotspots connectivity in a secure cluster of pervasive healthcare environment.

5. Research Method

5.1 Objectives

Pervasive mobile environments require architecture based on "Trust rather than just user authentication and access control", to provide the promising level of security. Research objective is to provide the conceptual and analytical framework with inherent security assurance for significant adaptation of trustworthy communication to meet the next generation ICT enabled services deliveries in human-centric solutions like healthcare. Thus a conceptual and analytical framework with cross platform application integration with consistent user experiences for enhancing the acceptance is proposed here to realize our approach. Future mobile applications with trusted security based on a) Context awareness while user mobility, b) Recommendation and c) dynamic node behavior monitoring and insider attacks evaluation are the main consideration.

This research has threefold interrelated objective; first of all understanding security assurance concerns, need and challenges, second goal is to build an energy-efficient conceptual model with trust based soft security parameters in user paradigm applications and services delivery. Finally providing a trust based secure pervasive healthcare application framework for self-care awareness to remote monitoring and quality diagnosis of chronic diseases.

5.2 Research Methodology

In this research, a multi-step system analysis and evaluation method is used. We have done Primary research - literature review including academic journals, national and international scholarly papers, peer-reviewed published articles, conference proceedings-

(i) To study the awareness about diabetes and myths related to it in diabetic patients in India.

(ii) To explore the awareness of the diabetes and management of disease in diabetic patients.

(iii) To understand the behavior of individuals toward diabetes management research.

Research Instrument: Well-designed questionnaire which was designed keeping in mind the objective of the study. Data collection was done through interview method using structured interview schedule. Predominantly Quantitative research with some Qualitative aspects included. Other tools used for research and data Coding /editing Microsoft Excel, SPSS Version 20.

6. Research Outcomes

Pervasive mobile environments require architecture based on trust rather than just user authentication and access control to provide the promising level of security. A distributed end-to-end multi-tier trust based secure pervasive healthcare framework has been proposed for pervasive healthcare for Diabetes as a case study in continuation of our research work done so far. Purpose of this case study it to validate our complete system. We start if for diabetic care and first and foremost focused on disease awareness for self-care to m-hospital care using mobile sensor devices.

6.1 Impact of Proposed Research

In this research focus is on enhancing the trust management and security assurance for enhancing the acceptance of human-centric pervasive application and services to realize-

(i) How can a trusted computing realize security infrastructure for future mobile applications?

(ii) Identifying QoS and social trust parameters for proposed trust metric.

(iii) Determining the trust based soft security assurance.

(iv) Security awareness for rich and consistent user experiences to adopt future mobile applications.

(v) Trusted and secure clustering of resource restricted and energy efficient pervasive services.

(vi) Promoting human-centric solution like m-healthcare for motivating and realizing the benefits of self-care educating awareness and remote diagnosis to reduce hospital sty burdens and curing in isolated areas.

A distributed end-to-end multi-tier trust based secure pervasive healthcare framework has been proposed for pervasive medical care as a case study. Purpose of this case study it to validate our complete system. We start if for diabetic care and first and foremost focused on disease awareness for self-care to m-hospital care using mobile sensor devices.

In the proposed healthcare framework patients will use trusted information in self-care decision making with system-specific security rules based on computational trust. The trust parameters that were discussed will be the support for awareness and transparency between the group members. The monitoring components of the framework will offer the feedback dynamics for enforces mechanisms for decision making. For the discussed case study of diabetes that is actually NOT diseases of blood sugar, but rather a disorder of insulin in our body. General main stream largely deals in treating diabetes and little address on underlying causes. Through the strong content management related to diseases insulin sensitivity as key component will be communicated for avoidance and preventive approach. Later on after connecting large number of patient's case studies, it will be used for predictive risk analysis and secondary cause diseases as its ultimate goal.

7. Conclusion

Trust Management and Security assurance in open, distributed and dynamic network like pervasive environment, technologically advanced to answer the inadequacy of traditional privacy and security mechanisms. Human being like trust notation security-critical communication is the key concern for our research work. Investigation of the exiting trust and security models for addressing the challenges and appraise the opportunities in autonomous mobile pervasive ad hoc networks has been done. A Bio-inspired approach using standard clustering technique and a trust metric designed to observe the node behavior vulnerabilities and other security requirements. Existing routing protocols examined to identify security threats and insider attacks with signal-strength attenuation also evaluated in the work done so far. An energy-efficient, trusted secure clustering using trust metric also proposed for significant adaptation of trustworthy communication in human -centric mobile applications where information is ubiquitous. In winding we explore the existing pervasive healthcare application and propose a trust based secure m-healthcare framework for diabetes in India. Application prototyping and cross platform app development supported by complete integrated web based healthcare solution implementation are our further steps under ongoing research. Eventually this research will lead to provide predictive risk analysis.

Acknowledgements

We would like to express deep gratitude to Dr. R.C. Joshi Ex. Prof. E. and C.E. Department at IIT Roorkee and Chancellor at Graphic Era University Dehradun for his valuable support and guidance in exploring relevant literature and continuous improvements in the proposed research. We are also grateful Dr. Rajeev Agrawal, Director G.L. Bajaj Institute of Technology and Management, Greater Noida for providing significant insights of subjective, mathematical formulation and simulation. We are highly obliged of Dr. Amal Shankar Shukla for his unconditional support, consistent guidance and motivation.

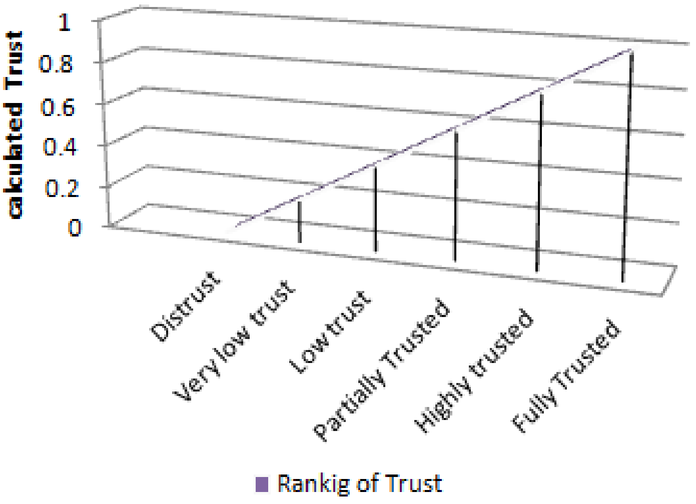

Figure 1. Computed trust ranking

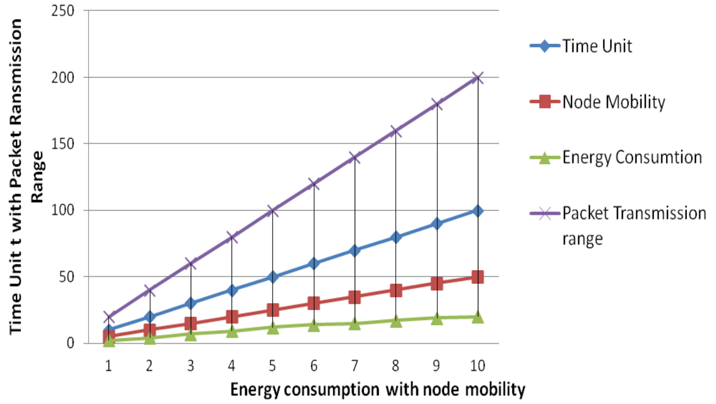

Figure 2. Lowest energy consumption

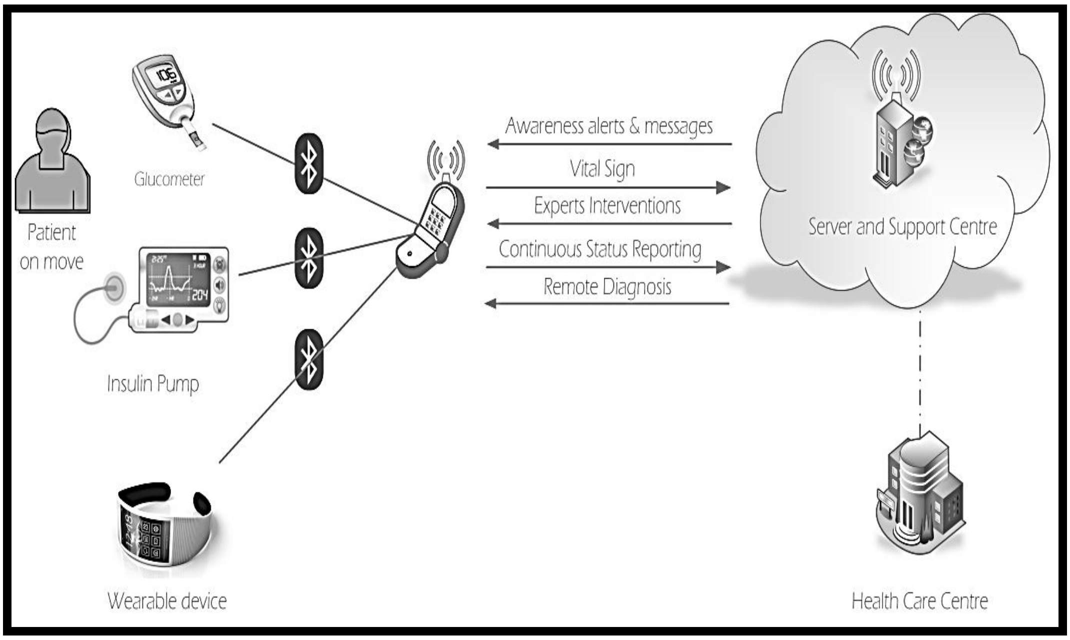

Figure 3. Human-device interaction for diabetic m-healthcare

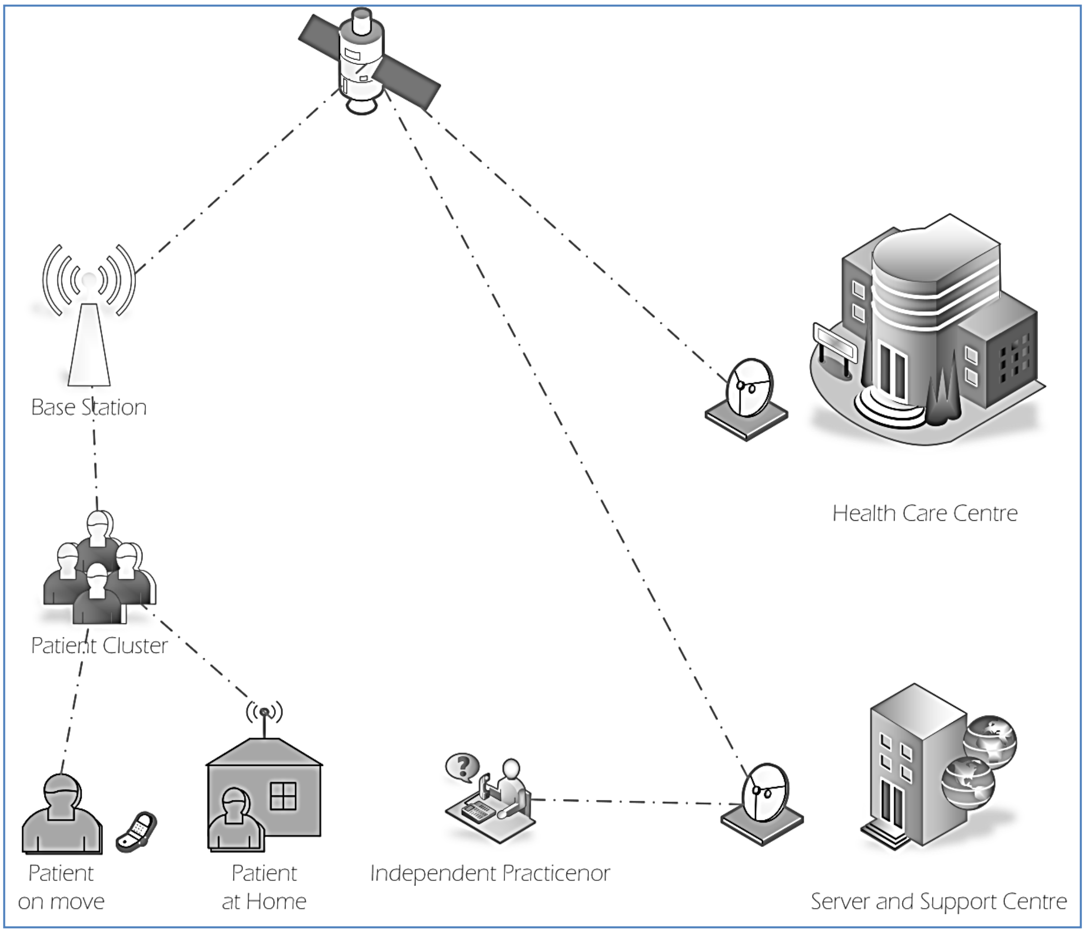

Figure 4. Pervasive healthcare application ecosystem

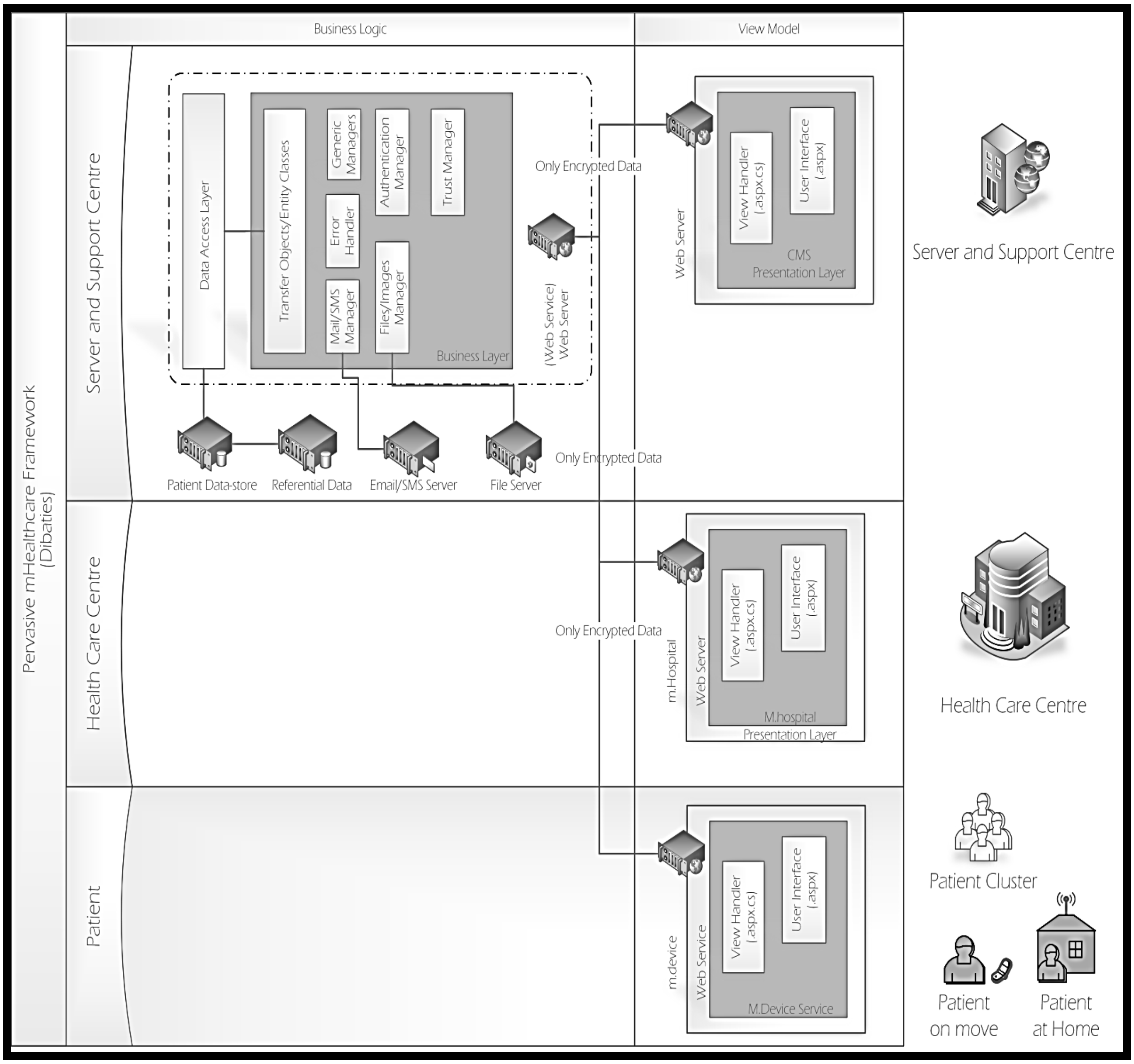

Figure 5. Conceptual framework for pervasive m-healthcare

References

Acampora, G., Cook, D. J., Rashidi, P., & Vasilakos, A. V. (2013). A survey on ambient intelligence in healthcare. Proceedings of the IEEE, 101(12), 2470-2494.

Alemdar, H., & Ersoy, C. (2010). Wireless Sensor Networks for Healthcare: A Survey”. In Proceedings of Computer Networks, 54(15), 2688–2710.

Ali, H., Shahzad, W., & Khan, F. A. (2012). Energy-efficient clustering in mobile ad-hoc networks using multi-objective particle swarm optimization. Applied Soft Computing, 12(7), 1913-1928.

Almenárez, F., Marín, A., Campo, C., & Garcia, C. (2004, August). PTM: A pervasive trust management model for dynamic open environments. In First Workshop on Pervasive Security, Privacy and Trust PSPT (Vol. 4, pp. 1-8).

Bao, F., Chen, I. R., Chang, M., & Cho, J. H. (2011). Hierarchical trust management for wireless sensor networks and its application to trust-based routing. In Proceedings of the 2011 ACM Symposium on Applied Computing, 9(2), (pp. 1732-1738). ACM.

Bao, F., Chen, R., Chang, M., & Cho, J. H. (2012). Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE Transactions on Network and Service Management, 9(2), 169-183.

Bu, S., Yu, F. R., Liu, X. P., Mason, P., & Tang, H. (2011). Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks. IEEE Transactions on Vehicular Technology, 60(3), 1025-1036.

Chang, E., Hussain, F., & Dillon, T. (2006). Trust and reputation for service-oriented environments: technologies for building business intelligence and consumer confidence. John Wiley & Sons.

Cho, J. H., Swami, A., & Chen, R. (2011). A survey on trust management for mobile ad hoc networks. IEEE Communications Surveys & Tutorials, 13(4), 562-583.

Cisco. (2010-2015). Cisco visual networking index: global mobile data traffic forecast, www.cisco.com

El-Haleem, A. M. A., & Ali, I. A. (2011). TRIUMF: Trust-based routing protocol with controlled degree of selfishness for securing MANET against packet dropping attack. International Journal of Computer Science, 8(4), 99-110.

Gaur, M. S., & Pant, B. (2014). A Bio-inspired trusted clustering for mobile pervasive environment. In Proceedings of the Third International Conference on Soft Computing for Problem Solving 259: (pp. 553-564). Springer India.

Gaur, M. S., & Pant, B. (2014). Trust metric based soft security in mobile pervasive environment. International Journal of Computer Network and Information Security, 6(10), 64-71.

Gaur, M. S., & Pant, B. (2015). Impact of signal-strength on trusted and secure clustering in mobile pervasive environment. Procedia Computer Science, 57, 178-188.

Gaur, M. S., & Pant, B. (2015). Trusted and secure clustering in mobile pervasive environment. Human-Centric Computing and Information Sciences, 5(32), 1-17.

Ghorbel, M., Khatib, M., Mhamed, A., & Mokhtari, M. (2009). Secured and trusted service provision in pervasive environment. In 2009 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, (pp. 400-405), IEEE.

Hsieh, M. Y., Huang, Y. M., & Chao, H. C. (2007). Adaptive security design with malicious node detection in cluster-based sensor networks. Computer Communications, 30(11), 2385-2400.

I. D. F. (2013), International Diabeted Federation Diabetes Atlas, 6th edition.

International diabetes federation, (2014). Key findings update, IDF diabetes Atlas. 6/e.

Liang, X., Li, X., Barua, M., Chen, L., Lu, R., Shen, X., & Luo, H. (2012). Enable pervasive healthcare through continuous remote health monitoring. IEEE Wireless Communications, 19(6), 10-18.

Liu, J., Yu, F. R., Lung, C. H., & Tang, H. (2009). Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks. IEEE Transactions on Wireless Communications, 8(2), 806-815.

Nwin, N., Whiting, D., Gariguata, L., Ghyoot, G., & Ganeds, D. (2011). Diabetes atlas, international diabetes federation, Brussels, Belgium, 5/e.

Sridhar, V., & Hämmäinen, H. (2011). Mobile Internet: Indian telecom leading the way, DataQuest.

T. C. G. (2010). TCG MPWG mobile trusted module specification, version 1.0, Revision 7.02 29.

T. C. G. (2009). Mobile Phone Work Group, Selected use case analyses-v 1.0.

Velloso, P. B., Laufer, R. P., Cunha, D. D. O., Duarte, O. C. M., & Pujolle, G. (2010). Trust management in mobile ad hoc networks using a scalable maturity-based model. IEEE Transactions on Network and Service Management, 7(3), 172-185.

Weiser, M. (1991). The computer for the 21st century-scientific American special issue on communications. Computers, and Networks (September 1991), 94-104.

Yang, H., Luo, H., Ye, F., Lu, S., & Zhang, L. (2004). Security in mobile ad hoc networks: challenges and solutions. IEEE Wireless Communications, 11(1), 38-47.

Zhang, K., Wang, C., & Wang, C. (2008). A secure routing protocol for cluster-based wireless sensor networks using group key management. In 2008 4th International Conference on Wireless Communications, Networking and Mobile Computing, (pp. 1-5), IEEE.