Biomedical Research 2017; 28 (8): 3456-3464 *ISSN 0970-938X*
www.biomedres.info

An energy aware end-to-end trust mechanism for IoT healthcare applications.

Praveen Kumar Reddy M*, M Rajasekhara Babu

School of Computing Science and Engineering, VIT University, Vellore, Tamil Nadu, India

Abstract

The current number of patients are increasing day by day in various countries. Present advances in computing technology and the Internet of Things (IoT) have provided economical and low cost equipment's like cameras, embedded devices, smartphones. Embedded computing empowers the deployment of Smart Health care applications that can improve medical treatment effectively. Most of existing Health Monitoring systems are vulnerable to environmental and operational damages. These existing systems are not guaranteed end to end trust for patient health data. Most of existing methods energy performance are very poor in terms of communication latency and communication overhead. We propose an energy aware end-to-end trust mechanism for IoT healthcare applications. We discuss how to provide end to end trust for IoT health applications and how to improve the efficiency of health care applications. The results of the evaluation determine the effectiveness of proposed method. When compared to existing method our proposed technique reduces 24% communication overhead and 18% latency between end user and gateways and provides end to end trust for medical data transferring from on medical sensor node to another.

Keywords: Energy, end to end trust, IoT, health care, latency, communication overhead.

Accepted on December 21, 2016

Introduction

Latest advances in computer technology have rise to another innovation: Internet of Things (IoT) [1-3]. The Internet of Things (IoT) gives availability to anybody at any place and any time. With the progress in innovation, there is a tremendous change in the society where everybody and everything will be allied [4]. The IoT is believed as the future assessment of the Internet that acknowledges machine-to-machine (M2M) learning [5]. The fundamental thought of IoT is to provide independent and secure connection and trade of information between applications and devices [6]. By the year 2020 it is estimated that 20 to 30 billion devices will be connected to the internet. IoT has emerged in various fields like smart cities, smart heath, smart homes. Increasing the number of sick people have grabbed a global attention towards their health. Due to increase in health care cost most of people are afraid and not able to afford that much huge cost. These scenarios have a made a way into the technology. Systems can be made out to monitor the patients and alert the nurse or concerned at the emergency situations. Smart Health Care (SHC) cares about the user's health. SHC comes with a collection of information systems, telemedicine and home automation products. It can be defined as a Smart Home that is furnished with particular gadgets for personal health care. These gadgets are primarily sensors and actuators that can make a move at whatever point a basic circumstance is distinguished [7,8]. This has been oppressed in a few works, where the researchers give out technological answers for the caretakers to monitor the needy.

The main theme is to provide patients who are suffering from sickness, some autonomy with the goal that they can experience their lives in a more independent way, cheap and best way. Security plays a major role in large scale networks. SHC gathers human related information from different sensors [9,10]. Such information is to be maintained with high privacy. In SHC applications privacy and security plays a major role as most of the devices will be communicated in wireless mode [11]. The Medical Sensor Network provides different IP-enabled sensor nodes, which can transfer health information about patients to remote healthcare sever. This confidential health information of patients has been routed through an unsecured network there will be loss of data, inconsistency, stealing of information will occur. If this happens, people may restrict use SHC. In this regard providing end to end security, privacy and trust for patient's confidential data is a major concern in SHC system. Due to advanced architectures of IoT based SHC systems, resource limits and security level essentials conventional secure protocols, protection schemes and security mechanisms cannot be reused [12]. Different researchers have proposed several innovate solutions for guaranteeing security in wireless sensor networks that are not directly suitable for IoT based SHC systems due to following disputes [13]:

1. Medical Sensor devices are having very low power storage, memory, bandwidth and latency.
2. Medical Sensor devices are very small they can be lost very easily.

The rest of the paper is organized as follows. The literature survey about IoT health care applications is explained in section 2. In section 3 we had presented a novel IoT Health Care Architecture. We presented Energy Aware End to End Trust Mechanism which is considered in section 4. Implementation and Experimental Analysis are presented in section 5. Finally, we concluded our work in Section-6.

Literature Survey

The Harvard sensor network lab had developed CodeBlue a popular research, health care project [14]. CodeBlue, a remote framework planned for deployment in crisis medicinal care, incorporating low-power, remote key sign sensors, PDAs, and PC-class frameworks. CodeBlue will boost first responder's ability to assess patients on scene, guarantee consistent exchange of information among caregivers, and encourage effective allotment of hospital resources. This framework supports reliable data transfer and provides a decentralized security model. In CodeBlue project Lorincz et al. [15] has suggested TinySec and Elliptic Curve Cryptography (ECC) for symmetric encryption and key generation. Kambourakis et al. [16] has explained some security models like snooping attack, Sybil attack, denial of service attack, related to CodeBlue project. Johns Hopkins University has developed MEDiSN system which aims at in-hospital patient monitoring [17].

In this method, the authors have proposed the encryption model for physiological screening, but the authors didn't specify which cryptosystems have been utilized for integrity and data confidentiality. Their study didn't cover abundant information concern for security. In [18] authors have proposed Sensor Network for Assessment of Patients (SNAP) which provides security for wireless monitoring systems. The main drawback of this model is it will not provide security for user's while providing medical information. Besides, the information gathered from medical sensors is passed on to a controller in plaintext design. Subsequently, the medical information of the patients can be altered by a malicious user. IBE-Lite technique is presented in [19] where efficiency problems, security and privacy issues are perceived. There are some security issues with this methodology like end-user/sensor to base station authentication is not considered. In this manner, distorted therapeutic data can be introduced due to absence of authentication and verification schemes.

In a study by Modadugu et al. [20] the authors have proposed Datagram Transport Layer Security (DTLS) to establish an end to end security. The DTLS protocol gives interchanges security for datagram protocols. The protocol permits client/server applications to impart in a way that is intended to avert tampering, message forgery, eavesdropping. The DTLS protocol works on Transport Layer Security (TLS) protocol and ensures security. The datagram semantics of the hidden transport are safeguarded by the DTLS protocol. Hummen et al. [21] authors have proposed Delegation-based Authorization and Authentication model for IoT. The proposed delegation model lacks in reliability and salacity since it depends on a unified delegation server. Their architecture suffers from an overhead problem and latency issues apart from that their architecture cannot be used for hospital domains. In addition, if a foe plays out a Denial of Service (DoS) attacks a substantial amount of stored security data can be repossessed. The delegation model actually gives authentication when utilizing the focal part of the designated server at the beginning stage of connection establishment. Muller et al. [22] proposed a platform for sensor network applications that provides a gateway for sensor networks and multi-tier architectures. The proposed platform is suitable for small scale and home applications.

Shen et al. [23] proposed a prototype 6LoWPAN for eHealthCare Wireless Sensor Networks. The proposed prototype makes the decisions of patient's health sates using Hidden Markov Model. In [24] the authors have proposed a wireless architecture for Personal Area Network (WPAN) which concentrates on providing security and ensures safety for users by using monitoring techniques. The framework depends on image processing and can give arrangements that are coordinated with other control gadgets. In this situation, a sensor in view of image processing has a blend of filters, casing rate examinations and different calculations that demonstration astutely in nature. This empowers the discovery of developments and examples of the exercises of an inhabitant, for example, speed and direction. It ought to be noted, however, that no endeavor is made to investigate the emotional condition of the occupants keeping in mind the end goal to evaluate the condition of their health. In [25] the author has proposed health care solution using mobile devices by combining IPV6 techniques with mobile devices in a wireless network to monitor continuous health condition of patients and furnish numerous efficient healthcare services. The wireless sensor network devices collect photoplethysmogram (PPG) signals and transfer the signals to server through internet. The information gathered from the server will be sent to android mobile device to the patient and doctor.

Zhan-feng et al. [26] has proposed sensor based Structure Health Monitoring system where they expected to do analog to digital conversion, analog signal conditioning and send the information to a base station for further investigation. However, this system is costly and cumbersome. Rahmani et al. [27] has developed a framework UT-GATE for smart e-health applications. In this work the authors have designed the gateways in an intelligent manner for processing the information, storing the data and to make the decisions at the edge of the network. The smart gate can quickly provide preparatory results and decrease the redundant communication to cloud by using data aggregation methods, machine learning techniques. Other studies have proposed a secure IoT health model. In this work, they are going to provide end to end trust model using smart gateways. This model is not suitable mobile applications [28,29].

Valenzuela et al. [30] propose a model which supports mobility for heath monitoring systems. This approach uses a facilitator sensor appended to the patient's body that takes the responsibility for communicating between sensor nodes and access points. Fotouhi et al. [31] proposed mobility solution in Wireless Sensor Networks (WSNs) which can be effectively employed for Body Sensor Systems (BSNs). In their work authors, have used various parameters like sensor velocity, Received Signal Strength (RSS) to specify handover time. This arrangement requires a constant trade of acknowledging messages between access point and sensor node to check network link. Due to the continuous exchange of messages leads more energy consumption, memory and transmission overhead.

IoT Health Care Architecture

IoT Health care applications are built to serve the people, which innately raise the necessities of reliability, security and safety. Moreover, the applications have to provide notifications and responses with respect to the status of patients. A health care management system has to ascertain the safety of patients by observing patients' activities and key signs. A health care management system should offer precise results in a timely fashion and should provide secure and reliable services for caregivers, physicians and patients. To ensure these necessities the framework requires reliable communication and less latency. Existing cloud based techniques can't guarantee the prerequisites of health care applications since there is a lack of integrity and confidentiality for the customer data which is present in the cloud. Due to the high utilization of cloud there is a problem in latency for applications, which require the maximum number of nodes to reduce delay. Mobility, geographic diversity and low latency are the important features required for IoT Health care applications. Cloud computing today is facing many challenges to satisfy the requirements of IoT devices. Therefore, to meet all these requirements a new platform is needed. Fog computing is a new platform which delivers services and web applications at the edge of the network. Fog services can be utilized in various applications and devices like smart mobiles, access points, edge routers by providing processing and storage services to end users. Figure 1 shows the architecture of IoT health care on which we apply energy aware end to end the trust derivation scheme. The responsibility of each layer in architecture is as follows.

Device layer: The bottom layer comprising of numerous physical gadgets like medical sensor devices that integrated into a wireless module to gather medical information. Sensor devices are enabled based on sensing, patient identification, signals are captured from body or room. The captured signals are used in treating with the treatment and determination of medical conditions. These signals are broadcasted to Fog layer via wired or wireless protocols.

Fog layer: The term Fog computing has been introduced by Cisco systems to overcome the drawbacks of Cloud computing. Fog computing is the extension of cloud computing, where fog computing provides services to users at the edge of the network [32]. Fog computing architecture is a virtualized platform which provides storage, computation and networking services between cloud data centers and end devices. Fog computing provides the services like storage, networking and computing similar to cloud computing apart from these services, fog is the extension of cloud by providing the services to the edge of the network. Edge of the network is the main important characteristic of fog which the extension of cloud. Today IoT is an emerging technology, every device is provided with sensing capabilities, monitoring and provide unique information. In recent years IoT is being used in many applications like smart city, smart hospitality, smart vehicles. In year 2015 the demand of IoT in IT industry will increase to14% and will reach to $3 trillion IoT devices by 2020 [33]. The key requirements of IoT are High reliability, Minimum latency, Power constrained and Highly distributed nodes [34]. To achieve key requirements in a better way existing networking technology has to be modified. IoT generates huge volume, velocity and variety of data the present Cloud computing paradigms are not feasible to maintain these of data, hardly support low latency, location awareness and mobility. Therefore, to meet all these requirements a new platform is needed. Fog computing, guarantees low latency, improves quality of services, location awareness since it has implemented at the edge of the network and utilizing all the resources that are accessible at the edge. Fog computing provides various advantages like improving the performance of the system in saving power, bandwidth, speed, decreases the cost and provides better QoS.

Cloud layer: The cloud layer includes data warehousing, broadcasting, big data analysis servers, which periodically executes data synchronization with the healthcare database server in the cloud. Patients data is classified into public data and private data public data can be accessible by patient such as blood group, patient ID, hospital number. Private data contains confidential information which cannot be accessed by patient like DNA etc.

Proposed Energy Aware End to End Trust Mechanism

In order to establish end to end security between medical sensor devices and end user, the end-client needs to start the session resumption with the sensor by transmitting a ClientHi message. The ClientHi message contains a session resumption expansion keeping up the session ticket and an arbitrary value A*. During this method, the medical sensor utilizes the accepted encrypted and authoritative session update by the smart gateway in order to restart the DTLS association which has previously been accomplished between the end-user and the smart gateway.

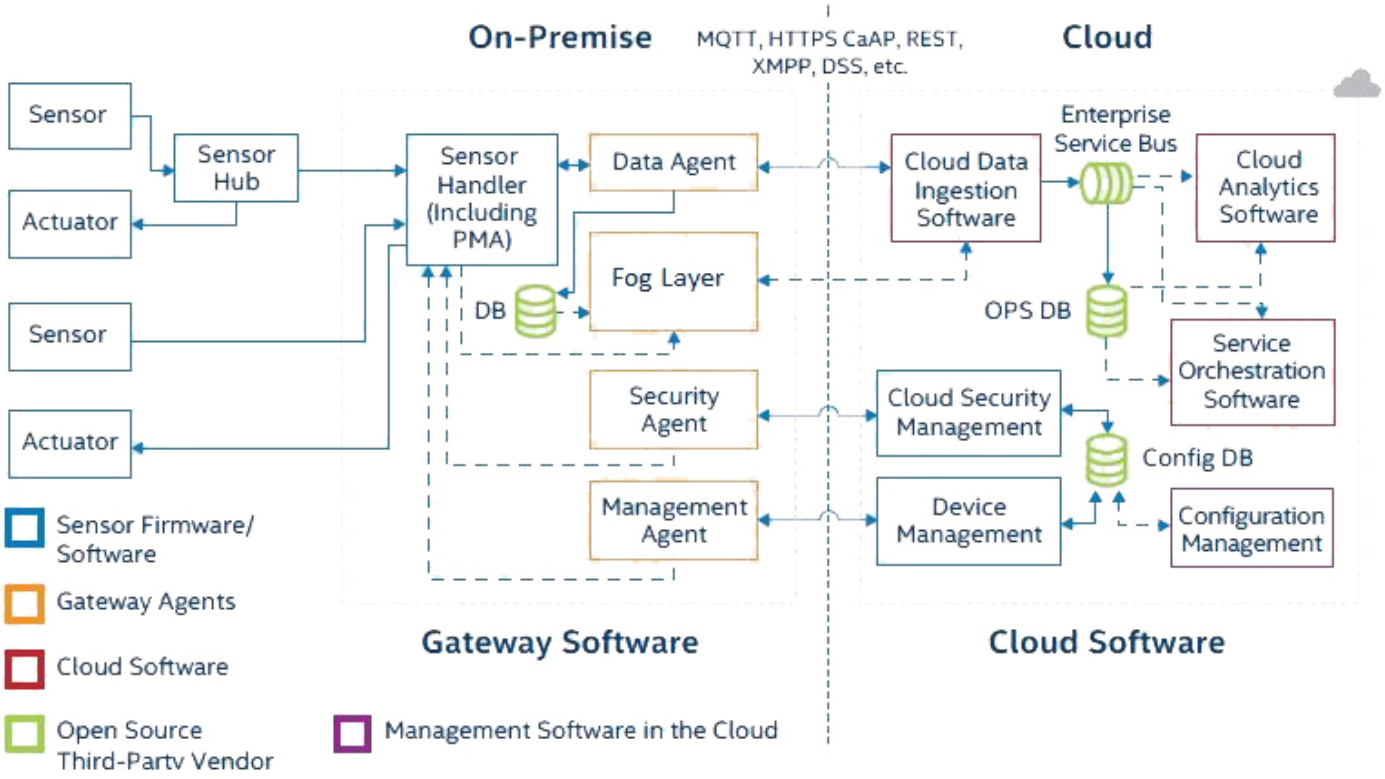

Figure 1. *The architecture of IoT healthcare system with energy aware end to end trust derivation scheme.*

Software Components of IoT system are described in Table 1.

Table 1. *Description of software components.*

Device Type	Responsibility	Software Type	Interface
Sensor	Collects health data from patients	Firmware and Hardware for Intelligent devices	Connects to sensor or gateway via wireless (e.g., ZigBee, BTLE, USB)
Sensor Hub	Aggregates data by connecting to actuators and sensors	Firmware and Hardware	Connects to sensor or gateway via wireless (e.g., ZigBee, BTLE, USB)
Actuator	Make actuation	Firmware and Hardware	Connects to sensor or gateway via wireless (e.g., ZigBee, BTLE, USB)
Sensor Handler	Interacts with sensors with help of API libraries (e.g., Mapping layer or Protocol Abstraction)	Middleware	Imparts sensor libraries through API calls
Security Agent	Provides security for sensors, actuators	Middleware and Software	Imparts with Cloud Security Management
Data Agent	Collects and formats information from sensors	Software	Imparts with sensor handler and cloud
Management Agent	Provides alerting, error handling for sensors and gateways	Middleware and Software	Imparts with device management in cloud
FOG Layer	Provides services at the edge of network	Software	Acts as gateway to reduce latency and overload
Cloud	Provide different services to end users	Service	Imparts with data agent and fog layer

The protocol for the DTLS session recommencement without server-side state applied in this process is demonstrated in Figure 1. Upon getting the session ticket extension, the medical sensor which behaves as a server requires to decrypt and affirm the rightness of the ticket utilizing the corresponding key which is the pre-master secret. As the session ticket is entirely affirmed, the sensor reacts with a Server Hello message accommodating a vacate session resumption extension and an ergodic value A". In the equal flight, the sensor also egresses a fresh session ticket, which encompasses the data of the present state that is the present master secret. The present master secret is calculated by Pseudo Random Function (PRF), that is, a

HMAC-based secret expansion function, across the former master secret key (pre-master secret) and the changed random values A* and A'', respectively. The ergodic values furnish forward secrecy meaning that revelation of the latest single key just allows for accessing to the data of that session and does not endanger the security of the former DTLS sessions. The fresh session ticket is carried through the new session ticket content and held by the end-user for a conceivable consequent session recommencement. This way the resource-constrained sensor offloads the computational and auctioning essence of its state towards the non-resource-constrained end-user. Afterward, by changing the Change Cipher Spec messages, the fresh keying material is employed in order to assure the communication distribution channel. At last, by changing the finished messages the rightness of the consorted keys and the integrity of all changed messages are affirmed. This resolves the handshake and allows the exchange of assuring application information.

In this process, to render the Session Ticket, the altered edition of recommended ticket construction advised in [35] is applied. This is because the recommended ticket construction directs to an excessive ticket size for resource-constrained network environments. Hence, it is essential to render an altered version of the recommended ticket construction that will accept the constraints of the device/network into account with reference to the transmission overheads. The new session ticket message includes a lifespan value and a session ticket. The lifespan value presents the number of seconds till the session ticket dies. The structure of the session ticket is frosted to the communing peers and only the ticket issuer could access the session ticket data. The suggested ticket structure in [35] advises to use AES-CCM for encryption with a 32-byte MAC and 12-byte Initialization Vector (IV)based on HMAC-SHA-256. Yet, in this process, an 8-byte MAC based on a 12-byte IV and HMAC-SHA-256 are applied, as they are the suggested cipher suites for secure CoAP over DTLS [36]. We employed our proposed session resumption-based end to-end trust scheme for IoT healthcare. The end-to-end trust is accomplished by (i) applying the full initial certificate-based DTLS between end-users and smart gateways and (ii) applying session resumption method which enables end-users and sensors to communicate the encrypted health-related data. The full operation substantially assuages the processing load on tiny sensors in terms of authorization, authentication, public key cryptography functions, certificate related operations.

Energy aware trust derivation for IoT health care

In IoT trust valuation plays a critical role. The proficiency of the trust, valuation process is controlled by trust derivation, as it regulates the performance of network and communication overhead due to limited power and bandwidth. In this paper, we have proposed Energy Aware Trust Derivation for IoT Health Care which provides end to end to security from IoT application.

Algorithm 1: Trust Derivation Algorithm

1: Process Initialization

2: **if** Node 'a' is ready

3: Broadcast Trust request to all nodes

4: **end if**

5: if Trust request is received

6: if Duplicate request is received

7: reject trust request

8: **return**

9: **else**

10: **if** Hop limit ≥ 0

11: Hop limit = Hop Limit -1

12: Broadcast Trust request again

13: **end if**

14: **if** Node 'b' belongs to neighbor set

15: forward trust replay with 'P' probability

16: discard trust request

17: **return**

18: **else**

19: reject trust request

20: **return**

21: **end if**

22: **end if**

23: **end if**

24: End

Analysis of trust derivation approach

Table 2. *Notations for trust derivation.*

Symbol	Meaning
G	Utility
P	Probability of forwarding trust reply
fs(e)	Cost of an arbitrary node for forwarding trust reply
X	No of Participating nodes
n	No of Optimal recommendations

In this method, we had assumed that an arbitrary node 'a' forwards trust reply with 'P' probability or remains idle with 1-P probability. For 'X' nodes at least one of node may reply trust request with $1-(1-P)^X$ probability (Table 2). As a result, Nash equilibrium can be calculated by

$$G(1-(1-P)^{X-1}) = G - f_s(e) \rightarrow (1)$$

Thus, the probability of forwarding trust reply can be denoted as

$$P = 1 - \left(\frac{f_s(e)}{G}\right)^{\frac{1}{X-1}} \rightarrow (2)$$

Setting Q=1-P and applying logarithm on both sides of (2), the following expression is obtained

$$\ln(G/f_s(e)) = (1-X)\ln Q \rightarrow (2)$$

Probability of choosing reply request by n nodes can be given as $C_X^n P^n (1-P)^{X-n}$. Thus, Nash equilibrium can be computed by

$$G\sum_{\beta=n}^{X-1} C_{X-1}^{\beta} P^{\beta}(1-P)^{X-\beta-1} = -f_s(e) \sum_{\alpha=0}^{n-2} C_{X-1}^{\alpha} P^{\alpha}(1-P)^{X-\alpha-1} + (G - f_s(e)) \left\{ C_{X-1}^{n-1} P^{n-1}(1-P)^{X-n} + \sum_{\beta=n}^{X-1} C_{X-1}^{\beta} P^{\beta}(1-P)^{X-\beta-1} \right\} \rightarrow (3)$$

The following expression can be obtained from above equation.

$$C_{X-1}^{n-1} P^{n-1}(1-P)^{X-n} = \frac{f_s(e)}{G} \rightarrow (4)$$

If we represent $U(P) = C_{X-1}^{n-1} P^{n-1}(1-P)^{X-n}$, the derivation of U(P) can be represented as follows $\frac{\delta U(P)}{\delta P} = C_{X-1}^{n-2} P^{n-2}(1-P)^{X-n-1}(n-1+P) \rightarrow (6)$

If we sent the derivative to zero, we find that U(P) function is increasing when P value is less than n-1/N-1. $f_s(e)/G$ is a deceasing function with G value. The larger value of G provides the participating nodes to deliver trust reply associated with the cost. All the participating nodes will deliver trust reply with P probability which ought to likewise consider the trade-off between security and energy efficiency algorithm 1 explains the pseudocode of providing the trust derivation for the network and the performance of the network like energy consumption, packet delivery ratio, time are calculated by computing $G/f_s(e)$. The simulation results and performance evaluation are explained in experimental analysis (Figure 2).

Implementation and Experimental Analysis

The architecture of the system shown in Figure 1 is constructed with the purpose of experimental evaluation, the end goal of which being secure and efficient authorization, authentication and also for making the proposed end-to-end trust scheme. To execute the suggested architecture, we make a layout that consists of UT-GATE smart e-health gateways, medical sensors, a remote server. UT-GATE is assembled using a Pandaboard [38] and a Texas Instruments (TI) SmartRF06 board that is integrated with a CC2538 module [39]. The Pandaboard is a low-cost, low-power single-board computer development platform that works on the TI OMAP4430 system-on-chip (SoC) that follows the OMAP architecture which is manufactured using 45 nm technology. The OMAP4430 processor is constructed with Cortex-A9 microprocessor unit (MPU) subsystem with dual-core ARM cores with symmetric multiprocessing at up to 1.2 Giga Hertz (GHz) each. UT-GATE is installed in Ubuntu OS which allows to control devices and services such as notification and local storage and uses 8 GB of external memory.

In order to find out the feasibility of our architecture, the network simulation tool, Cooja by Contiki, uses the Wismote [40] platform that is a common resource-limited sensor. Wismote is configured with a 16 MHz MSP430 micro-controller, 16 kB of RAM, 128 kB of ROM, an IEEE 802.15.4 radio transceiver, and supports 20-bit addressing too. For evaluating, we use OpenSSL version 1.0.1.j, which is an open source tool that is used here to create elliptic curve public and private keys from the NIST P-256 (prime256v1) and X.509 certificated. X.509 certificates are the superior form of certificates and are used in the certificate-based module of DTLS [41]. OpenSSL API is used for server association to end user which provides all essential operations associated to end-user like certificate, configuration, session state, handshake and cipher. Tiny DTLS [37] is an open-source execution of DTLS in symmetric key-based mode. We widen it with abide for the certificate-based DTLS as well as session resumption. Relic-toolkit [38] is an open source cryptography library which is used for public key functions. We have used MySQL database for non-static and static records. Non-static record stores bio-signals which are synchronized between cloud server database and Pandaboard database. Static records, which are carried off by system admin which include crucial information required by the DTLS handshake. xSQL Lite tool is used processing cloud server database.

Energy performance analysis

In this section, we are going to analyze the performance of proposed technique in terms of energy.

Transmission overhead: Transmission overhead is defined as the number of bits, communicated for a message, that do not represent the data bits of the message. Table 3 compares transmission overhead of our proposed technique with [21]. Simulation results have been done using Cooja. To measure the transmission overhead the pcap tool is employed with Cooja simulator. In [21] transmission overhead is 1609 bytes which results in 24 fragments for transmitting messages from the server to the end user. Our proposed technique requires 1180 bytes which results 18 fragments for transmitting messages. Thus, the transmission overhead of our proposed technique is diminished by 24% compared to [21].

Latency: Latency is defined as the time required for packet to move from one point to another. Latency plays a crucial role in real time applications. In our work, we have calculated latency in terms of communication latency and data handover latency. Communication latency deals from gateway to end user for authorization and authentication. Data latency deals two gateways for mobility enabled end to end trust scheme. The

data handover latency and communication latency are projected on 20 Mb/s internet connection.

Table 3. *Comparing the performance results with Hummen et al. [21].*

Method	Transmission - Overhead (Bytes)	Latency-GE (Seconds)	Latency-EG (Seconds)
Proposed Work	1180	4.998	~15
Hummen et al. [21]	1609	5.99	~15
	24	18	0

Table 4. *Data handover latency between two different gateways with various packet sizes.*

Packet Size (Bytes)	Data handover latency (Milliseconds)
5	2.178
10	2.278
30	2.395
50	2.589
100	2.845
200	3.104
250	3.206
500	3.356
1KB	3.701
5KB	4.602

Communication latency: To estimate the communication latency, the interval that is spent from the end-user (EN) to sensor node is calculated. The processing time can be calculated by summing of communication latency from sensor node to the gateway (EG) and gateway to end user LatencyEN = LatencyEG+ LatencyGE. In this paper, to calculate the communication latency of the UT-Gate to the end-user, a proxy server is abutted to the network. By the proxy server, the transmittal latency between the end-user and the UT-Gate may be well calculated as the proxy server minds to requests broadcast from the end user to the UT-Gate and vice versa without fiddling or changing them. To calculate the communication latency of GE, the Fiddle proxy server, which is a desktop application program, is applied to get over requests and replies. Fiddle whirls a heavy number of services including HTTP/HTTPS and security testing traffic recoding. According to our psychoanalysis, the proposed architecture accomplishes most equal EG serving time to the existing [21]. However, the proposed model substantially reduces the serving time wanted for EG compared to existing models. As shown in Table 1, in our approach, the serving time took for EG is about 4.988 s, whereas this time gains to about 5.99 s in [21] architecture. Thus, considering the latency from the gateway to the end-user, the proposed model gets around 18% betterment compared to the [21] architecture.

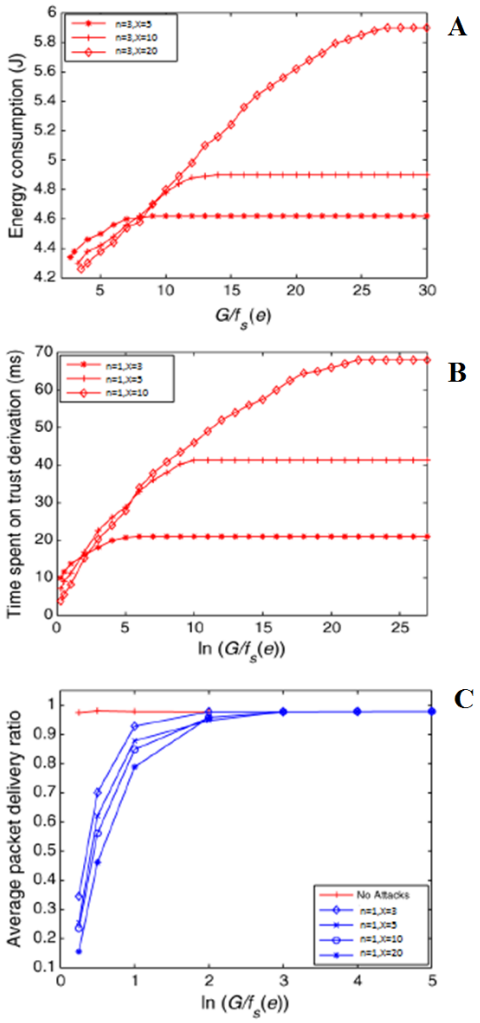

Figure 2. *Effect of $G/f_s(e)$ performance on network when (n=1). (a) Energy consumption. (b) Time spent on trust derivation. (c) Packet delivery ratio.*

Data handover latency: To manifest how our proposed end to-end Trust mechanism enables mobility, we went through a real-time system in which 2 UT-GATE gateways with the configuration accounted above. We presume that these gateways are associated through the fog bed where one of the gateways behaves as a client and the other one plays as a server. In the experimentations, we made a 100-bytelookup board for each gateway that comprises of: (i) control data which consists of the DTLS session resumption posit, data about the authorized health care provider, medical sensors, patients' IDs and ID's (ii) Patients' health information which includes body temperature, heart rate, and oxygen saturation. In our Psychoanalysis, we premeditated the latency of the data handover process between the gateways. To demo the scalability of our work, we conceived contents with several sizes which could need to be changed between the gateways for the information handover process. As could be derived from the Table 4, the data handover latency between 2 gateways is worthless and mobility is abided in an intelligent way with no computational and processing effect to the sensing element. In summation, by raising the packet size, latency

marginally increases displaying the scalability of our approach. As adverted before, seamless mobility is an essential in healthcare IoT systems. The experimentations demo that our proposed end-to-end trust mechanism also provides accompaniment for this feature. It ought to be noticed that projecting a novel mobility approach is extraneous to the proposed idea. It implies that any fog-based mobility solution can be aggregated with our trust scheme.

Conclusion

This paper proposes an efficient energy aware end to trust mechanism for IoT healthcare system. Based on existing survey our proposed technique provides better security features. Our system architecture consists of three-layer device layer, fog layer, and the cloud layer. The seamless mobility for medical sensors and the alleviation of sensors, processing loads were a result of the distribution nature of smart gateways in the fog layer. We have proposed how to provide end to end trust for IoT health applications and how to improve the efficiency of health care applications. The results of the evaluation determine the effectiveness of proposed method. The proposed technique reduces 24% communication overhead and 18% latency between end user and gateways and provides end to end trust for medical data transferring from on medical sensor node to another.

References

1. European Commission Information Society. Internet of Things Strategic Research Roadmap, 2009.
2. Xu LD, He W, Li S. Internet of things in industries: A survey. IEEE Trans Ind Inf 2014; 10: 2233-2243.
3. Li S, Xu LD, Zhao S. The Internet of things: A survey. Inf Syst Front 2015; 17: 243-259.
4. Zheng J, Simplot-Ryl D, Bisdikian C, Mouftah H. The Internet of Things. IEEE Commun Magazine 2011; 49: 30-31.
5. Huang Y, Li G. Descriptive Models for Internet of Things. IEEE Int Conf Intel Control Informat Process, 2010.
6. Fan T, Chen Y. A Scheme of Data Management in the Internet of Things. IEEE Int Conf Network Infrastructure Digital Content, 2010.
7. Rialle V, Duchene F, Noury N, Bajolle L, Demongeot J. Health “Smart”home: information technology for patients at home. Telemed J e-Health 2002; 8: 395-409.
8. Stankovic JA, Cao Q, Doan T, Fang L, He Z, Kiran R, Lin S, Son S, Stoleru R, Wood A. Wireless sensor networks for in-home healthcare: potential and chal- lenges, in: High Confidence Medical Device Software and Systems Workshop (HCMDSS), 2005.
9. Yang G, Xie L, Mantysalo M, Zhou X, Pang Z, Xu LD, Kao-Walter S, Chen Q, Zheng L. A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box. IEEE Trans Ind Inf 2014; 10: 2180-2191.
10. Yan H, Xu LD, Bi Z, Pang Z, Zhang J, Chen Y. An Emerging Technology-Wearable wireless sensor networks with applications in human health condition monitoring. J Manage Anal 2015; 2: 121-137.
11. Malasri K, Wang L. Addressing security in medical sensor networks, in: Proceedings of the 1st International Workshop on Systems and Networking Support for Healthcare and Assisted Living Environments, 2007.
12. Hung X, Khalid M, Sankar R, Lee S. An efficient mutual authentication and access control scheme for WSN in healthcare. J Netw 2011; 6: 355-364.
13. Chakravorty R. MobiCare: A programmable service architecture for mobile medical care, in: Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops, 2006.
14. Malan D, Fulford-Jones T, Welsh M, Moulton S. CodeBlue: An Ad hoc sensor network infrastructure for emergency medical care, in: Wearable and Implantable Body Sensor Networks, 2004.
15. Lorincz K, Malan D, Fulford-Jones T, Nawoj A, Clavel A, Shnayder V, Mainland G, Welsh M, Moulton S. Sensor networks for emergency response: Challenges and opportunities. IEEE Pervasive Comput 2044; 3: 16-23.
16. Kambourakis G, Klaoudatou E, Gritzalis S. Securing medical sensor environments: The codeblue framework case, in: The Second International Conference on Availability, Reliability and Security, 2007.
17. Ko J, Lim J, Chen Y, Musvaloiu R, Terzis A, Masson G, Gao T, Destler W, Selavo L, Dutton R. MEDiSN: Medical emergency detection in sensor networks. ACM Trans Embedded Comput Syst 2010; 11: 1-11.
18. Malasri K, Wang L. Addressing security in medical sensor networks, in: Proceedings of the 1st International Workshop on Systems and Networking Support for Healthcare and Assisted Living Environments, 2007.
19. Tan C, Wang H, Zhong S, Li Q. IBE-Lite: A lightweight identity-based cryptography for body sensor networks. IEEE Trans Inf Technol Biomed 2009; 13: 926-932.
20. Modadugu N, Rescorla E. Datagram Transport Layer Security (DTLS) Version 1.2, in: RFC 5238, 2012.
21. Hummen R, Shafagh H, Raza S, Voig T, Wehrle K. Delegation-based authentication and authorization for IP-based Internet of things, in: 11th IEEE International Conference on Sensing, Communication, and Networking 2014.
22. Mueller R, Rellermeyer JS, Duller M. Demo: A Generic Platform for Sensor Network Applications. IEEE Int Conf Mobile Adhoc Sensor Systems, 2007.
23. Romero E, Araujo A, Moya JM, de Goyeneche JM, Vallejo JC, Malagon P, Villanueva D, Fraga D. Image processing based services for ambient assistant scenarios, in: Distributed Computing, Artificial Intelligence, Bioinformatics, Soft Computing, and Ambient Assisted Living. Lecture Notes in Computer Science, 5518, Springer, Berlin, Heidelberg, 2009.

24. Jung SJ, Myllyla R, Wan-Young C. Wireless machine-to-machine healthcare solution using android mobile devices in global networks. IEEE Sensors J 2013; 13: 1419-1424.
25. Jung SJ, Myllyla R, Chung WY. Wireless machine-to-machine healthcare solution using android mobile devices in global networks. IEEE Sensors J 2013; 13: 1419-1424.
26. Zhan-feng G, Yan-liang D, Mu-biao S, Biaoping C. Network Sensor and Its Application in Structure Health Monitoring System. Int Conf Innovat Comput Informa Control, Beijing, China, 2006.
27. Rahmani AM, Thanigaivelan NK, Gia TN, Granados J, Negash B, Liljeberg P, Tenhunen H. Smart e-health gateway: Bringing intelligence to IoT-based ubiquitous healthcare systems. 12th Annual IEEE Consumer Commun Networking Conference 2015.
28. Moosavi SR, Gia TN, Rahmani AM, Nigussie E, Virtanen S, Isoaho J, Tenhunen H. SEA: A secure and efficient authentication and authorization approach for IoT-based healthcare systems using smart gateways, in: The 6th International Conference on Ambient Systems, Networks and Technologies, 2015.
29. Moosavi SR, Gia TN, Nigussie E, Rahmani AM, Virtanen S, Tenhunen H, Isoaho J. Session resumption-based end-to-end security for healthcare Internet-of-things, in: IEEE Int Conf Comput Informa Technol 2015.
30. Valenzuela S, Chen M, Leung V. Mobility support for health monitoring at home using wearable sensors. IEEE Trans Inf Technol Biomed 2011; 15: 539-549.
31. Fotouhi H, Alves M, Zamalloa MZ, Koubaa A. Reliable and fast handoffs in low power wireless networks. IEEE Trans Mob Comput 2014; 13: 2620-2633.
32. Bonomi F, Milito R, Zhu J, Addepalli S. Fog computing and its role in the internet of things. Proceedings of the first edition of the MCC workshop on Mobile cloud computing. ACM, 2012.
33. Stolfo SJ, Salem MB, Keromytis AD. Fog computing: Mitigating insider data theft attacks in the cloud. Security and Privacy Workshops (SPW), 2012 IEEE Symposium on. IEEE, 2012.
34. Ivan S, Wen S. The fog computing paradigm: Scenarios and security issues. Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on. IEEE, 2014.
35. Hummen R, Gilder J. Extended DTLS session resumption for constrained network environments. Technical Report 2013.
36. Bormann C, Shelby Z, Hartke K. Constrained Application Protocol (CoAP), draft-ietf-core-coap-18, IETF, 2013.
37. http://sourceforge.net/p/tinydtls
38. http://pandaboard.org/
39. http://www.ti.com/lit/ug/swru321a
40. http://www.aragosystems.com/en/documentcenter
41. http://tools.ietf.org/html/rfc5280

***Correspondence to**

Praveen Kumar Reddy M

School of Computing Science and Engineering

VIT University

India