Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 52 (2015) 452 – 459

Procedia Computer Science

6th International Conference on Ambient Systems, Networks and Technologies (ANT 2015)

SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways

Sanaz Rahimi Moosavi[1*], Tuan Nguyen Gia[1], Amir-Mohammad Rahmani[1,2], Ethiopia Nigussie[1], Seppo Virtanen[1], Jouni Isoaho[1], Hannu Tenhunen[1,2]

[1]*Department of Information Technology, University of Turku, Turku, Finland*
[2]*Department of Electronic Systems, Royal Institute of Technology, Stockholm, Sweden*

Abstract

In this paper, a secure and efficient authentication and authorization architecture for IoT-based healthcare is developed. Security and privacy of patients' medical data are crucial for the acceptance and ubiquitous use of IoT in healthcare. Secure authentication and authorization of a remote healthcare professional is the main focus of this work. Due to resource constraints of medical sensors, it is infeasible to utilize conventional cryptography in IoT-based healthcare. In addition, gateways in existing IoTs focus only on trivial tasks without alleviating the authentication and authorization challenges. In the presented architecture, authentication and authorization of a remote end-user is done by distributed smart e-health gateways to unburden the medical sensors from performing these tasks. The proposed architecture relies on the certificate-based DTLS handshake protocol as it is the main IP security solution for IoT. The proposed authentication and authorization architecture is tested by developing a prototype IoT-based healthcare system. The prototype is built of a Pandaboard, a TI SmartRF06 board and WiSMotes. The CC2538 module integrated into the TI board acts as a smart gateway and the WisMotes act as medical sensor nodes. The proposed architecture is more secure than a state-of-the-art centralized delegation-based architecture because it uses a more secure key management scheme between sensor nodes and the smart gateway. Furthermore, the impact of DoS attacks is reduced due to the distributed nature of the architecture. Our performance evaluation results show that compared to the delegation-based architecture, the proposed architecture reduces communication overhead by 26% and communication latency from the smart gateway to the end-user by 16%.

Peer-review under responsibility of the Conference Program Chairs
Keywords: Internet of Things; Healthcare; Smart Home/Hospital; Smart Gateway; Security; Authentication; Authorization

1. Introduction

Recent advances in information and communication technologies and embedded systems have given rise to a new technology: Internet of Things (IoT)[1]. IoT enables people and objects in physical world as well as data and virtual environments to interact with each other, hence realizing smart environments such as: smart transport systems, smart cities, smart healthcare, and smart energy as part of a prosperous digital society. The rising cost of healthcare, and the prevalence of chronic diseases around the world urgently demand the transformation of healthcare from a hospital-centered system to a person-centered environment, with a focus on citizens' disease management as well as their wellbeing[2]. It has been predicted that in the following decades, the way healthcare is currently provided will be transformed from hospital-centered, first to hospital-home-balanced in 2020th, and then ultimately to home-centered

* Corresponding author. Tel.: +3-582-333-8647.
E-mail address: saramo@utu.fi

Peer-review under responsibility of the Conference Program Chairs
doi:10.1016/j.procs.2015.05.013

in 2030th[3]. This essential transformation necessitates the fact that the convergence and overlap of the IoT architectures and technologies for smart spaces and healthcare domains should be more actively considered[2,4,5,6].

Security is a major concern wherever networks are deployed at large scales. IoT-based healthcare systems deal with human-related data. Although collected from innocuous wearable sensors, such data is vulnerable to top privacy concerns[7]. In IoT-based healthcare applications, security and privacy are among major areas of concern as most devices and their communications are wireless in nature[8]. Due to direct involvement of humans in IoT-based healthcare applications, providing robust and secure data communication among healthcare sensors, actuators, patients, and caregivers are crucial. Misuse or privacy concerns may restrict people to utilize IoT-based healthcare applications. Conventional security and protection mechanisms including existing cryptographic solutions, secure protocols, and privacy assurance cannot be re-used due to resource constrains, security level requirements, and system architecture of IoT-based healthcare systems[9]. To mitigate the aforementioned risks, strong network security infrastructures for a short or long-range communication are needed. There are significant security solutions to current wireless networks which are not directly applicable to IoT-based healthcare applications due to the following challenges[10]: i) security solutions must be resource-efficient as medical sensor nodes have limited processing power, memory, and communication bandwidth. Thus, using conventional cryptography techniques that require heavy computations are infeasible, and ii) medical sensor nodes can be easily lost or abducted as they are tiny in terms of size.

Recently, there have been efforts in designing *Smart e-Health Gateways* for IoT-based healthcare applications[2]. In most of IoT-based healthcare applications, especially in smart homes/hospitals, there exists a bridging point (i.e., gateway) between a sensor network and the Internet which often just performs basic functions such as translating between the protocols utilized in the Internet and sensor networks. In a smart home/hospital, where the mobility and location of patients are confined to hospital facilities or buildings, gateways can play a key role. The stationary nature of such gateways enables them with the exclusivity of being non-resource constrained in terms of power consumption, memory, and communication bandwidth. This property can be exploited by outsourcing some burden of resource-constrained medical sensors/actuators to be performed on smart e-health gateways. By taking responsibility for handling some burdens of a sensor network and a remote health-care center, a smart e-health gateways can cope with a number of challenges in ubiquitous healthcare systems such as security, scalability, and reliability.

In this paper, we present a secure and efficient authentication and authorization architecture for IoT-based healthcare using distributed smart e-health gateways called *SEA*. SEA exploits the aforementioned features of distributed smart e-health gateways to outsource some burden of medical sensor nodes that enable those sensors to communicate securely and efficiently beyond independent network domains. By providing the established connection context to the medical sensor nodes, these devices no longer need to authenticate and authorize a remote healthcare center or a caregiver. Thus, any malicious activity can be blocked before entering to a medical constrained domain. We employed DTLS handshake protocol as it is the main IP security solution for the IoT. To the best of our knowledge, SEA is the first effort in proposing a secure and efficient authentication and authorization approach for IoT-based healthcare applications using smart e-health gateways. We elaborate the proposed approach from the viewpoint of security as well as performance analysis. To provide a proof of concept, we also demonstrate our prototype of a IoT-based healthcare architecture using smart e-health gateway and discuss the design and implementation of our prototype.

The remainder of this paper is organized as follows: In Section 2, the related works and the motivation of this work are discussed. Section 3 describes the proposed secure and efficient authentication and authorization architecture for IoT-Based healthcare systems. Demonstration of our proposed architecture and experimental results are provided and discussed in Section 4. Finally, Section 5 concludes the paper.

2. Related Work and Motivation

For the discussion of related work, we recognize two main research directions: (i) IoT-based Healthcare Security and (ii) Smart Gateways.

2.1. IoT-based Healthcare Security

CodeBlue is one of the most popular healthcare research projects that has been developed at the Harvard sensor network Lab[11]. In this approach, several medical sensors are placed on patients' body. CodeBlue has been expected to be deployed in in-hospital emergency care, stroke patient rehabilitation and disaster response. The authors of CodeBlue admit the necessity of security for IoT-based medical applications. However, the security aspects of CodeBlue is still pending or it is left as a future work. Lorincz *et al.*[12] suggest that Elliptic Curve Cryptography (ECC)[13] and TinySec[14] are efficient solutions to be used for key generation and symmetric encryption in the CodeBlue project, respectively. But, so far their proposed solution has not been implemented yet. Kambourakis *et al.* discuss some attack models and security threats concerning the CodeBlue project: denial-of-service attack, snooping attack, grey-hole attack, sybil attack, and masquerading attacks[15]. To establish an interoperable network security between end-peers from independent network domains, variants of conventional end-to-end security protocols have been recently proposed among which Datagram Transport Layer Security (DTLS) is one of the most relevant protocols[17]. In this regard, Hummen

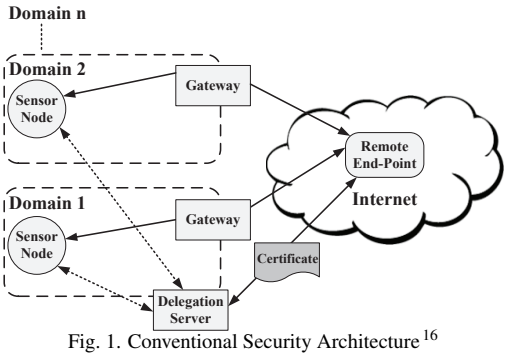

Fig. 1. Conventional Security Architecture [16]

et al. [16] present an implementation of a delegation architecture based on an off-path delegation server. As depicted in Fig. 1, their proposed delegation-based architecture relies on a centralized delegation server. However, their proposed architecture lacks scalability and reliability. More precisely, their architecture cannot be extended to be employed for multi-domain infrastructures, e.g. large in-home/hospital domains. Also, their proposed architecture suffers from a considerable network transmission overhead resulting to a long transmission latency. Moreover, if an adversary performs a Denial of Service (DoS) attack or compromises the delegation server, a large quantity of stored security context of a constrained domain can be retrieved. More precisely, in multi-domain networks, a DoS attack can disrupt all the available constrained medical domains as the functionality of the IoT-based healthcare still depends on the centralized delegation server.

2.2. Smart e-Health Gateway

There have been many efforts in designing gateways for one or several specific applications and architectural layers. Muller *et al.* [4] present a gateway called SwissGate which handles and optimize the operation of sensor networks. They transparently employ their proposed gateway on home automation applications. Shen *et al.* [5] propose a prototype of a smart 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks) border router that makes local decisions of users health states based on a Hidden Markov Model. Finally, Rahmani *et al.* [2] present a smart e-health gateway called *UT-GATE* in order to bring intelligence into IoT-based ubiquitous healthcare systems. These gateways are intelligent in the sense that they have been empowered to autonomously perform local data storage and processing, to learn, and to make decision at the edge of the network (i.e., in a distributed fashion), thanks to the provided embedded processing power and storage capabilities of the gateways. A smart gateways can rapidly provide preliminary results and reduce the redundant remote communication to cloud servers by using data aggregation, embedded machine learning, and compression techniques, thus offering the basic services at the edge of the network. In this way, remote cloud computers will just provide premium services which are often computationally intensive and require to access to the central database.

As can be noticed from Fig. 2, in a smart home/hospital, gateway is in a unique position between the both Body/Patient/Local Area Network (BAN/PAN/LAN) and Wide Area Network (WAN). Thus, this promising opportunity can be exploited by different means such as collecting health and context information from those networks and providing different services accordingly. As mentioned above, compared to the conventional gateways which often just performs basic functions such as translating between the protocols used in the Internet and sensor networks, smart e-health gateways are empowered with the property of being non-resource constrained in terms of processing power, memory, power consumption, and communication bandwidth. Moreover, certificate-based DTLS handshake that is employed to authenticate and authorize remote end-users imposes significant overheads to constrained medical sensor nodes. These resource requirements specially barricade secure and efficient communications among medical sensor nodes and remote end-users. As a result, our proposal is motivated by the fact that in a smart hospital/home, the strategic position and the distributed nature of smart e-health gateways can be exploited to handle the main computation and communication overhead of medical sensor nodes deduced from end-user authentication and authorization.

3. Secure and Efficient Authentication and Authorization (SEA) Architecture

The architecture of IoT-based healthcare monitoring system using smart e-health gateways in home/hospital domain(s) is shown in Fig. 2. In such a system, patient health-related information is recorded by body-worn or implanted sensors, with which the patient is equipped for personal monitoring of multiple parameters. This health data can be also supplemented with context information (e.g., date, time, location, and temperature) which enables to identify unusual patterns and make more precise inferences about the situation. The proposed system architecture includes the following main components: i) Medical Sensor Network (MSN), enabled by the ubiquitous identification, sensing, and communication capacity, bio-medical and context signals are captured from body/room which is used for treatment and diagnosis of medical states. The signal is then transmitted to the gateway via wireless or wired communication

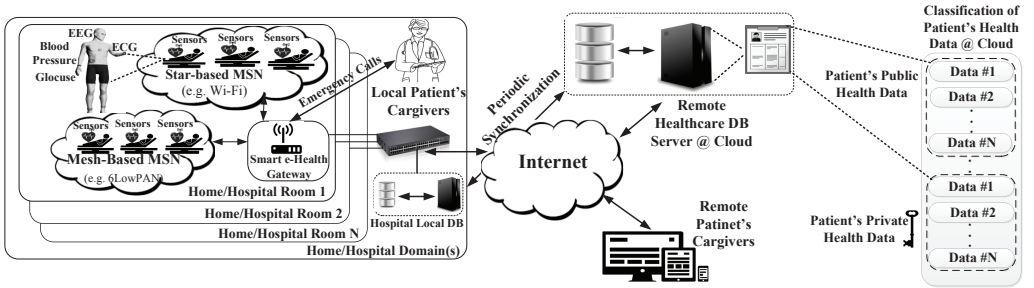

Fig. 2. The Architecture of an IoT-based Healthcare Monitoring System Using Smart e-Health Gateways in Home/Hospital Domain(s)

protocols such as Serial, SPI, Bluetooth, Wi-Fi or IEEE 802.15.4. ii) Smart e-Health Gateway, which supports different communication protocols, acts as a touching point between the MSN and the local switch/Internet. It receives data from different sub-networks, performs protocol conversion, and provides other higher level services such as data aggregation, filtering and dimensionality reduction[2]. iii) Back-End System, the back-end of the system consists of the remaining components, a local switch (in in-hospital domains), a cloud computing platform that includes broadcasting, data warehouse and big data analytic servers, and hospital local database (DB) that periodically performs data synchronization with the remote healthcare DB server at the cloud to continuously synchronize patients' health data over time. In cloud computing platform accessability to patients-related health data is classified as public data (e.g., patients' ID or blood type) and private data (e.g., DNA) based on their relevance. iv) Web clients as a graphical user interface for final visualization and apprehension. The collected health and context information represents a vital source of big data for the statistical and epidemiological medical research (e.g., detecting approaching diseases).

Our proposed SEA architecture exploits distributed smart e-health gateways to perform authentication and authorization of remote end-users securely and efficiently on behalf of medical sensors. As mentioned before, the main role of a gateway in general is to support different wireless protocols and inter-device communication. However, in the area of IoT-based healthcare, the role of a gateway has been extended to provide additional services such as: acting as local repository, to temporarily store sensors' and users' information, providing local processing of sensors' data and bringing intelligence by enhancing with data fusion, aggregation, and interpretation techniques. For example, *UT-GATE*[2] is a smart e-health gateway which is composed of dual-core ARM Cortex-A9 cores with symmetric multiprocessing at up to 1.2GHz each. It supports up to 128GB memory and has been powered by Ubuntu Operating System (OS). Likewise, *Intel IoT Gateways*[6] which enable connectivity up to the cloud and enterprises and down to the sensors, pre-process filtering of selected data for delivery, local decision making, data encryption and software lock down for security. Intel IoT Gateway includes choice of Intel processors: Intel Quark SoC X1000, Intel Quark SoC X1020D, and Intel Atom processor E3826 and supports external SD memory. As shown in Fig. 1, conventional security architecture proposed for IP-based IoT relies on a centralized *Delegation Server* that can provide a constrained device with necessary security contexts[16]. However, in this architecture, if an adversary performs a Denial of Service (DoS) attack or compromises the delegation server, a large quantity of stored security context of a constrained domain can be retrieved. More precisely, in multi-domain networks, a DoS attack on delegation server can disrupt all the available constrained medical domains as the functionality of the IoT-based healthcare still depends on the centralized delegation server. To fulfill the above challenges, we exploit the aforementioned features of the smart e-health gateways to perform authentication and authorization more securely and efficiently using a distributed approach. In this architecture, the major responsibility of the smart e-health gateway is to provide the constrained medical device with essential security contexts to enable them to securely communicate with the remote end-user. To build the necessary security context along with remote end-point, smart e-health gateway acts on behalf of medical constrained devices. Afterward, the established security context is handed over to a constrained medical device.

Compared to typical gateways as well as delegation server, since smart e-health gateways has a local database, it can temporarily store medical sensors' information and provide local processing of medical sensors' data, hence its role can be authorized as an embedded server. By exploiting the above-mentioned features of smart e-health gateways, the authentication and authorization task of a centralized delegation server can be broke down to be handled by distributed smart e-health gateways. Hence, in each room/sub-domain of smart medical constrained domains (i.e., home, hospital, and elderly house) authentication and authorization of remote end-points can be handled by an exclusive smart e-health gateway. As a result, in a multi-domain smart home/hospital network if an adversary performs a DoS attack or compromises one of the smart e-health gateways, only the associated medical constrained sub-domain can be disrupted. In the proposed SEA architecture, first, we intend to re-use available security protocols to implement authentication and authorization among independent network domains. Second, we try to provide essential security context to medical constrained devices that have limited hardware resources to securely communicate with remote healthcare center. Our proposed SEA architecture focuses on a fact that the smart e-health gateway and the remote end-user, have sufficient resources in order to perform various heavy-weight security protocols as well as certificate validation efficiently. To provide an interconnection between a remote end-user (i.e., a remote healthcare center or a caregiver) and a constrained medical device, a smart e-health gateway is introduced to build an IP-based security

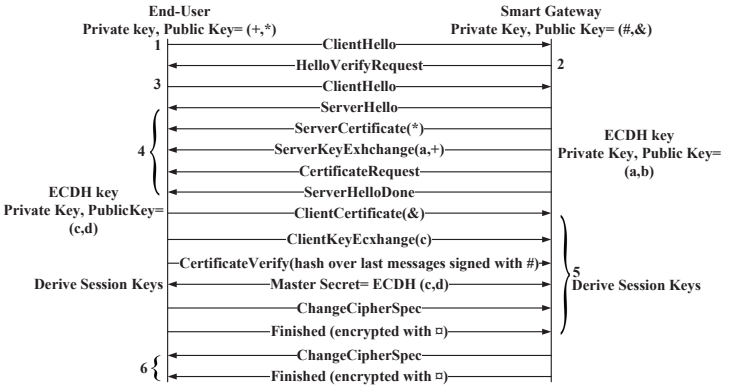

Fig. 3. Mutual Certificate-based DTLS Handshake Between End-user and Smart Gateway

protocol i.e., Datagram Transport Layer Security (DTLS)[17]. DTLS handshake protocol is the main IP security solution of IoT. A full handshake begins with a *ClientHello* message, that includes the security parameters for the connection which is used later during the handshake to compute the pre-master secret key. Flight 3 contains additional cookie from *ClientHelloVerify*. Flight 4 includes several messages and starts with *ServerHello* message which contains the negotiated cipher suite for the current handshake and the smart gateway's random value which is utilized later during the handshake to compute the master secret key. The agreed cipher suite relies on supported cipher suites by end-user. If the smart gateway and the end-user cannot agree on a common cipher suite, the handshake is canceled with a *HandshakeFailure* alert message. The next message of flight 4 is smart gateway's *Certificate* message which holds gateway's certicate-chain. The first certificate in the chain, includes the smart gateway's public key which is created using *OpenSSL* in version of 1.0.1.j. OpenSSL is an open source project for implementing SSL, TLS and various cryptography libraries such as symmetric key, public key, and hash algorithms. It is commonly utilized for creating and managing keys and certificates. Once the certificate is validated, end-user can extract smart gateway's public key. The *CertificateRequest* is only sent in a mutual handshake and includes the lists of smart gateway's valid certificates. The *ServerKeyExchange* message is only sent with specific cipher suites that need more parameters in order to compute master secret key. cipher suite employed in this work is $TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CCM\_8\_SHA\_256$ indicates the use of elliptic cryptography particularly *Elliptic Curve Diffie-Hellman* (*ECDH*) and *Elliptic Curve Digital Signature Algorithm* (*ECDSA*). Furthermore, for encryption AES-based CCM with an IV of 8 bytes is used. With this cipher suite, ServerKeyExchange message contains the ECDH public key of the smart gateway and the detail of the associated elliptic curve. The *ServerHelloDone* message announces the end of flight 4 messages. The first message of flight 5, is the end-user's certificate in case mutual authentication is run. *ClientKeyExchange* includes additional parameters utilized to compute the master secret key. In this case, the ECDH public key of the smart gateway is conveyed. *CertificateVerify* is a message which enables the end-user to prove to the smart gateway that it carries the private key which corresponds to the public key contained in the certicate. Thus, it is only transmitted in the mutual authentication. With the *ChangeCipherSpec* message, the end-user informs the smart gateway that next messages will be encrypted using the agreed cipher suites and secret keys. The *Finished* message includes the encrypted hash over all flight messages which ensure that both peers have been performing handshake based on unmodified flight messages and the handshake is performed successfully. In flight 6, the smart gateway responds with its own ChangeCipherSpec and Finished messages. With the Finished messages both peers agree to send and receive securely protected application information over this connection. Upon this connection setup, as shown in Fig. 4, the remote end-point and the smart e-health gateway mutually authenticate each other. It is supposed that within the certificate-based DTLS handshake, from one hand, the smart e-health gateway authenticates (*Auth-req.1*) the remote end-point through certicates. In this regard, similar to current web browsers, smart e-health gateways hold a pool of of trusted certificate. On the other hand, the smart e-health gateway, either authenticates (*Auth-req.2*) to the remote end-point through certificates within the DTLS handshake mechanism or based on an application-level password once the handshake is terminated. The major goal of this work is to hand over the necessary security context, i.e. authorization or remote end-users to constrained medical devices. Since in the proposed SEA architecture, the validation of the certificate-based DTLS handshake and the access right of the remote end-user is implemented by the smart e-health gateway instead of the resource-constrained medical devices, any malicious activity can be blocked at the first step of the whole process. Thus, by building secure connections on behalf of the medical sensor, the smart e-health gateway can securely and efficiently control with which remote end-user this medical sensor can communicate. Once the mutual authentication between end-user and smart gateway is done successfully, end-user authorizes (*Authz.*) as a trusted entity so that data query from user's side is transmitted to the medical sensor node through the smart gateway.

To facilitate security and authorization of communication, it is also required that both entities, constrained medical sensor and smart e-health gateway, mutually authenticate (*Mut-auth.*) one another within a local smart home/hospital network domain. In SEA, this is done by performing a public key-based DTLS handshake between both entities.

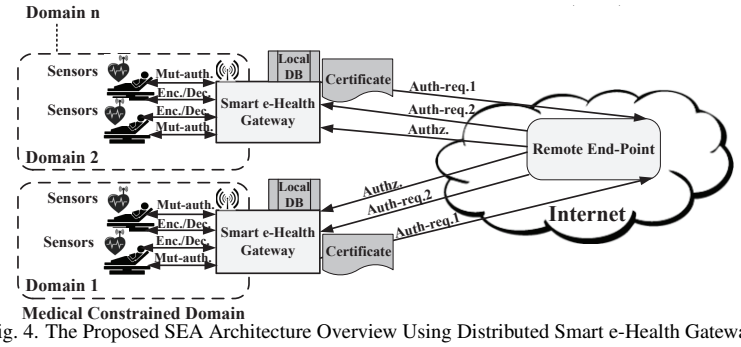

Fig. 4. The Proposed SEA Architecture Overview Using Distributed Smart e-Health Gateways

Although, symmetric key-based DTLS handshake protocol provides an efficient alternative to public key-based DTLS handshake, the symmetric key-based handshake needs secret keys to be pre-shared and readily available at both communication end-points. Moreover, compared to the symmetric key-based DTLS handshake, obtaining secret points in a public key-based handshake implies the computation of elliptic curve discrete logarithm problem. Since solving the discrete logarithm problem is as hard as integer factorization, this problem cannot be solved effortlessly[13]. In this architecture, for public key-based authentication and key agreement, ECC primitives, namely ECDSA[13] and ECDH[18], are utilized which are more efficient compared to their RSA[19]-based counterparts[16]. ECDSA provides the both authentication and message integrity protection of an information and it is utilized with regards to the key exchange protocol in DTLS handshake. ECDH is used to securely exchange secret information in an insecure communication. In this regard, each of the peers, constrained medical sensor and smart e-health gateway, generate their own private and public keys and exchange their generated pubic keys between themselves. Once mutual authentication and key exchange protocol is done, it is required that both peers agree upon a common key. This shared common key can be generated using an already agreed elliptic curve between the both peers. Using the shared common key, one peer (i.e., constrained medical sensor) encrypts the gathered patients' medical data applying the efficient *Advanced Encryption Standard* (*AES-CCM*)[20] algorithm and transmits the encrypted medical information (*Enc./Dec.*) to the smart e-health gateway and vice versa. AES-CCM offers confidentiality, integrity, and authentication of payload which compared to other commonly known symmetric encryption/decryption algorithms (e.g., RC5, and Triple-DES), it is known as one of the most efficient ones. Moreover, AES is supported by many constrained devices used for IoT platforms. This make AES-CCM desirable encryption/decryption algorithm choice for constrained devices. The use of distributed smart e-health gateways in this approach enable to address the previously mentioned challenges of the conventional architecture. In the proposed SEA architecture: first, a great part of the work (i.e., authentication and authorization of a remote end-user or a remote healthcare center) is shifted to be performed by distributed smart e-health gateways(s), thus, compared to the conventional architecture, network transmission overhead and latency is reduced. Second, the privacy of patients, vital certificates, and key negotiation materials are effectively protected. Third, the IoT-based healthcare architecture becomes more scalable and reliable as the architecture is changed from centralized to distributed fashion.

4. Implementation and Evaluation

In this section, first, we describe the details of the proposed SEA implementation for the IoT-based healthcare using smart e-health gateways. Second, we discuss the the evaluation of the proposed SEA implementation which is divided into two main sections: (i) transmission overhead and (ii) latency. Finally, we provide a fair comparison between the result of this work and the state-of-the-art delegation based authentication and authorization approach[16].

4.1. Implementation

To Implement SEA, we setup a platform that consists of medical senor nodes, UT-GATE smart e-health gateway, remote server, and end-users. In this platform the UT-GATE provides medical data collected from medical sensor nodes to end-users through web browsers to their devices. UT-GATE is constructed from combination of a Pandaboard[21] and Texas Instruments (TI) SmartRF06 board integrated with CC2538 module[22]. The Pandaboard is low-power, low-cost single-board computer development platform based on TI OMAP4430 system-on-chip (SoC) following OMAP architecture and fabricated using 45nm technology. OMAP4430 processor is composed of Cortex-A9 microprocessor unit (MPU) subsystem including dual-core ARM cores with symmetric multiprocessing at up to 1.2GHz each. In UT-Gate, 8GB external memory added to the Pandaboard and powered by Ubuntu OS which allows to control devices and services such as local storage and notification. To investigate the feasibility of the proposed SEA architecture, similar to the existing studies on the security of medical sensor nodes, *WiSMote*[23] platform which is a common resource-limited sensor node in utilized[2,7,8,10,12,16]. Wismote is equipped with a 16MHz MSP430 micro-controller, an IEEE 802.15.4 CC2520 radio transceiver, 128KB of ROM, 16KB of RAM, and supports 20-bit addressing. We selected this platform as it offers enough processing power to implement public key-based DTLS handshake protocol.

Table 1. Performance comparison with the state-of-the-art authentication and authorization approach for IoT.

	Transmission-overhead (*byte*)	$Latency_{GE}$ (*s*)	$Latency_{NG}$ (*s*)
Hummen et al.[16]	1609	6.08	~ 15
SEA approach (This work)	1190	5.001	~ 15
SEA approach improvements (%)	26	16	0

4.2. Security and Performance Analysis

For the evaluation of the proposed SEA approach, similar to the delegation-based architecture, we use the open source tool *OpenSSL* to create elliptic curve public and private keys from the NIST P-256 (prime256v1) and X.509 certificates. X.509 certificates are the prevailing form of certificates and are employed in the certicate-based mode of DTLS[24]. As the code-base of the proposed approach, we employed *tinyDTLS*[25], which is an open-source implementation of DTLS in symmetric key-based mode, to extend it with support of the public key-based as well as certificate-based modes. For the public-key functions, we utilized the *Relic-toolkit*[26] which is an open source cryptography library tailored for specific security levels with emphasis on efficiency and flexibility. The MySQL database is set up for static and non-static records. Static storage, which is managed by system administrators, includes white tables, essential data required by DTLS handshake protocol and a user authentication mechanism, and consistent configurations of different services. White table encompassing the lists of sensor nodes identification, is used as a premise in pursuance of supporting the DTLS handshake between a smart e-health gateway and registered medical sensor nodes. It also keeps track of communication of those sensor nodes. Essential data is used for DTLS handshake and end-user authentication mechanism in the direction of guaranteeing a complete end-to-end security between a gateway and an end-user. Non-static records storing up-to-date bio-signals that are synchronized between the Pandaboard database and a cloud server database with the intention of maintaining large and long-term e-health data records. The cloud server database is processed with the assistance of xSQL Lite which is the third party tool for data synchronization. With respect to the cryptographic primitives and to make a fair comparison, we followed similar cipher suites (which are current security recommendations for constrained network environments[27]) as employed in the state-of-the-art authentication and authorization architecture for IP-based IoT[26]. In this regard, we utilize elliptic curve NIST-256 for public-key operations, $AES\_128\_CCM\_8$ (with an IV of 8 bytes) for symmetric-key operations, SHA256 for hashing purposes. The presented results are based on averages over 100 runs and it is shown in Table 1.

4.2.1. Security Analysis

In delegation-based architecture[16], if an attacker runs a DoS attack or compromises the delegation server, a large quantity of stored security context of a constrained domain can be retrieved. Specifically, in multi-domain networks, a DoS attack can disrupt all the available constrained medical domains as the functionality of the IoT-based healthcare still depends on the centralized delegation server. Whereas, in this work, in a multi-domain smart home/hospital network, if an adversary performs a DoS attack or compromises one of the smart e-health gateways, only the associated medical sub-domain can be disrupted. Because, authentication and authorization task of a centralized delegation server is broke down to be handled by distributed smart e-health gateways. Thus, compared to the delegation-based architecture, the proposed SEA approach becomes more scalable and reliable as the architecture is changed from centralized to distributed fashion. In addition, in delegation-based approach if an adversary compromises a constrained sensor node, the master key can be accessed easily as it is pre-shared between the delegation server and the sensor node during the bootstrapping process. However, in SEA approach, the shared master key is generated using an agreed elliptic curve algorithm between the both sensor node and smart e-health gateway. Obtaining this master is not easily possible as it implies the computation of elliptic curve discrete logarithm problem which is as hard as integer factorization.[13]. Based on the discussion above, the proposed SEA architecture has higher level of security compared to the state-of-the-art delegation-based architecture.

4.2.2. Transmission Overhead

As discussed before, to perform the certificate-based DTLS handshake, all 15 messages are needed to establish a DTLS connection. When transmitted over size-constrained IEEE 802.15.4 radio links, these messages must additionally be split into several packet fragments due to their extensive message size[16]. As Table 1. presents, we compared the transmission overhead of the proposed SEA approach to the state-of-the-art architecture for a successful certificate-based DTLS connection. In delegation-based architecture, the measured transmission overhead of the certificate-based DTLS handshake is 1609 bytes which cause in total 24 fragments for the transmission of all handshake messages from the delegation server to the end-user[16]. In contrast, the proposed SEA architecture requires transmission of 1190 bytes and it cause 18 fragments totally. As a result, the transmission overhead in the proposed SEA architecture reduces by 26% compared to the delegation-based architecture.

4.2.3. Communication Latency

Latency is defined as the time required from sending a request to confirming the shared session key between two peers. This metric is vital for time-critical applications such as IoT-based medical domains. To estimate the

communication latency, the processing time which is spent from sensor node to the end-user (*NE*) is calculated. This processing time deduced from the summation of communication latency from sensor node to smart gateway (NG) and smart gateway to end-user which can be written as: $Latency_{NE} = Latency_{NG} + Latency_{GE}$. In this work, to compute the communication latency from the UT-Gate to the end-user, a proxy server is adjoined to the network. Through the proxy server, transmission latency between the end-user and the UT-Gate can be easily measured as proxy server listens to requests transmitted from the end-user to the UT-Gate and vice versa without tampering or modifying them. To compute the communication latency of *GE*, Fiddle[2] proxy server which is a computer application is employed to track requests and responses. Fiddle offers a large number of services including security testing and HTTP/HTTPs traffic recoding. According to our analysis, the proposed SEA approach achieves an almost equivalent *NG* processing time to the delegation-based architecture[16], which it takes up to 15*S* for the certificate-based DTLS handshake. However, the proposed SEA approach considerably reduces the processing time required for *GE* compared to the delegation-based architecture. As shown in Table 1, in SEA, the processing time required for *GE* is about 5.001*S* whereas this time increases to about 6.08*S* in the delegation-based architecture. Thus, regarding the latency from the gateway to the end-user, the proposed SEA architecture obtains about 16% improvement compared to the delegation-based architecture.

5. Conclusion

In this paper, we presented a secure and efficient authentication and authorization architecture for IoT-based healthcare systems using distributed smart e-health gateways. Sensors used in medical applications are extremely resource-constrained for which reason they cannot cope with cryptography techniques demanding heavy computations. To alleviate this limitation, we proposed an architecture that employs distributed smart e-health gateways which perform authentication and authorization on behalf of the medical sensors. This reduces the overhead imposed in the medical sensors without compromising the security. The proposed architecture relied on the certificate-based DTLS handshake protocol which is the main IP security solution for IoT. Our security analysis showed that the proposed architecture is more secure than the centralized delegation based architecture. This is due to the distributed nature of the proposed architecture as it has more resilience over DoS attacks and it uses a more secure key management technique. The performance analysis revealed that our proposed authentication and authorization architecture reduces communication overhead by 26% and communication latency from the smart gateway to the end-user by 16%, compared to the state-of-the-art architecture. Therefore, the presented architecture is a very promising solutions to provide scalable and reliable end-to-end security for IoT-based healthcare systems.

Acknowledgment

The authors wish to acknowledge the financial support by the Finnish Cultural Foundation, HPY Foundation, and Nokia Foundation during the course of this project.

References

1. European Commission Information Society. Internet of Things Strategic Research Roadmap, 2009.
2. A. Rahmani et al. Smart e-Health Gateway: Bringing Intelligence to IoT-Based Ubiquitous Healthcare Systems. In *CCNC'15*, 2015.
3. C. Koop et al. Future Delivery of Health Care: Cybercare. *EMBM*, 27(6):29–38, 2008.
4. R. Mueller et al. Demo: A Generic Platform for Sensor Network Applications. In *MASS'07*, pages 1–3, 2007.
5. W. Shen et al. Smart Border Routers for eHealthCare Wireless Sensor Networks. In *WiCOM'11*, pages 1–4, 2011.
6. Intel. Intel IoT Gateway, 2014. http://www.intel.com/content/www/us/en/embedded/products [accessed 2014-01-22].
7. M. Ameenet al. Smart e-Health Gateway: Bringing Intelligence to IoT-Based Ubiquitous Healthcare Systems. *JMS*, 36(1):93–101, 2012.
8. K. Malasri et al. Addressing Security in Medical Sensor Networks. pages 7–12, 2007.
9. X. Hung et al. An Efficient Mutual Authentication and Access Control Scheme for WSN in Healthcare. *JN*, 6(3):355–364, 2011.
10. R. Chakravorty. A programmable Service Architecture for Mobile Medical Care. In *PerCom'06*, pages 5 pp.–536, March 2006.
11. D. Malan et al. CodeBlue: An Ad hoc sensor Network Infrastructure for Emergency Medical Care. In *WIBSN'04*, 2004.
12. K. Lorincz et al. Sensor Networks for Emergency Response: Challenges and Opportunities. *IEEEPC*, 3(4):16–23, 2004.
13. N. Koblitz. Elliptic Curve Cryptosystems. *JAMS*, 48:203–209, 1987.
14. C. Karlof et al. TinySec: A Link Layer Security Architecture for Wireless Sensor Networks. In *ICENSSS*, pages 162–175, 2004.
15. G. Kambourakis et al. Securing Medical Sensor Environments: The CodeBlue Framework Case. In *ARES'07*, pages 637–643, 2007.
16. R. Hummen et al. Delegation-based Authentication and Authorization for the IP-based Internet of Things. In *SECON'14*, 2014.
17. E. Rescorla and N. Modadugu. Datagram Transport Layer Security (DTLS) Version 1.2. In *RFC 5238*, 2012.
18. W. Shengbao et al. Cryptanalysis and Improvement of an Elliptic Curve Diffie-Hellman Key Agreement Protocol, 2007.
19. R. Rivest et al. A Method for Obtaining Digital Signatures and Public-key Cryptosystems. *JACM*, 21(2):120–126, 1978.
20. J. Daemen et al. Specification of Rijndael. In *The Design of Rijndael*, volume 17, pages 31–50, 2002.
21. PandaBoard. PandaBoard Platform Information. http://pandaboard.org/ [accessed 2014-01-22].
22. SmartRF06 Evaluation Board User's Guide. http://www.ti.com/lit/ug/swru321a/swru321a.pdf [accessed 2014-01-22].
23. Arago Systems. Wismote. http://www.aragosystems.com/en/document-center [accessed 2014-01-22].
24. D. Cooper et al. Internet X.509 Public Key Infrastructure Certificate Profile. http://tools.ietf.org/html/rfc5280 [accessed 2014-01-22].
25. O. Bergmann. TinyDTLS. http://sourceforge.net/p/tinydtls/code/ci/master/tree/ [accessed 2014-01-22].
26. D. Aranha et al. RELIC is an Efficient Library for Cryptography. http://code.google.com/p/relic-toolkit/ [accessed 2014-01-22].
27. Z. Shelby et al. Constrained Application Protocol (CoAP), draft-ietf-core-coap-18, IETF. 2013.