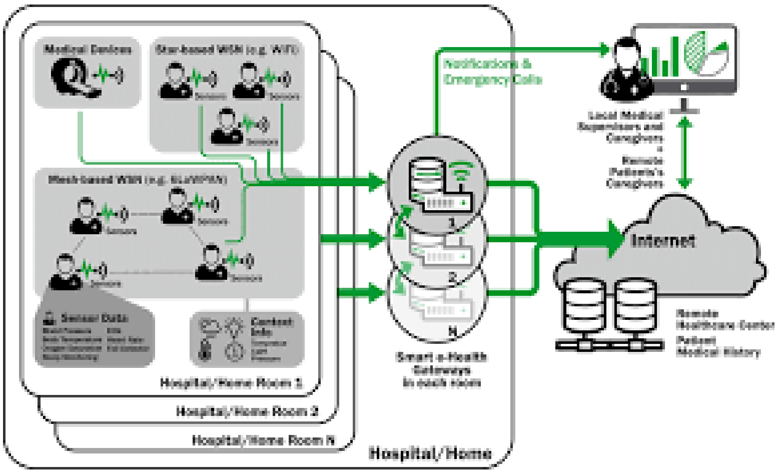
Health Monitors

+

Secure and Efficient Authentication and Authorization (SEA) Architecture

The architecture of IoT-based healthcare monitoring system using smart e-health gateways in home/hospital do-main(s) 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.



Protocols such as Serial, SPI, Bluetooth, Wi-Fi .ii) Smart e-Health Gateway, which supports dif-ferent 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 reduction2. iii) Back-End System, the back-end of the system consists ofthe remaining components, a local switch (in in-hospital domains), a cloud computing platform that includes broad-casting, 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).

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 protocol.

Implementation

To Implement SEA, we setup a platform that consists of medical senor nodes, UT-GATE smart e-health gateway, re-mote server, and end-users. In this platform the UT-GATE provides medical data collected from medical sensor nodesto 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 microprocessorunit (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 andservices 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, WiSMote23 platform which is a common resource-limited sensor node in utilized2,7,8,10,12,16. Wismote is equipped with a 16MHz MSP430 micro-controller, an IEEE802.15.4 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.

Evaluation

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-25 and X.509certificates. X.509 certificates are the prevailing form of certificates and are employed in the certicate-based mode of DTLS24. As the code-base of the proposed approach, we employed tiny DTLS 25 , which is an open-source implemen-tation 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 configura-tions 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 P and aboard 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 environments27) as employed in the state-of-the-art authentication and authorization architecture for IP-based IoT26. In this regard, we utilize elliptic curve NIST-256 for public-key operations, AES128 CCM 8 (with an IV of 8 bytes) for symmetric-key operations, SHA 256 for hashing purposes. The presented results are based on averages over 100 runs.