A Secure Cloud Framework for ICMetric Based IoT Health Devices

Ruhma Tahir
University of Essex
Wivenhoe Park
Colchester, United Kingdom
rtahir@essex.ac.uk

Hasan Tahir
University of Essex
Wivenhoe Park
Colchester, United Kingdom
htahir@essex.ac.uk

Ali Sajjad
British Telecom Ltd
Adastral Park
Ipswich, United Kingdom
ali.sajjad@bt.com

Klaus McDonald-Maier
University of Essex
Wivenhoe Park
Colchester, United Kingdom
kdm@essex.ac.uk

ABSTRACT

Wearable devices are an important part of internet of things (IoT)with many applications in healthcare. Prevalent security concerns create a compelling case for a renewed approach by incorporating the ICMetric technology in IoT healthcare. The ICMetric technology is a novel security approach and uses the features of a device to form the basis of cryptographic services like key generation, authentication and admission control. Cryptographic systems designed using ICMetric technology use unique measurable device features to form a root of trust. This paper uses the MEMS bias in a body wearable Shimmer sensor to create a device ICMetric. The ICMetric identity is used to generate cryptographic key to perform encryption and decryption of patients data which is being communicated to health professionals. The cloud based component of the proposed framework provides much needed distributed data processing and availability. The proposed schemes have been simulated and tested for conformance to high levels of security and performance.

Keywords

Cryptography; security; ICMetric; Internet of Things; cloud computing; secure healthcare systems;

1. INTRODUCTION

Advances in the field of ubiquitous and pervasive computing has resulted in the creation of a new computing paradigm called the Internet of Things. The Internet of Things is a collection of devices and systems which are designed as ubiquitous elements thus enabling the creation of smart environments. Devices for the Internet of Things have varying capabilities and purpose. Some devices are intended to be worn on the body while others will be mounted on a wall. This implies that more than often these devices will be sharing highly critical information. For example an IoT wearable health device will monitor the physiological signals and then forward the data to a heath provider. In such scenarios the importance of security cannot be denied.

Internet of Things based devices are available in various forms and sizes for instance televisions, refrigerators, watches, camerasetc. As devices integrate into daily life it must be recognized that attacks can lead to violation of physical security and privacy. As the Internet of Things grows, companies are trying to design innovative systems that revolutionize how we interact with technology. While innovations are noteworthy it has also been seen that some devices do not possess the security services they should have. In this paper a security framework has been proposed that studies the security of wearable devices in the Internet of Things. The proposed security framework is based on the novel Integrated Circuit Metric (ICMetric) technology and has been extended to the domain of Cloud Computing by outsourcing the data monitoring and analysis components to the cloud environment while still conforming to the privacy and confidentiality requirements of the user domain. Conventional security algorithms have design weaknesses which have led to systems being exposed. Conventional cryptography uses algorithmic intractability as a root of trust. This is not always the best basis for cryptographic algorithms, which is why researchers are considering other methods upon which security can be based. The ICMetric technology uses features of a device to form the basis of cryptographic services. The ICMetric technology uses unique measurable features of a device which cannot be created by an adversary. This results in a unique identity called the ICMetric of a device and is used as a root of trust in cryptographic services. What sets the ICMetric technology apart from other fingerprinting technologies is the fact that the ICMetric of a device is never stored on a system and never communicated.The ICMetric technology is used to generate cryptographic keys thereby enabling device verification while providing a strong link between the device and cryptographic key. To address the issues related to secure remote monitoring of patients using healthcare IoT devices, we propose the development of a secure cloud framework for patient monitoring which is based on the ICMetric technology. The features translate directly into providing high levels of security at the cost of very limited resource.

The biggest advantage of the designed scheme is that at no point during the lifecycle of its secure functioning, does it require any human intervention. This is particularly important from the patient's perspective since taking patient input is not a plausible concept while securely transmitting health data. Therefore all the security functions of our framework are based on ICMetric data derived from the respective devices.

The research makes the following contributions to the secure cloud framework for health IoT devices based on the ICMetric technology:

The first contribution of this paper is a study on features which can be used for the creation of a device ICMetric. The paper

shows that MEMS sensors possess a unique bias which can be used for ICMetric generation. The study is based on a testbed of six identical Shimmer sensors. The accelerometer, gyroscope and strain gauge sensors have been used for taking readings and then studied statistically.The proposed scheme intends to bind a cryptographic key with the sensor's ICMetric information.

The second contribution of the paper is a secure admission control and mutual authentication process as a core component. This part of the design is aimed at recognizing each IoT device which is part of the application. It recognizes each patient based on allocated sensors, and the health professional based on his end device. So this component authenticates, authorizes and evaluates each entity prior to secure communication of the health data.

A challenge with the generated device ICMetric is the entropy and length of the generated secret value. Hence the third contribution of the paper is a strong symmetric session key that is based on the communicating parties device ICMetric. The generated symmetric key facilitates secure communications between the patient and the health professional.

The fourth contribution of the paper is a demonstration of encryption/ decryption and integrity of a criticality trigger from the patient to the health professional. The trigger is an indication to the health professional that a patient is experiencing an episode of some medical emergency and that an appropriate action is required. The trigger is encrypted/ decrypted based on the generated symmetric session key between the patient and the health professional.The generated session key also serves to carry out mutual authentication between the patient and the medical specialist.

The fifth contributionin the framework is the use ofcloud environment for scalability and distributed data processing services. The cloud has been used to enhance the practicality of the framework by providing the functionalities of availability and data analysis of patient data.

The remainder of this paper is organized as follows; section 2 discusses recent advancements in the field of IoT. Section 3 highlights some threats in wearable IoT systems. Section 4 discusses in detail the ICMetric technology and its design principles. A detailed attack model is also presented in this section. Section 5 presents the concept of a sensor bias in MEMs sensors. Section 6 details the basic system design and the design goals of the proposed framework. Section 7 presents a detailed study on how the ICMetric can be generated using MEMS sensor bias. In section 8, details of the proposed scheme are presented with focus on admission control and symmetric key generation. Section 9 presents a study on the cloud component of the proposed scheme from various perspectives like security, scalability and stability. The proposed schemes have been simulated and analyzed in section 10 and 11. The paper concludes in section 12 with a summary of findings and directions for future work.

2. INTERNET OF THINGS

The internet of Things (IoT) is a network of smart devices that collect and communicate data through various forms of network connectivity. Hence the IoT is a collection of devices that sense various parameters and then communicate these on the internet. A user may have many IoT capable devices that connect to each other and share information. The emergence of IoT is due to advancements in the field of embedded systems, pervasive and ubiquitous computing. IoT devices interact directly with the physical world which means that the data can be large which is why the data is often processed via the cloud. Once the data is available on the cloud it is processed by applications that are designed with machine learning and data analytical algorithms. IoT devices come in many forms with varying applications and capabilities. For instance devices can be designed for health monitoring, fitness monitoring, home automation, industrial support, entertainment and gaming.

2.1 Wearable Technology

The IoT is composed of many different forms of devices. Some devices are mounted on a wall, some are designed to be carried while others are meant to be worn on the body. Wearable computing has been conceived to promote ubiquitous and pervasive computing. What sets wearable technology apart from conventional smart devices is the fact that wearable device are intended to be worn on the body and not carried. Given below are some application domains related to wearable devices.

Health monitoring – Devices that monitor the physiological signals of the wearer. These devices are worn on the body and can measure a range of body signals like EMG, EMI, ECG etc. Health monitoring devices are often embedded with MEMS sensors to provide features like fall detection in the elderly.

Fitness monitoring – Devices designed to be worn during physical exercise. Fitness monitoring devices are pedometer based devices equipped with MEMS sensors to compute distance covered, steps taken and calories burnt. Fitness monitoring devices also measure heart rate as an indicator of exercise.

Wearable devices are not just limited to health monitoring and fitness monitoring. Some wearable devices are worn during gameplay like head wearable displays that create an immersive environment. Similarly some devices assist users like wearable displays and devices that help with warehouse management, item tracking, location determination etc.

3. THREATS IN WEARABLE IoT DEVICES

Research[1] shows that IoT devices have three limitations that are a barrier to their wide adoption. The limitations are battery life, chipset limitation and design concerns. These limitations have an impact on how devices are designed and what services they offer. Owing to these limitations many essential services like cryptography are often ignored.

Healthcare wearable devices are a major innovation[2] in the field of IoT. Research[3] shows that IoT devices will revolutionize how healthcare services are provided. Wearable devices allow patients to be constantly monitored thus promoting point of care services. In the research authors have identified four challenges faced by wearable devices i.e. confidentiality, authentication, network security and a hostile environment.

A recent research [4]shows that authentication can be carried out by using bioelectrical impedance signals. The authors show that it is possible to use a Shimmer health sensor to authenticate a device wearer with 98% accuracy. The proposed system does not offer any other cryptographic service like confidentiality. Authentication alone is an incomplete cryptographic system and gives a false guarantee of security.

A recent research[5] shows that even widely marketed devices possess weaknesses. The authors study the fitness watch Fitbit and show that it possesses weaknesses. After reverse engineering the

tracker the authors show that the device transmits user credentials in plain text. It has also been demonstrated that any HTTP data processing takes place is in plain text. The Fitbit also possesses a weakness in which a physical exercise can be forged by simply attaching the device to the wheel of a moving vehicle.

Any system that possess cryptographic implementations are not immune from attacks. Research[6][7][8] shows that cryptographic keys can be attacked through various methods like brute force, cold boot attack, malware etc. Each form of attack exploits a certain element of the system which is why no single solution can guarantee a fool proof system. Attacks on cryptosystems and various forms of IoT devices creates a compelling case for a renewed security approach.

4. INTEGRATED CIRCUIT METRIC

Cryptographic algorithms rely on a widely published algorithm which means that the security is based on a secret key. To ensure that the system remains secure the cryptographic keys are kept secret. If stored cryptographic keys are captured then the entire system can be exposed. Owing to this reason cryptographers are constantly increasing key sizes. An increase in the key size only ensures that the keys are safe from brute force attack but does not entirely eliminate the possibility of cryptographic key theft. Research shows that cryptographic keys can be attacked in many ways and efforts to increase the key size are often inadequate. Cryptographic systems may also use algorithmic intractability to offer security. Algorithmic intractability cannot guarantee security which is why research is attempting to base a cryptographic implementation on novel roots of trust like Physically Unclonable Functions[9][10] and Integrated Circuit Metric.

The Integrated Circuit Metric (ICMetric) technology[11][12] is a novel approach for deterring key theft in cryptographic systems. The technology has two purposes first as a key theft deterrent and secondly as a basis for cryptographic services. The ICMetric technology proposes entirely eliminating stored keys from a system. To generate a key, unique measurable device features are obtained to create a device identity called an ICMetric. The security of the ICMetric technology lies in finding unique device hardware and software features which cannot be easily predicted by an adversary. The individual device features are extracted and processed to produce an identification for the device. The identification is called a device ICMetric and is used as a basis for key generation. Once the key is generated it is used for the provision of cryptographic services and then entirely discarded. Hence the keys are generated when required and discarded thereafter.

Previous researches [13][14][15] on ICMetric generation show that the ICMetric can be generated using the Program Counter (PC) and Cycles Per Instructions (CPI). The experiments have shown that unique features can be extracted using the PC and CPI but the concept has not been applied to smart devices and the IoT.ICMetric generation is composed of two steps i.e. the calibration phase and the operation phase. These phases are applied only when required after which the cryptographic keys and any associated data is discarded. Data related to the ICMetric or device features is never communicated even to trusted features. The two steps of ICMetric generation are as follows:

4.1 Calibration Phase

In the calibration phase suitable features are selected and readings are obtained by providing the required stimulus. The readings are used to establish frequency distributions and histograms for each feature. The frequency distributions are subjected to statistical analysis. This produces statistical credentials suitable for ICMetric generation.

4.2 Operation Phase

In the operation phase feature sets are established using statistical credentials. The individual feature values are combined to generate a unique ICMetric. The ICMetric is processed in a key generation algorithm to generate a cryptographic key.

4.2.1 Combining Features

The final ICMetric is computed by combining individual statistical credentials by either using the feature addition technique or the feature concatenation technique.

By using the feature addition technique, individual feature values are added to create a device ICMetric. The resulting ICMetric is highly diverse but lacks length.If F is a device feature then the device ICMetricunder the feature addition technique can be represented as:

$$icmetric = \sum_{i=1}^{n} F_i$$

If a longer ICMetric is required then the feature concatenation technique is suitable. Here the individual feature values are concatenated to produce a longer yet less diverse ICMetric. If || is the concatenation operator then the device ICMetric under the concatenation technique can be represented as:

$$icmetric = F_1||F_2||\cdots||F_n$$

5. MEMS BASED SENSOR FEATURES

The ICMetric of a device is based on unique device features. Hence the security of ICMetric lies on identifying features that are extractable by the legitimate owner of a device but not by an adversary. Device features can be explicit and implicit. The problem with using explicit features is that often they can be easily extracted by the adversary. For example the MAC address is a unique feature of a device but can be captured without much effort. An adversary can obtain the MAC address from the exterior of a device or even by using a network surveillance tool. This research demonstrates the ICMetric can be generated using the bias in a MEMS sensor.

Research shows that no two sensors are created alike[16]. Sensors made by a single manufacturer having the same design, material and manufacturing process will differ from each other considerably. These variations are beyond the control of the manufacturer and can be noticed in the readings obtained from the sensor. A common variation in MEMS sensors is an operational bias. This bias is introduced when a sensor is mounted onto the main board. When a sensor is being soldered onto the main board heat and pressure causes a slight deformation of the sensor. This deformation causes a bias in the sensor readings. There are other reasons[17] for the bias like operational temperature, wear of the sensor components and inconspicuous damage.Modern consumer wearable devices are embedded with MEMS sensors which enable them to offer a wide range of services. For instance many wearable devices are being embedded with an accelerometer, gyroscope, strain gauge sensors. These sensors enable the detection of inertial motions of the wearer of the device. Even though these sensors are designed as precision components; they do not possess the required perfection. This research shows that it is possible to use the MEMS bias to generate a device ICMetric.

6. FRAMEWORK ASSUMPTIONS

The proposed health sensing cloud application, details a system for ICMetric based IoT devices to guarantee a system that can assist in secure communication of patient data between the patient and doctor, while deterring all forms of key capture.

6.1 System Model

The proposed scheme is designed for all entities/devices which form part of the IoT healthcare network and have trust in the healthcare provider's server. The healthcare provider's server is responsible for controlling individual IoT devices in the network. The server enables IoT devices that have never had contact before to interact securely and confidentially. The following assumptions are made for the proposed scheme:

- The communication links between the server of the healthcare provider and IoT devices are all unprotected. Therefore, the data being transmitted over the communication channel should be protected.
- Each entity (sensor, device, etc.) that is part of the health monitoring application needs to be registered with the healthcare provider's server.
- The server is operated by the healthcare provider and is responsible for assigning all the network specific configurations to successfully join a network.Figure1 shows the high level system architecture of the proposed solution; connecting the patient and the health professional with the health care provider's server, and outsourcing the data storage and analysis functionality to the cloud service provider.

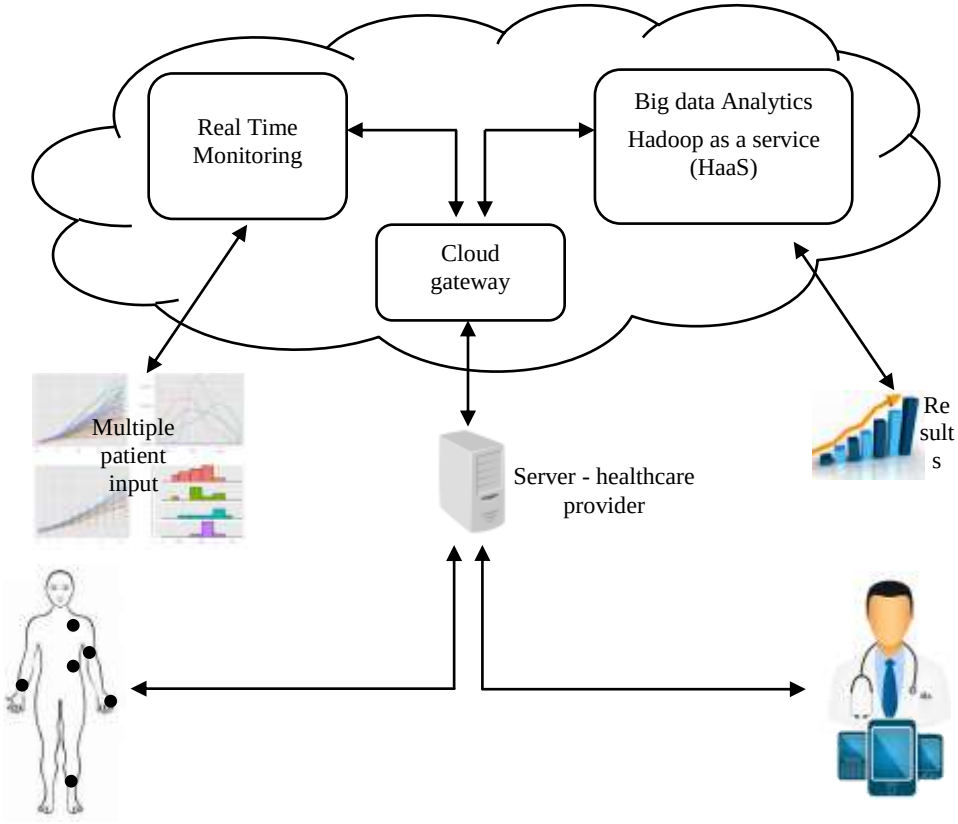


Figure 1. System architecture for the proposed secure IoT health care system

6.2 Adversary Model

Health care IoT comprise of dedicated devices that aim to sense and monitor data. The security of healthcare IoT devices has become particularly important, since the risk of health data theft has been recognized. Prevalence of attacks on healthcare systems; stakeholders like device manufacturers, administration agencies, health professionals and researchers have started paying extra emphasis on the implementation of security in healthcare IoT applications. A major threat facing healthcare IoT is the possibility of data leakage while it is being transmitted over the channel. Eavesdropping is a major threat to patient privacy, the adversary can easily read unencrypted messages being transmitted over the network. The captured messages can reveal important information to the attacker about the patient, which can pose a serious threat to patient privacy. Patient's data can be safeguarded from these attacks by employing proper security measures in the system that provide privacy to the sensed patient data.

6.3 Security Goals

Security and privacy issues have been described as the most challenging problems in health monitoring systems in IoT. The security of patient's health records has always been a major concern since the adoption of computers in the healthcare domain. There are several security and privacy challenges that healthcare IoT applications generally try to address, so as to secure the healthcare data in an application. The proposed secure health sensing system based on ICMetric, aims to fulfil the following security and privacy challenges:

Session Key Generation. A fundamental goal of the scheme is to generate strong ICMetric session keys. This goal ensures generation and use of keys with high entropy and adequate size, so that pre-computed attacks are not possible and keys are not brute-forced easily.

Confidentiality. A vital security goal of the scheme is to maintain confidentiality of healthcare data transmitted by the IoT devices.Preserving the secrecy of patient's health data is of utmost importance, so that the data is not leaked to adversaries.

Mutual Authentication. An essential security goal of the proposed scheme is to authenticate healthcare devices in the IoT. Authentication ensures that only authenticated devices are recognized at the server and any impersonating entities are eliminated at source. This goal ensures that only authenticated health professional, server and registered IoT devices can get access to the patient data.

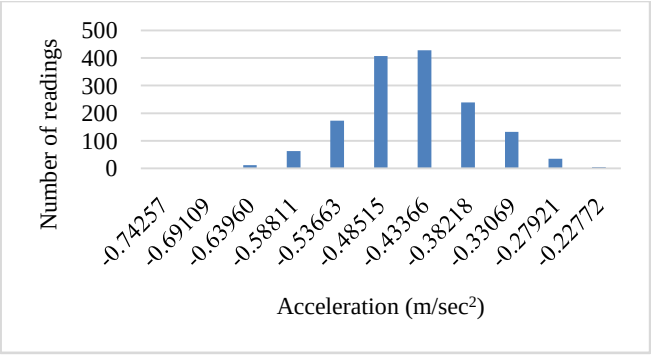
Integrity. A central goal of the proposed framework is to maintain integrity of data transmitted by the healthcare devices in the IoT. Integrity ensures that the manipulation of healthcare data by adversaries is detected at the recipient.

Availability. An important goal of the proposed framework is to ensure that the relevant data and information is available to the authorized health professional at all the times. Owing to this the framework has to be resistant to denial of service attacks from adversaries.

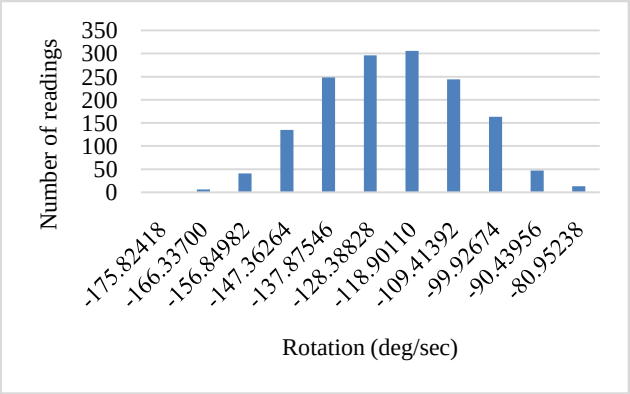
Analysis. Another key goal of the proposed framework is that the data collected from the different data sources can be aggregated and processed for the purpose of current and future medical research and analysis. This increases the usability and practicalityof the framework beyond its basic scope.

7. MEMS BIAS ESTABLISHMENT

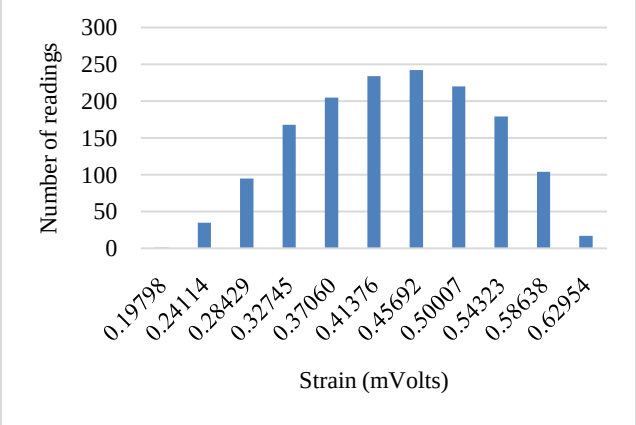
Study on MEMS sensors shows that the bias in a sensor can be used to create a device ICMetric. Experiments show that each sensor possesses a unique bias which can be recreated if the sensor is subjected to the same stimulus. To create the device ICMetric from a MEMS sensor a sensor testbed is assembled which is composed of six identical Shimmer sensors. The stimulus is created by leaving the sensor on a flat surface which is free from vibrations and movement. When subjecting the sensors to this stimulus then under ideal conditions the target sensors should sense no acceleration, rotation or strain.Experiments show that this is not the case and that the readings vary considerably. Owing to limitation of space a graph is provided for one axis of accelerometer, gyroscope and strain gauge. A total of 1500 sensor readings have been obtained to test the presence of a unique sensor bias. Unimodal distributions have been obtained for the six Shimmer sensors that form the testbed. Figure 2 shows graphs from a Shimmer accelerometer, gyroscope and strain gauge. The above graphs confirm that the response to a stimulus can vary from sensor to sensor. The unimodal distributions show that every sensor has an operational range within which the sensor responds. This operational range is unique to a sensor and cannot be predicted by an adversary. The MEMS bias is easy to recreate by the user of a device as there is no need for special instrumentation or actions required by the user. Also a user does not need to provide any form of input for establishing the sensor bias.



(a)



(b)



(c)

Figure 2. Unimodal distributions from a Shimmer sensor embedded with accelerometer, gyroscope and strain gauge.

Given in the table 1 are the statistical indicators for the above graphs. The statistical indicators confirm that each sensor has a different bias which differs from device to device and from axis to axis. Each statistical indicator confirms that the population behavior is unique for each sensor. Even if two statistical indicators are similar then other statistical indicators will differ to show the varying operations of each sensor. The analysis of variance (ANOVA) p-value confirms that there is significant difference between the sensor readings.

Table 1. Statistical indicators for the unimodal distributions from a Shimmer accelerometer, gyroscope and strain gauge

	Accelerometer	Gyroscope	Strain gauge
Mean	-0.43432	-127.81196	0.41427
Standard deviation	0.07083	16.48308	0.09056
Skewness	0.01077	0.02725	-0.07965
Confidence interval	-0.43791 to -0.43074	-128.6463 to -126.9775	0.40969 to 0.41886
Kurtosis	0.01234	-0.44354	-0.8269
p-value	0.00	0.00	0.00

8. ICMETRIC BASED SECURE TRANSMISSION PROTOCOL

The proposed security framework details an ICMetric centered cloud based health monitoring scheme. The proposed scheme is intended to improve the security of health monitoring applications by providing secure key generation, mutual authentication, confidentiality, integrity and availability of the health data in combination with the ICMetric technology.

The secure data transmission protocol is responsible for securely conveying the patient readings between the patient, health professional and the health organization's servers. The security protocol proposed here seeks to improve the security of health monitoring applications by providing secure admission control, authentication, confidentiality and integrity of the health data in combination with the ICMetric technology. The servers are responsible for controlling individual entities in the network. The servers enable entities that have never had contact before to interact securely and confidentially. The servers are operated by the healthcare provider and are responsible for assigning all the network specific configurations to successfully join a network. The following section details the steps involved in the secure functioning of the health monitoring cloud application based on the ICMetric technology:

8.1 Secure Admission Control

Key management and secure communication schemes are useful only if the IoT devices join the network through a secure admission process. The admission control scheme employed in the proposed secure transmission protocol is used only once when the device registers for the first time. The process is initiated when an IoT device requests to register by supplying necessary credentials. The device registration consists of the following unique activities.

- When an entity wishes to register with the server, its necessary credentials are forwarded to the health organization's server where the registration is digitized.
- Once the entity is registered, the server is updated with a unique identification and a 128 bit random per-entity value (called "salt").

8.2 Symmetric Cryptographic Module

This section provides the architectural details of the symmetric key cryptographic module in the protocol design. The symmetric cryptographic module provides security functionalities that facilitate secure transmission of data between the server and the IoT device. The symmetric cryptographic module automatically generates an ICMetric based session key between the sensor and the server, which is resilient to pre-computed attacks. The design of the proposed protocol is based on zero knowledge proof[18][19], which is coherent with the design principles of the ICMetric technology of not transmitting the device ICMetric. The proposed symmetric cryptographic module doesn't require the exchange of ICMetric information between parties for the purpose of authentication and key generation, neither does it require human intervention to work; the keys are automatically generated based on the ICMetric of the IoT device. The generated ICMetric symmetric keys are then used for securely communicating the data between the patient and the health professional. The process of symmetric key generation and authentication is carried out between the IoT device and the server to establish symmetric session key for secure data communication between the patient and the health professional.

To formally start the ICMetric based symmetric key generation process each registered sensor that wishes to communicate generates its own ICMetric. The entity ID is the identifying attribute for an entity assigned by the server at the time of registration. The $salt$ is generated by the server as a random number 128-bit number at the time of registration. The device generates its verifier v at registration time and sends it to server as

$$x = h(icmetric||salt||ID)$$
$$v = g^x mod\ n$$

where g is a generator of the multiplicative group and n is a safe prime.

The authentication process for the purpose of sending data readings to the server is initiated by the entity, when it sends an initiation request containing its ID to the server asking for the assigned salt value. On contacting the server, each sensor receives the salt stored on the server under its sensor ID. Now the sensor computes a based on its $icmetric$, the assigned $salt$ and ID.

$$a = h\,(icmetric||\,salt\,||\,ID) \quad (6)$$

and uses it to calculate verifier A for sending it to the server.

$$A = g^a\ mod\ n \quad (7)$$

The server does a similar operation to calculate b based on own salt, id and ICMetric value

$$b = h\,(icmetric_s||\,salt_s\,||\,ID_s) \quad (8)$$

Then the server calculates B and also adds the public verifier to it and sends B to the sensor.

$$B = (kA + g^b)\ mod\ n \quad (9)$$

Where $k = h(N||g)$

Both sides compute a random scrambling parameter $u = h\,(A \,||\, B)$ based on the exchanged A and B. So both sides can now construct the shared session key. The sensor constructs it as follows:

$$K_A = (B - k \cdot v)^{a+ux} \; mod\; n \tag{10}$$

The server constructs it as follows

$$K_S = (A \cdot v^u)^b \tag{11}$$

Both sides now possess the same secure session key K based on the respective formulae.

To complete the authentication, now the sensor needs to prove to server that its key is identical. In order to do so, the sensor constructs the message M_1 and sends it to the server,

$$M_1 = h\,(\,N \,||\, g \,||\, ID_A \,||salt_A \,||\, A \,||\, B \,||\, K_A\,) \tag{12}$$

The server will calculate M_2 using its own K_S and compare it against the message received from the sensor. If both keys don't match, the authentication fails resulting in refusal of communication request. If the sensor request is authenticated, the data can safely be relayed to the server. After an entity is authenticated and joins the network, its session key is kept in a secure cache and is valid for a set time period. The same process is carried out between the server and the doctor for the establishment of an ICMetric session key.

8.3 Confidentiality and Integrity Module

Once the session key is in place, secure communications can be carried out using any recognized symmetric key algorithms such as AES, 3DES. In the design, AES[20]is used to securely send health data between the entities and KGC. In this step, the designintegrates all the individual ICMetric based components with the symmetric encryption/ decryption scheme to achieve data confidentiality between the parties. This module performs encryption/ decryption and checks the integrity of the transmitted data based on AES-HMAC.

9. CLOUD STORAGE, PROCESSING AND ANALYSIS

All the data required for high-availability real-time monitoring of patients or required as input to data analysis algorithms, is transferred to the Cloud Gateway. The Cloud Gateway is a customised virtual machine that acts as an entry-point for the data into the cloud environment, as well as performing the job of middleware between the real-time monitoring and data analysis components of the framework. It also ensures that the data is stored and transmitted securely while it is being hosted in the cloud environment. To achieve the secure storage goal, it uses the data-at-rest encryption features, that have recently been offered by some cloud service providers [21], which allow the users of the cloud service to encrypt their data on cloud with their own encryption keys [22]. To achieve the secure transmission goal, it makes use of the Inter-Cloud Virtual Private Network (ICVPN) solution [23], which allows the users of the cloud service to establish dynamic and encrypted communication tunnels between their virtual machines running the cloud environment.

In order to cater for the system goal of availability of the data, the Cloud Gateway again make use of the cloud's scaling capability to dynamically increase both the number and processing capability of the virtual machines that constitute the Real-time Monitoring component of the framework [24][25]. This allows the framework to be able to keep up with the demands generated by the users at run-time and send the status and notification about the patients to the healthcare providers in a timely manner.

For achieving the system goal of long-term data storage and analysis, the Cloud Gateway is able to communicate and interact with a number of Hadoop [26] based data analysis services from different cloud platforms [27]. The data relevant for this purpose is sent to the analysis services and algorithms and the subsequent reports and results are shared with the healthcare professionals.

10. IMPLEMENTATION AND EVALUATION

The working prototype of the proposed health sensing cloud framework has been implemented using C. The scheme has been implemented on a first generation Intel Corei3 3.2 Ghz processor with 6 GB RAM. The ICMetric secure transmission protocol has been implemented using the CyaSSL[28] and OpenSSL[29] cryptographic library. The design principles of the proposed secure cloud based health sensing framework for IoT devices has coherence with the ICMetric technology. The proposed framework has been evaluated by measuring the RAM consumption and running time for carrying out secure communications between the patient, health professional and the server based on 256 bit ICMetric keys.

The evaluation of the running time of the ICMetric based health sensing framework is done using the programs runtime itself, whereas the memory consumed is evaluated using Valgrind[30][31]. The Valgrind results for memory evaluation; measure the memory consumed during the program's lifetime and is represented in terms of useful heap, extra heap, total heap and stack.

10.1 Running time Performance of ICMetric Secure Transmission Protocol

This section evaluates the performance of the ICMetric Secure transmission protocol. Simulation results confirm that the ICMetric technology can be used to enhance the security of IoT systems with minimum impact on resource demand. It is evident from the table 2 that the running time for the generation of ICMetric based session key is 0.0035 seconds, which proves that the proposed scheme is able to provide session key generation at very minimal amounts of time consumption.

Table 2. Running time for generation of ICMetric based session key

Key size	256 bit
Time taken	3576 microseconds

The time performance of the confidentiality and integrity module that is responsible for carrying out the encryption / decryption of a data block using the ICMetric session key also needs to be assessed. Figure 3is a graph in which the 128 and 256 bit AES-HMAC key variants are compared with the time taken. It is evident from the graph that an increase in the key size has a slight change on the time performance of the application. Therefore the proposed scheme is able to provide secure communications without substantial time performance overheads.

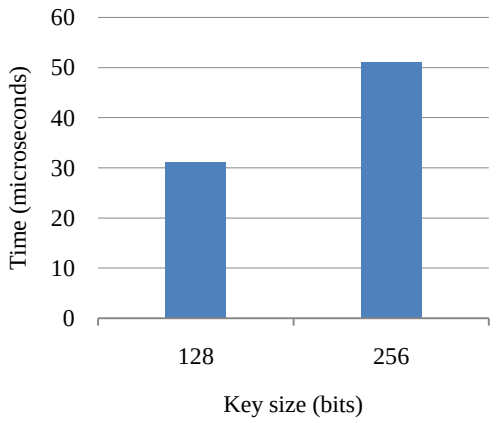


Figure 3. Running times for ICMetric based AES-HMAC.

10.2 RAM Consumption of the ICMetric Secure Transmission Protocol

Studying the scheme with reference to memory demand is also a necessary task. Once again, a 128 bit ICMetric is used as input for testing the prototype. The memory performance of the ICMetric secure transmission protocol is analyzed using Valgrind. The generated graphs depict memory profile of the protocol by presenting the program lifecycle and the memory (bytes) consumed.

Figure 4 presents a memory profile graph for mutual authentication and session key generation of 256-bit ICMetric key. It is evident from the graph that the maximum total memory consumed for session key generation and authentication using 256-bit key is around 9 KB, which is very suitable for resource constrained devices. This proves that the proposed scheme is able to provide high levels of security at the cost of very small amount of memory.

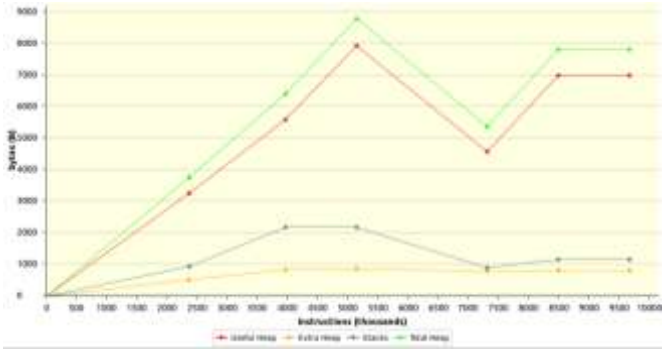


Figure 4. RAM consumption for 256-bit ICMetric session Key.

The figure 5 shows a memory profile graph for the 256-bit AES encryption/ decryption using ICMetric session key. It is evident from the graph that the maximum total memory consumed for encryption/ decryption using 256-bit key is 3.8 KB, which is again very suitable for resource constrained devices. This proves that the proposed scheme is able to provide high levels of security without much impact on memory demands.

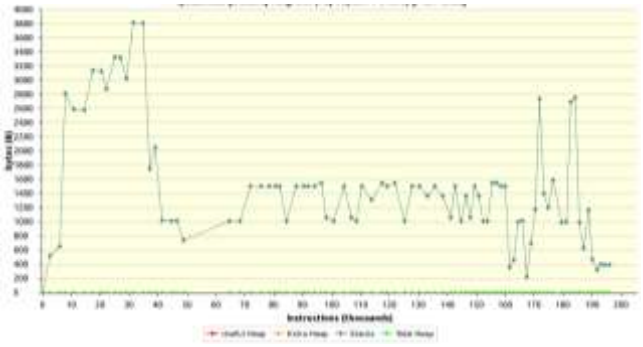


Figure 5. RAM consumption for ICMetric based 256-bit AES-HMAC

11. SECURITY ANALYSIS

The cloud based secure ICMetric health monitoring framework combines the security advantages of ICMetric and security properties of the designed symmetric framework for the generation of a strong session key between the patient and the health specialist. No entity in the application relies on stored passwords. They rather generate their ICMetric value at runtime, this safeguards the device from device capture attacks. A major advantage of using ICMetric for our health monitoring application is that all the security is provided based on the ICMetric based keys, therefore at no point is there a need for human intervention. This is particularly important from the patient's point of view since human intervention is not always possible for authentication, therefore the authentication functionality is carried out based on a device ICMetric.

Each device concatenates its ICMetric with a random per-user value (salt) and stores the hash value of the result along with the salt. This makes certain kinds of brute-force attacks, rainbow table attacks and dictionary attacks more difficult. The security features of our design also prevent the possibility of man in the middle attack. If there is a man-in-the middle attack, the sending and receiving parties are not able to generate the same session keys resulting in a failed authentication rejection decision by the server.

For the authentication of each entity's device our scheme is based on the mixing of the salt value from the server with the ICMetric of each device, and hashing it to produce a value that can be used for authentication of each entity's device. This feature ensures authenticity/ identification of participating entities and also assures the origin of information; since only entities that have been assigned a salt value from the server can communicate with other entities in the network. This feature helps ensure that all the sensors allocated to a patient are registered under his/her identification. The scheme ensures that the health professional who receives the triggered data is also registered. This enables only specific authenticated medical specialists to receive the data.

To generate the symmetric key, the generating entity/ device must have the knowledge of the assigned salt value and must then generate its ICMetric. Knowing only one of them does not allow the generation of symmetric key. This safeguards the network from attackers, since only authenticated entities that have been registered/ assigned a salt by the server can form part of the symmetric key generation process. The symmetric session key is valid for the duration of session, this also prevents the application from brute force attacks, since the key is only valid for a session. Each of the sensors sends a trigger to the server which forms a single packet of all the three sensor readings to send to the health

specialist. This provides obvious efficiency advantages since only a single block of encrypted health data is sent to the health specialist. The cloud based storage and analysis component of the framework ensures that the health data is always available to the health professional. This safeguards the health monitoring system from DoS attacks and also provides summarized results of the patients data to the health professionals for decision making.

12. CONCLUSION

Wearable healthcare devices have revolutionized the way in which healthcare is delivered. With the advent of wearable computing it has now become possible to deliver healthcare beyond the confines of the hospital. A vast benefit of such arrangements is a reduction in the health costs while patients enjoy improvement in healthcare and comfort. While there are many advantages of monitoring a person's health remotely a major hurdle with this healthcare model is the provision of security. Attacks on healthcare systems are a global occurrence that has become a leading source of concern. Attackers attempt to attack healthcare systems with an intention of stealing data so that it can be used for a range of purposes like medical identity theft and prescription theft. A patient's health can be monitored by using both invasive and noninvasive sensors/ devices. Devices like pacemakers can be implanted into a patient's body while other variants can also function externally. Similarly there are sensors that monitor a person's vital signs like breathing, heart rate and body temperature at regular intervals. Since these sensors monitor a person's physiological responses therefore it is imperative to secure the device, data, patient and health professional in a resource efficient but comprehensive manner.

A cloud based ICMetric patient monitoring system is presented in this paper. The proposed scheme effectively combines the functionalities of ICMetric based secure transmission protocol for providing mutual authentication, integrity and confidentiality of data in a resource efficient manner. The proposed security architecture is able to prevent most threats related to secure communication of health data, while considering the constraints that embedded systems demand. The design decisions of proposed framework makes it particularly suitable for resource constrained environments, which require elimination of computationally expensive and resource intensive operations while providing the required security. The cloud based secure health monitoring framework addresses the need for secure remote monitoring of patients by providing secure access control, authentication and confidentiality of the transmitted triggers to the health professional. The security analysis and implementation results of the scheme make it evident that the proposed framework is very suitable for health monitoring applications in terms of security and resource consumption.

We have also shown how the proposed framework can be extended to utilize the benefits of cloud computing while still not compromising on the security of the data. Cloud's scalability and distributed data processing capabilities have been harnessed in the framework's design to cater for the availability and data analysis objectives, while existing cloud security features have been integrated with the framework's core ICMetric based security components in order to share the benefits of both domains.

The future plan of this work is to evaluate the proposed scheme through experiments and analysis on real cloud environments, thus benchmarking the results against existing schemes that provide security in resource constrained environments.

13. REFERENCES

[1] V. Morabito, "Wearable Technologies," in *The Future of Digital Business Innovation*, Cham: Springer International Publishing, 2016, pp. 23–42.

[2] J. Hofdijk, B. Séroussi, C. Lovis, F. Sieverink, F. Ehrler, and A. Ugon, Eds., "Transforming Healthcare with the Internet of Things," in *Proceedings of the EFMI Special Topic Conference 2016*, 2016.

[3] J. Lindström, "Security challenges for wearable computing a case study," in *4th International Forum on Applied Wearable Computing (IFAWC)*, 2007.

[4] C. Cornelius, R. Peterson, J. Skinner, R. Halter, and D. Kotz, "A wearable system that knows who wears it," in *12th annual international conference on Mobile systems, applications, and services - MobiSys '14*, 2014, pp. 55–67.

[5] M. Rahman, B. Carbunar, and M. Banik, "Fit and Vulnerable: Attacks and Defenses for a Health Monitoring Device," 2013.

[6] D. Genkin, L. Pachmanov, I. Pipman, A. Shamir, and E. Tromer, "Physical key extraction attacks on PCs," *Communications of the ACM*, vol. 59, no. 6, ACM, pp. 70–79, 23-Jun-2016.

[7] J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felten, "Lest We Remember: Cold-Boot Attacks on Encryption Keys," *Communications of the ACM*, vol. 52, no. 5, ACM, p. 91, 01-May-2009.

[8] I. Kizhatov, "Physical Security of Cryptographic Algorithm Implementations," Universite Du Luxembourg, 2011.

[9] D. Merli and R. Plaga, "Physical unclonable functions: devices for cryptostorage," in *Proceedings of the 3rd international workshop on Trustworthy embedded devices - TrustED '13*, 2013, pp. 1–2.

[10] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *Proceedings of the 9th ACM conference on Computer and communications security - CCS '02*, 2002, p. 148.

[11] S. Tahir and I. Rashid, "ICMetric-Based Secure Communication," in *Innovative Solutions for Access Control Management*, vol. 36, IGI Global, 2016, pp. 263–293.

[12] E. Papoutsis, "Investigation of the Potential of Generating Encryption Keys for ICMETRICS," University of Kent, 2009.

[13] X. Zhai, K. Appiah, S. Ehsan, H. Hu, D. Gu, K. McDonald-Maier, W. M. Cheung, and G. Howells, "Application of ICmetrics for Embedded System Security," in *2013 Fourth International Conference on Emerging Security Technologies*, 2013, pp. 89–92.

[14] Y. Kovalchuk, H. Hu, D. Gu, K. McDonald-Maier, D. Newman, S. Kelly, and G. Howells, "Investigation of Properties of ICmetrics Features," in *2012 Third International Conference on Emerging Security Technologies*, 2012, pp. 115–120.

[15] Y. Kovalchuk, K. McDonald-Maier, and G. Howells,

"Overview of ICmetrics Technology – Security Infrastructure for Autonomous and Intelligent Healthcare System," *Int. J. u- e- Serv. Sci. Technol.*, vol. 4, no. 3, pp. 49–60, 2011.

[16] M. Bhushan and M. B. Ketchen, "Variability," in *CMOS Test and Evaluation*, New York, NY: Springer New York, 2015, pp. 201–239.

[17] D. J. Fonseca, M. Sequera, D. J. Fonseca, and M. Sequera, "On MEMS Reliability and Failure Mechanisms," *Int. J. Qual. Stat. Reliab.*, vol. 2011, pp. 1–7, 2011.

[18] T. Wu, "The Secure Remote Password Protocol," in *Proceedings of the Symposium on Network and Distributed Systems Security NDSS 98*, 1998, vol. 4, pp. 97–111.

[19] T. Perrin, T. Wu, N. Mavrogiannopoulos, and D. Taylor, "Using the Secure Remote Password (SRP) Protocol for TLS Authentication," 2007.

[20] S. Gueron, "Intel Advanced Encryption Standard (AES) New Instructions Set," 2012.

[21] Google, "Encryption at Rest in Google Cloud Platform," 2016.

[22] Google Cloud Platform, "Supplying Your Own Encryption Keys," 2016. [Online]. Available: https://cloud.google.com/storage/docs/gsutil/addlhelp/SupplyingYourOwnEncryptionKeys. [Accessed: 05-Dec-2016].

[23] A. Sajjad, M. Rajarajan, A. Zisman, and T. Dimitrakos, "A scalable and dynamic application-level secure communication framework for inter-cloud services," *Futur. Gener. Comput. Syst.*, vol. 48, pp. 19–27, 2015.

[24] Google, "Google Cloud Load Balancing," 2016. [Online]. Available: https://cloud.google.com/load-balancing/.

[25] W.-H. Liao, S.-C. Kuai, and Y.-R. Leau, "Auto-scaling Strategy for Amazon Web Services in Cloud Computing," in *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*, 2015, pp. 1059–1064.

[26] H. Lu, C. Hai-Shan, and H. Ting-Ting, "Research on Hadoop Cloud Computing Model and its Applications," in *2012 Third International Conference on Networking and Distributed Computing*, 2012, pp. 59–63.

[27] Amazon Web Services, "Amazon EMR Developer Guide."

[28] WolfSSL, *CyaSSL User Manual*. 2014.

[29] J. Viega, M. Messier, and P. Chandra, *Network security with OpenSSL*. O'Reilly, 2002.

[30] "Valgrind Documentation," 2016.

[31] M. Wolff, "Massif-Visualizer Memory Profiling UI," 2011.