Journal of Fundamental and Applied Sciences

ISSN 1112-9867

Available online at http://www.jfas.info

Research Article

Special Issue

ICMAPEN: AN ICMETRIC BASED SECURITY FRAMEWORK FOR SLEEP APNEA MONITORING

R. Tahir[1,*], H. Tahir[1], A. Sajjad[2], K. D. Maier[1]

[1]University of Essex, Colchester, United Kingdom

[2]British Telecom Ltd, Adastral Park, Ipswich, United Kingdom

Published online: 24 November 2017

ABSTRACT

Smart devices are becoming increasingly powerful which is why they are being used for point of care health services. Wearable devices can be purchased which allow continuous monitoring of a wearers vital signs. The data is generated, processed and stored remotely where it can be readily accessible to health professionals. Recent attacks on healthcare systems and health data shows that the systems are insecure and that security is a major hurdle in their wide adoption. Conventional cryptographic systems rely on stored keys for the provision of security. The stored keys can be captured in many ways which leads to the system being exposed. The ICMetric technology remedies this by eliminating the need for stored keys. Thus, the ICMetric technology functions as a key theft deterrent and as a basis for cryptographic services. This paper studies the design and implementation of an ICMetric based health monitoring system for people diagnosed with sleep apnea. The proposed system provides key generation, authentication and confidentiality by using the novel ICMetric technology. The proposed scheme is constituent of a cloud computing component which enables remote monitoring and data storage for access by health professionals.

Author Correspondence, e-mail: rtahir@essex.ac.uk

doi: http://dx.doi.org/10.4314/jfas.v9i7s.50

This paper studies the performance of the proposed schemes by studying the running time. The security of the scheme has also been studied to show that the system provides high levels of security without resource compromise.

Keywords: ICMetric; Sleep apnea; Cloud computing; Authentication; Confidentiality

1. INTRODUCTION

Attacks on healthcare data and healthcare systems is not a new occurrence. Recent ransomware attacks on computation systems has infected more than 200,000 individuals and 300,000 computation systems. Rapid developments in healthcare has resulted in the creation of devices which can be worn on the body for continuous health monitoring. Many of these devices measure and forward physiological data of a patient to remote servers where it is accessible to health professionals.

Elderly and persons with long term illnesses are now opting for point of care services so that their health can be monitored from the comfort of their home. Although these systems are still undergoing development a major concern in their wide adoption is security. Health monitoring devices operate in the physical world while the data they capture is processed virtually. Hence the boundaries between the physical world and the virtual world have greatly diminished thus the importance of strong security provisions cannot be denied. Body wearable health devices measure, process and forward necessary physiological data hence privacy, confidentiality, integrity, etc. need to be ensured.

Conventional cryptographic system relies on the use of stored keys for the provision of security. If these keys are compromised, then the entire system can be broken. Research has shown that there are multiple and diverse methods of compromising a system. Hence a renewed approach is needed that eliminated the need for stored keys for the provision of security. This paper studies the Integrated Circuit Metric (ICMetric) technology as the basis for a range of cryptographic services which can be used for ensuring security in body wearable healthcare systems. The ICMetric technology is a novel trust basis which has two functions i.e. as an alternative to stored keys and as the basis for cryptographic services. This paper has studied the integration of ICMetric technology for improving health monitoring in patients with sleep apnea.

This paper presents the design and implementation of a secure health monitoring system for patients with sleep apnea. The proposed system uses the ICMetric technology for the provision of security. A combination of RSA and ICMetric technology is a novel concept that promises higher levels of security without excessive resource demand. The system is a cloud based solution where the physiological data is placed by the health device. This data is accessible to the health professional for real time health monitoring.

The remainder of this paper is structured as follows; section 2 discusses sleep apnea and the importance of health monitoring applications for monitoring of patients. Section 3 discusses in detail the ICMetric technology with its design principles, along with a detailed study on how the ICMetric can be generated using MEMS sensor bias. Section 4 highlights the fact that threats on wearable IoT systems have led to security based design goals for sleep apnea monitoring applications. In section 5, details of ICMApen are presented with focus on admission control and asymmetric key generation, confidentiality and cloud storage. Section 6 focuses on the simulation and results of ICMApen, concluding with a discussion on the security advantages of the design. The paper concludes in section 7 with a summary of findings and directions for future work.

1.1. Sleep Apnea

A medical condition which is being monitored in the point of care setting is sleep apnea. The condition is a form of chronic sleeping disorder caused by shallow or infrequent breathing while a patient is sleeping. Conclusive studies have shown that sleep apnea is accountable for symptoms like day time sleepiness, cardiac arrhythmia, systemic hypertension, myocardial infarctions and sudden cardiac death. There are three types of sleep apnea which are recognized by complete or nearly complete cessation of airflow. Episodes of sleep apnea can occur many times in a single night or may not occur for many nights. It has been estimated that there may be 5-30 individual episodes of sleep apnea in a single hour. Major indicators of sleep apnea are cardiac rhythm abnormalities, reduction in the blood oxygen saturation levels and chest volumes. Detecting the occurrence of an episode of sleep apnea does not require extensive equipment.

Under normal circumstance a person who has not consumed alcohol will have 96-97% blood oxygen saturation. Owing to the effect of altitude on oxygen saturation, specific oxygen

desaturation indexes have not been standardized. It is generally believed that blood saturations around 90% are considered mild. Ranges between 80% - 89% are classified as moderate while readings below 80% are classified as severe.

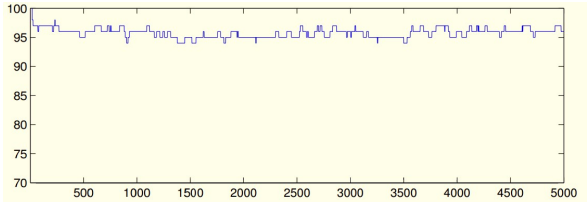

Fig.1. Oxygen saturation graph for a subject without sleep apnea. The oxygen saturation has an approximate range of 95% - 97%.

Figure 2 shows the oxygen saturation in a subject with no history of sleep apnea. While figure 3 shows the oxygen saturation in a subject suffering from sleep apnea. The fluctuation in the graph is an indication of the relationship between sleep apnea and blood oxygen saturation. There are limited medications which have shown much success in the treatment of sleep apnea. A method for treating sleep apnea is through wearable body sensors that can monitor a patient while he is asleep. Persons with sleep apnea can be monitored by using body sensors that can detect the heart rate, chest volume (respiration force) and blood oxygen concentration over the period of sleep.

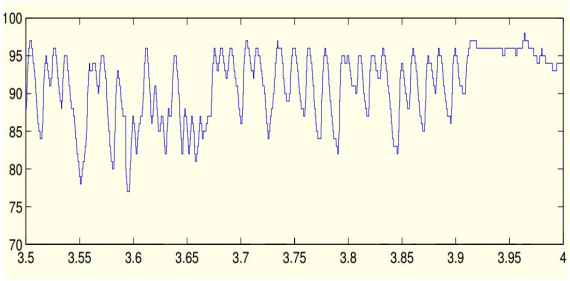

Fig.2. Oxygen saturation graphs for a subject with sever sleep apnea. The oxygen saturation fluctuates frequently between 77% and 97%.

These three physiological readings are considered strong indicators hence they can be individually and collectively used for the identification of persons who are experiencing sleep apnea. Perhaps the greatest advantage of this pervasive technology is the generation of an alert if a person is having difficulty breathing during/ after an episode of sleep apnea.

1.2. Integrated Circuit Metric (ICMetric)

Cryptographic algorithms base their design on intractability for the provision of security. Research has shown that attackers can attack a system without compromising the algorithmic design. Thus, a novel root can improve the security of cryptographic algorithms by eliminating weaknesses and flaws in the existing system.

Cryptographic algorithms are made public while the keys are kept secret to ensure security. If the keys are compromised, then the system is also compromised. As the cryptographic keys are stored therefore they are always at risk of being captured by attackers. The ICMetric technology [1] is an effort to resolve issues associated with stored keys by using features of a device to generate a device identity called the ICMetric. The ICMetric of the device is used as the basis for key generation and then confidentiality services. The ICMetric of a device is generated when required and discarded after use. Thus, for an attacker the ICMetric or its associated keys are not available on the system. The strength of the ICMetric technology lies in using features that are difficult to predict and recreate. Thus, the ICMetric technology processes features more complex than the conventional MAC addresses and IP addresses.

The ICMetric technology is unique in its design because it adds an extra layer of protection to the traditional cryptographic development suite. Thus, the ICMetric technology has been designed as an addon layer that promotes pluggability and design integration. Even though the ICMetric technology has been conceived as a pluggable technology it possesses properties which need to be observed. An important property that needs to be observed is that the ICMetric of a device is never communicated. Every device with the same environment, settings, operating system etc should have its own unique ICMetric. Thus, the stability and practicality of the ICMetric technology lies in choosing features that are truly unique to a device.

Extensive work [1] on the ICMetric technology has shown that the features of a device can be used as the basis for cryptographic key generation. Previous research [2] has also investigated suitable features for the generation of the ICMetric. Our previous research on MEMS sensors found in many modern wearable devices has shown that there is a bias in MEMS sensors. This bias is unique to each sensor and cannot be recreated even by the manufacturer. Detailed experiments and statistical analysis of sensors found in the body wearable Shimmer sensor

has shown that the bias in every sensor axis is unique and unpredictable. The findings of the study are not limited to the Shimmer sensor. It is a well-established fact that no two sensors are manufactured alike. Thus, the same methodology can be applied to any device that is embedded with either an accelerometer, gyroscope or a strain gauge sensor. Most modern health monitoring devices are now equipped with an accelerometer and a gyroscope. These two sensors are used to enable motion detection, fall detection etc. Many modern smart devices cannot provide the wide range of available services without the help of an accelerometer and gyroscope sensor.

Besides using MEMS sensor bias our previous research [2] has also shown that the ICMetric of a device should also incorporate explicit features like calibration matrices, MAC addresses, device ID's, serial numbers etc. By combining implicit and explicit features the uniqueness and unpredictability of the device ICMetric can be insured.

1.3. Security Goals

Prevalence of attacks on healthcare systems have made the stakeholders very particular about incorporating security in healthcare IoT applications. ICMApen aims to address these security concerns by proposing a secure fully functional ICMetric based sleep apnea monitoring system.

A fundamental goal of ICMApen is to generate an ICMetric asymmetric key pair. Fulfilling this goal means having keys with high entropy and adequate size to deter key guessing attacks on ICMetrics.

An essential security goal of ICMApen is to authenticate user sensors and the health professional, without the actual transmission of the ICMetric number.

A vital security goal of ICMApen is to maintain confidentiality of the sleep apnea readings. This data collected from the sensors can be aggregated and processed for current and future medical analysis. This increases the usability and practicality of ICMApen beyond its basic scope.

An important goal of ICMApen is to ensure that the sleep apnea data and information is available to the authorized health professional at all the times. Owing to this the framework must be resistant to denial of service attacks from adversaries.

1.4. ICMApen Design

Our proposed security framework details an ICMetric based health monitoring scheme for patients with sleep apnea, referred to as ICMApen. ICMApen is an idea to improve the security of sleep apnea monitoring applications, thereby providing authentication and confidentiality of the monitored health readings on the cloud. Figure 3 shows the ICMApen general system architecture connecting the patient, the cloud and the health professional. The following section details the steps involved in the secure functioning of our sleep apnea monitoring application based on ICMetric:

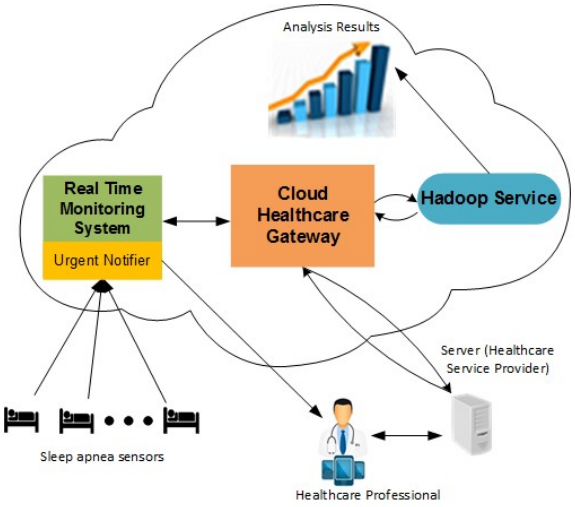

Fig.3. System architecture for the proposed ICMApen

1.5 ICMetric Number Establishment

The proposed architecture is based on the use of sensors that are wearable on the human body, as clearly depicted in the system architecture shown in figure 3. To extract physiological readings, we propose the use of three individual sensors that can be used with Arduino or Arduino compatibles. The pulse rate can be extracted using the Amped sensor. This is a plug and play sensor powered by a 3 volt or a 5 volt Arduino that can be worn on the earlobe or the finger. The chest volume is an indicator of pulmonary ventilation which can be measured by sensors that measure the movement of the chest. These sensors are mostly in the form of a band that is worn around the ribcage under the armpits. The sensors can measure the respiratory excursions of the body non-invasively. The determination of peripheral capillary oxygen saturation (SpO_2) is measured with the help of an oximetry device. We propose using an

earlobe based Nonin pulse oximeter that can be easily interfaced with Arduino. The extracted ICMetric key from each sleep

1.6 Secure Admission Control

The requirement and importance of secure admission control is obvious as key management and secure communication schemes are effective only after the devices join the network in a secure admission process. The registration process is composed of a sub process where all the sensors allocated to a patient will be recorded on the database. The server maintains the identification of all the sensors assigned to a patient. This sensor identification is crucial in authenticating the patient. Each sensor that is part of the network generates an ICMetric basis number (icm) based on the extracted feature values. The ICMetric basis number of each registered sensor is used by the server to compute and store:

$$h = hash(icm + s) \quad (1)$$

Where icm is the ICMetric basis number of the sensor and s is the salt value assigned to the patient.

1.7 Confidentiality

ICMApnea uses the RSA [3] algorithm to transmit the patient sleep apnea readings in encrypted form to the cloud and the health professional. It uses the ICMetric of the patient's sensor along with the RSA algorithm to generate a strong public-private key pair. The communication between the patient and the health professional does not happen repeatedly, only urgent events/ triggers are communicated so that the professional can take a timely action. In our situation, a trigger would be a person experiencing a certain number of apnea episodes in an amount of time, as depicted by the urgent notifier in the figure 3. Other triggers can also include health factors like irregular heartbeats or a limited chest volume, that would instantly send a signal via the urgent notifier to the health professional. Having a trigger based monitoring system removes the need for constant observation of the subject.

1.8 Cloud Storage

All the sensor data from the monitored sleep apnea patients is gathered by the Real-Time Monitoring Service [4] that is deployed on the Cloud. The monitoring service allows for setting of notification policies that are enforced by the Urgent Notifier component, so that in

case of abnormal or anomalous readings from a sensor, urgent notifications can be sent directly to the healthcare professionals; bypassing the normal flow of the system. Under normal operations, the data required as input to data analysis algorithms is transferred to the Cloud Healthcare Gateway (CHG), which processes it and sends it to the Hadoop cluster. The CHG is a customised virtual machine that acts as the entry and exit point for the data into and out of the Cloud environment, as well as performing the job of a middleware between the real-time monitoring and data analysis components of the framework.

The CHG 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, we use its data-at-rest encryption features, that have recently been offered by some Cloud Service Providers [5], which allow the users of the Cloud service to encrypt their data on Cloud with their own encryption keys [6]. To achieve the secure transmission goal, we make use of the Inter-Cloud Virtual Private Network (ICVPN) solution [7], which allows the users of the Cloud service to establish dynamic and encrypted communication tunnels between their virtual machines running on the Cloud environment.

In order to cater for the system goal of availability of the data, the Cloud Gateway again makes 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 [4][8]. 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.

2. RESULTS AND DISCUSSION

We implement the working prototype of ICMApen using C on Linux. The implementation of the working prototype is done using OpenSSL and cyassl library. These lightweight libraries have been used to boost the performance of our scheme. The key generation module of the ICMApen implementation takes as input a 128 bit ICMetric number, which is fed to the RSA cipher for the communication of encrypted sleep apnea patient readings.

2.1 Results

The efficiency of ICMApen is evaluated based on the running time of the prototype. Simulation results confirm that the ICmetric technology can be used to enhace the security of sleep apnea monitoring systems with minimum impact on resource demand. It is evident from the figure 4, that the running time for the generation of ICMetric based RSA key is around 1 millisecond, which proves that the proposed scheme can provide ICMetric-RSA key at very minimal amounts of time consumption.

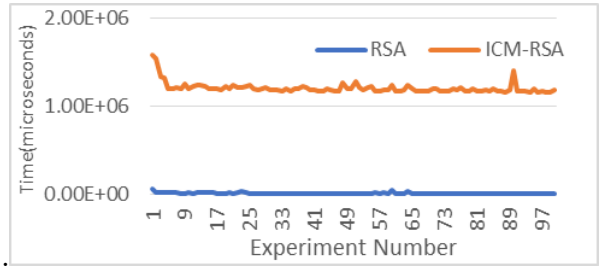

Fig.4. Execution time comparison of the RSA key generation with extended RSA key generation for a 1024 bit key

The time performance of the confidentiality module that is responsible for carrying out the encryption / decryption of a data using the ICM-RSA key is assessed in figure 5. The time taken for ICMetric based encryption/decryption operation is compared against the time taken by standard RSA encryption/decryption. It is evident from the graph that the ICMetric key has a change on the time performance of the application. Therefore, the proposed scheme can provide secure communications without substantial time performance overheads.

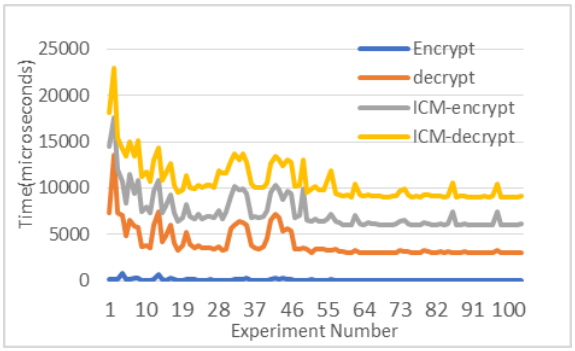

Fig.5. Execution time comparison of RSA encrypt/decrypt with ICMetric-RSA encrypt/decrypt using a 1024 bit key

2.2 DISCUSSION

ICMApen framework combines the security advantages of ICMetric and security properties of the designed ICM-RSA encryption/decryption between the patient and the health professional. 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 RSA-ICM 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 asymmetric 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 asymmetric key generation process.

The cloud based storage and analysis component of the framework ensures that the health data is always available to the health professional and urgent timely readings are sent in case of emergencies. The Hadoop component safeguards the health monitoring system from DoS attacks and provides timely summarized results of the patient's data to the health professionals for decision making.

3. CONCLUSION

Health monitoring using smart wearable devices is now recognized as a promising method of administering healthcare. Patients are now able to opt for health services without leaving the comfort of their home. Devices are available which can be worn on the body for continuous health monitoring. Even though these devices are being manufactured and sold many lack security provisions. Recent attacks on healthcare systems and healthcare data is a testimonial to this fact. Attackers can exploit weaknesses in cryptographic implementations to gain access to a system. One such weakness is cryptographic key theft.

Traditionally, cryptographic algorithms have relied on stored keys for the provision of security. Research has shown that stored keys can be attacked through various methods. A recent development which aims to solve this problem is the ICMetric technology. This technology eliminates the need for stored keys as they are generated when required and discarded thereafter. The key is generated using the features of a device. Thus, the ICMetric technology is a key theft deterrent and a basis for cryptographic services.

This paper presents the design and implementation of a secure health monitoring for people with sleep apnea. The proposed system is based on the novel ICMetric technology and provides key generation, authentication and confidentiality services without the need for stored keys. This paper demonstrated that it is possible to generate the key of a device using features unique to the devices. The paper then shows how a key can be generated using the ICMetric of the device. It is then shown that the key can be used to provide confidentiality using the Rabbit stream cipher. The proposed system is constituent of a cloud component which allows the patients to place their physiological data on the cloud. Owing to this service the data is made available remotely thereby making it possible for health professionals to monitor their patients continuously. To show that the scheme is efficient in its functioning we present a time

consumption analysis. In the end an in-depth security analysis of the scheme is presented to prove that the proposed schemes provide high levels of security.

4. ACKNOWLEDGEMENT

This work has been supported by CHIST-ERA under the User-Centric Security, Privacy and Trust in the Internet of Things topic through the SPIRIT project, funded via EPSRC grant EP/P016006/1.

5. REFERENCES

[1] Papoutsis, E. (2009). Investigation of the Potential of Generating Encryption Keys for ICMETRICS. University of Kent.

[2] Tahir, R., Tahir, H., & McDonald-Maier, K. (2015). Securing health sensing using integrated circuit metric. Sensors (Switzerland), 15(10), 26621–26642.

[3] Hinek, M. J. (2009). Cryptanalysis of RSA and its variants. CRC Press.

[4] Liao, W.-H., Kuai, S.-C., & Leau, Y.-R. (2015). Auto-scaling Strategy for Amazon Web Services in Cloud Computing. In 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity) (pp. 1059–1064). IEEE. http://doi.org/10.1109/SmartCity.2015.209

[5] Google. (2016a). Encryption at Rest in Google Cloud Platform.

[6] Google Cloud Platform. (2016). Supplying Your Own Encryption Keys. Retrieved December 5, 2016, from https://cloud.google.com/storage/docs/gsutil/addlhelp/SupplyingYourOwnEncryptionKeys

[7] Sajjad, A., Rajarajan, M., Zisman, A., & Dimitrakos, T. (2015). A scalable and dynamic application-level secure communication framework for inter-cloud services. Future Generation Computer Systems, 48, 19–27. http://doi.org/10.1016/j.future.2015.01.018

[8]Google. (2016b). Google Cloud Load Balancing. Retrieved from https://cloud.google.com/load-balancing/

How to cite this article:
Tahir R, Tahir H, Sajjad A, Maier K D. Icmapen: an icmetric based security framework for sleep apnea monitoring. J. Fundam. Appl. Sci., 2017, *9(7S), 545-557.*