Volume 6, Issue 4, April 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Privacy and Preserving Support for Internet of Things using SHA-2 in Healthcare ECG Monitoring

Raghuvaran.U.M
Software Engineering
M.Tech,
SRM University, India

B.Jothi
Software Engineering
Assistant Professor
SRM University, India

Krishnaveni.S
Software Engineering
Assistant Professor
SRM University, India

Ayyappan Jayavel.MPT
Physiotherapy
Assistant Professor
SRM University, India

Abstract- New generic cryptanalytic techniques for hash function based on MD5 and SHA-1, along with the fact that the SHA-2 family of hash functions was designed with a similar structure. The security of such technology has been a challenge over years and a majority of attacks is based on guessing the distance of the rotation where data is located. To ensure the patient data security and integrity the healthcare providers need to implement strong digital security and encryption methods for the user. To handle all emerging attacks and security challenges, algorithms have to be implemented to run a constant business continuity service in the field of health care. To ensure the confidentiality and security of electronic information (patient EMR, patient identifier, hospital medical records, etc.).This project is implementing using Java Platform as Frontend and Backend as HTML .The sha-2 algorithm provides a unique security framework which ensures full protection against web-services based attacks as well as vulnerability based IPS and DOS attacks from harming a healthcare providers applications. This project guarantees the availability of locally hosted and globally dispersed mission and patient applications services and data centers. To provide full protection against emerging attacks, it utilizes the latest security measures such as SHA-2 encryption algorithm .The SHA-2 algorithm is widely implemented in popular security applications and protocols like SSL, TLS , IPsec , S/MIME, SSH, PGP etc. There are many Crypto Currencies that rely on SHA-2 as a part of their Proof of work scheme.SHA-2 rightfully performs the most basic SHA function of effectively verifying the procedure of message authentication along with password verification as well.

Keywords- Healthcare, Computing, Privacy Preserving, Secure Hash Algorithm, Mobile-Healthcare, Remote Healthcare.

I. INTRODUCTION

Today Medical world started to implement these are the problem causes are Denial of service attack, Timestamp, Data loss, Data integrity[1]. These are existing problems in my base paper AES algorithm was used in existing mobile health care application ,system initialization the algorithm used is AES, as the algorithm cannot transmit the PHI data of a medical user who is in a critical situation.AES algorithm is not ready to encrypt and it takes a lot of time to be sent and occupies a large memory.The MD5 algorithm was used in existing mobile health care application to ensure the security of the medical user database ,but it has many implications some of them are, It's the less secure when compared to SHA -2.Message digest length bits exceeds 128bits.The MD5 algorithm can prevent attacks to some extents only, MD5 can be accessed only in 32-bit machines.These are the problem identification arean existing technology of mobilehealthcare application has a drawback due to security lapsing and time. So in my proposed work, I have replaced AES & MD5 algorithm by SHA-2 algorithm. SHA provides 2^{160} bit operation to break the original encrypted message .It's more fast and robust.The sha-2 algorithm has proved that there is no internal attack reported up to yet and so far.The sha-2 algorithm is more secure and sends the bunches of data without time lapsing to the PHI.

ATTRIBUTE	JUSTIFICATION	PRIORITY
Security	System security is empowered by the SHA-2 algorithm with its multiple variants.	High
Availability	The data source needed to implement the measure is available and accessible within the timeframe for measurement. The costs of abstracting and collecting data are justified by the potential for improvement in healthcare applications	High
Performance	Performance gain and achieve over 50% improvements in both End user satisfaction and Health service provider.	High

Contribution

This will ensure the better privacy of the user medical data to be stored in PHI using the SHA-2 algorithm. Instead of glucose meter device and application we are going to approach theIOT devices.

II. PROPOSED SYSTEM

The software should be active by 24/7 to monitor the user health. Mobile application should be aware of receiving data from wearable (sensor) devices.IOT Device should convert messages into PHI data format which is readable by Trust Authority. The network should be uninterrupted and easy to communicate with cloud server by all time. The software security should be guaranteed by proposing an algorithm for PHI data, which is accessible by user & Trust Authority. These are the requirements Analysis are Users need IOT Device as a wearable healthcare device which mobile can communicate through Bluetooth. The user should have Smartphone supported by Android or IOS mobile operating system in which user can install M-healthcare application. User need 3G network connection to upload the PHI to cloud server which is trustable network communication such as Airtel, Aircel, Vodafone,Etc.,PHI data should be secured bySHA-2 which preserves the privacy of user PHI stored on a cloud server.

Electrocardiography (ECG) Sensor:

Heartbeats are triggered by bioelectricalsignals of very low amplitude generated by a special set of cells in the heart (the SAnode). Electrocardiography (ECG) enables the translation of these electrical signals intonumerical values, enabling them to be used in a wide array of applications. Our sensorallow data acquisition not only at the chest ("on-the-person"), but also at the handpalms ("off-the-person"), and works both with pre-gelled and most types of dryelectrodes. The bipolar configuration is ideal for low noise.

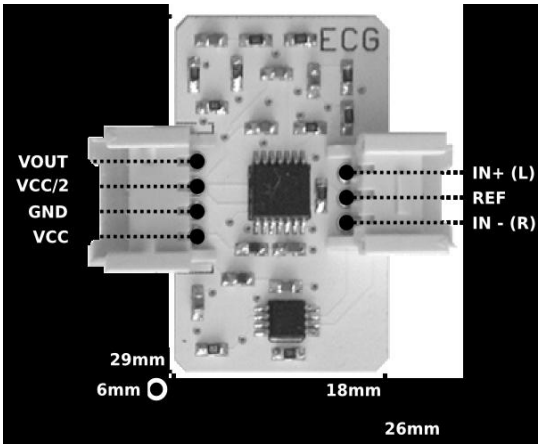

Fig. 1. Pin-out and physical dimensions of ECG sensor

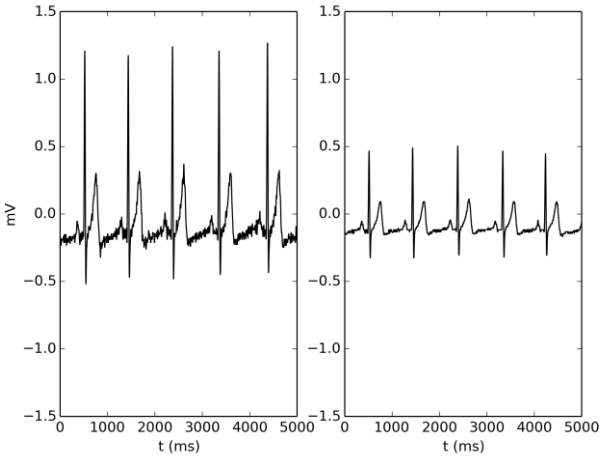

Fig.2. Typical raw ECG data (acquired with BITalino) using 2 electrodes at the hands (left) and 3 electrodes at the chest (right).

IoT-Internet Of Things:

The Internet of Things (IoT) is an environment in which objects, animals or people are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. IoT has evolved from the convergence of wireless technologies, micro-electromechanical systems (MEMS) and the Internet. The concept may also be referred to as the Internet of Everything.A thing, in the Internet of Things, can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low -- or any other natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network.

Product Description:

Lumisense IoT board designed to meet a variety of online application needs with distinct advantages that enable the embedded system designer to easily, quickly and seamlessly add internet connectivity to their applications.The module's UART update feature and webpage control make them perfect for onlinewireless applications such as biomedical

monitoring, environmental sensors, and data from portable battery operated wireless sensor network devices. Lumisense IoT board featured with SIM900 GPRS modem to activate internet connection also equipped with a controller to process all input UART data to GPRS based online data.

DIAGRAM:

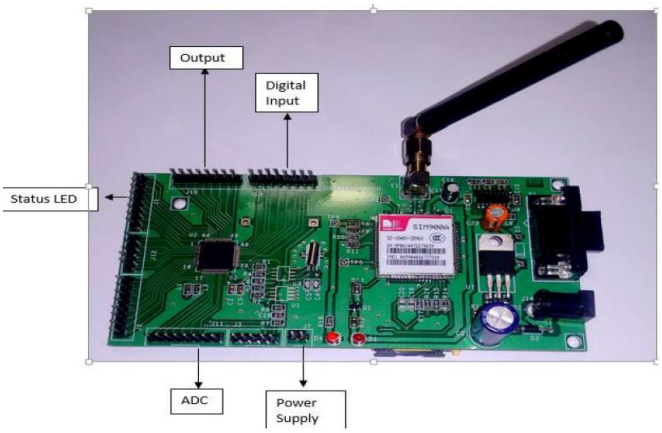

Fig 3. Internet of things device

PICMICROCONTROLLER (PIC16F877A)

Microcontroller Core Features:

High-performance RISC CPU

- Only 35 single word instructions to learn
- All single cycle instructions except for program branches which are two cycle
- Operating speed: DC - 20 MHz clock input DC - 200 ns instruction cycle
- Up to 8K x 14 words of FLASH Program Memory, Up to 368 x 8 bytes of Data Memory (RAM) Up to 256 x 8 bytes of EEPROM Data Memory
- Pin out compatible to the PIC16C73B/74B/76/77

III. CONCLUSION

In this paper, we have explained the secure and privacy preserving opportunistic computing framework for internet of things (IoT), which clearly explains the usage of SHA-2 in security and transmission of the patient ECG data.

REFERENCES

[1] Manda et al., International Journal of Advanced Research in Computer Science and Software Engineering 3(9),September - 2013, pp. 97-102

[2] .A. Toninelli, R. Montanari, and A. Corradi, "Enabling Secure Service Discovery in Mobile Healthcare Enterprise Networks," IEEE Wireless Comm., vol. 16, no. 3, pp. 24-32, June 2009.

[3] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Handshake with Symptoms-Matching: The Essential to the Success of My healthcare Social Network," Proc. Fifth Int"l Conf. Body Area Networks (BodyNets "10), 2010.

[4] Y. Ren, R.W.N. Pazzi, and A. Boukerche, "Monitoring Patients via a Secure and Mobile Healthcare System," IEEE Wireless Comm., vol. 17, no. 1, pp. 59-65, Feb. 2010.

[5] R. Lu, X. Lin, X. Liang, and X. Shen, "A Secure Handshake Scheme with Symptoms-Matching for mHealthcare Social Network," Mobile Networks and Applications—special issue on wireless and personal comm., vol. 16, no. 6, pp. 683-694, 2011. [5] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption," IEEE Trans. Parallel and Distributed System, to be published.

[6] M.R. June, S.W.P. Ng, N.L. Myo, J.Y. Khan, and W. Liu, "Wireless Body Sensor Network Using Medical Implant Band," J. Medical Systems, vol. 31, no. 6, pp. 467-474, 2007.

[7] R. Lu, X. Lin, X. Liang, and X. Shen, "A Secure Handshake Scheme with Symptoms-Matching for m-Healthcare Social Network," Mobile Networks and Applications—special issue on wireless and personal comm., vol. 16, no. 6, pp. 683-694, 2011

