International Journal of Engineering Research ISSN:2319-6890)(online),2347-5013(print)
Volume No.5 Issue: Special 4, pp: 790-991 20 May 2016

Secret Sharing of IoT Healthcare Data Using cryptographic algorithm

K. Niranjana Devi
PG Student, Dept. of Computer Science and Engineering
Kamaraj College of Engineering and Technology
Virudhunagar, India
niranju.038@gmail.com

R. Muthuselvi
Dept. of Computer Science and Engineering
Kamaraj College of Engineering and Technology
Virudhunagar, India
rmuthuselvicse@kamarajengg.edu.in

Abstract—Healthcare data are vital in patients surveillance. These data should have best quality to give finest treatment to patients. Many security threats affect originality of medical data. Nowadays anytime anywhere access of medical data is provided with the help of astounding technology called Internet of Things (IoT). IoT based healthcare has enormous applications however, it facilitates data abuse such as data breach and healthcare fraud. Sensitive, protected data is theft by the unauthorized person due to data abuse which degrades the quality of medical service. In this paper, secure data routing is done in IoT based healthcare to enhance security of medical data. Encryption algorithms are used to provide data confidentiality.Hashing techniques guarantee data integrity. Our simulation results show our algorithm provides security to healthcare data.

Keywords—Internet of Things (IoT); Wireless Sensor Networks (WSNs); Smart Healthcare; Data Confidentiality; Data Integrity; Cryptographic algorithms;

I. INTRODUCTION

Healthcare data are crucial to study and understand a patient's condition and to give the best possible treatment to them. Quality of data is the important which helps to provide optimal treatment to the patients. Pervasive healthcare systems apply information and communication technology to access data anywhere and anytime by the medical persons [1].

Internet of Things is the astonishing technology which allows ubiquitous computing. IoT based healthcare allows remote health monitoring, chronic diseases, and elderly. Some other important potential applications are compliance with treatment and medication at home. These applications provide reduction of costs, increasing quality of life, and enrich the user's experience [2].

Researchers build smart healthcare environment to obtain benefits of IoT based healthcare. Smart healthcare is nothing but monitoring of medical data with the help of smart devices. Sensors are one of the smart devices which measure heart rate, sleep patterns, blood pressure, body temperature, brain activity and other health related data.

Electronic processing of health care data facilitates data abuse. A data breach is one of the types of data abuse that is nothing but security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized person. Information contained in health care records has longer value and is rich enough for identity theft. Health care is the most affected industry by data breach. Fig. 1 shows that criminal attack is the major cause of data breaches [3].

Another type of data abuse is health care fraud. It includes health insurance fraud, drug fraud, and medical fraud. Such events made erroneous data in medical records. Health insurance fraud is described as an intentional act of deceiving, concealing, or misrepresenting information that results in health care benefits being paid to an individual or group. It can be committed either by an insured person or by a provider [4]. Drug fraud is a type of fraud in which drugs, legal or illegal, are cut or altered in such a way that diminishes their value below that which they are sold for. It consequences substance bad trip or overdose [5]. Medical fraud is the major risky data abuse which modifies health parameters. Since doctors give treatment based on the healthcare data medical fraud leads to loss of life. This erroneous information affects economy and human life. Patients are often unaware of medical identity theft until a curious bill or a surprising line of questioning by a doctor exposes the issue.

To maintain originality, data provenance is also required in smart medical application. This contains contextual information about the data, such as information about sensor patient association, data device association, and which parties handled the data. It is mainly used for providing non reputation. Such data should be secured against passive attacks like eavesdropping and data spoofing attacks. Eavesdropping of contextual information about health data leads severe violation of privacy. Traditional security mechanisms for transferring data provenance are energy inefficient.

This work is focused on solving security issues in smart health care. Major challenge for employing security scheme in wireless sensor network is lower processing power, memory and energy. Design of security protocol has three major aspects such as access control, data integrity and data confidentiality. Access control prevents identity theft by denying unauthorized parties in the network. Access control matrix or access list is used to provide various accesses to various levels of user. Hashing can be used for preventing data modification by the third party. Encryption of medical data provides confidentiality.

ISSN:2319-6890)(online),2347-5013(print)
20 May 2016

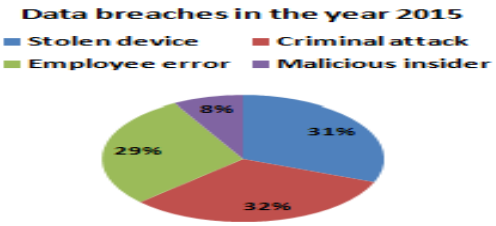


Fig. 1 Causes of health care data breaches

This paper is structured as follows. Section II lists some relevant previous work. Section III describes our system model. Section V discusses the experimental setup and results. Conclusion and future enhancements are drawn in Section VI.

II. Related Work

Healthcare devices and applications deal with private information such as personal healthcare data. Smart devices connected to global networks for providing anytime, anywhere data access. IoT healthcare domain is the target of attackers. To facilitate secure IoT healthcare domain, it is critical to identify and analyze distinct features of IoT security and privacy, including security requirements, vulnerabilities, threat models, and countermeasures, from the healthcare perspective.

An attacker may devise different types of security threats to compromise both existing and future IoT medical devices and networks. Some threats are tangible, some are predictable, and many are hard to predict. Some attacks disturb the information sent via network. Interruption, Interception, Modification, Fabrication and Replay are the attacks based on information disturbtion [6]. User Compromise, Hardware Compromise and Software Compromise are the attacks can be launched based on host properties [7]. Protocol and layer specific compromise are the attacks based on properties of network [8].

Confidentiality is the security requirements of IoT based healthcare for maintaining secrecy. Confidentiality ensures the inaccessibility of medical information for unauthorized users. In addition, confidential messages resist revealing their content to eavesdroppers.

To secure the data provenance for sensors used in IoT based healthcare, fingerprint matching algorithm is exploited. It enables two parties to generate closely matching fingerprints associated with a data session. Third party can later verify the details of the transaction, on that wireless link on which the data was transmitted. These fingerprints are very hard for an eavesdropper to falsify; they are lightweight compared with traditional provenance mechanisms and enable interesting security properties such as accountability, non repudiation, and resist man-in-the-middle attacks [9].

Due to resource conservation of wireless sensor networks cryptographic algorithms are used to generate fingerprints [10]. Encryption is used to make secret data that is functionally different from the original data. Public key cryptography is not used in sensor networks since sensor has limited resources. Symmetric key cryptography algorithms are used in sensor network. The secure symmetric algorithm should not able to break easily by brute force attack. It depends on strength of algorithm and length of the key. AES is one of the symmetric key cryptography algorithms which is easy to implement. It operates on a 4 by 4 array of bytes and has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits with 10, 12, and 14 number of rounds [11]. However it consumes more energy and requires high memory storage [12]. Skipjack has licensing issues. RC5 is optimal for encryption in sensor networks with lower computation power [13]. Extended Tiny Encryption Algorithm (XTEA) corrects weakness of TEA. This algorithm was designed by Roger Needham and David Wheeler on 1997. Until now this algorithm is not broken and is suitable for low power configured devices [14]. Encryption without an authentication mechanism is proven as insecure [13]. Further authentication and data integrity is maintained for stronger authentication. To provide data integrity and authentication various hash functions based MAC protocols are used.

III. System Model

IoT uses several communication technologies to connect things to each other. Fig. 2 shows some of the communication technologies used in IoT. Wi-Fi is applied for content sharing and distribution. ZigBee is used for low power sense & control networking. Cable replacement and wearable devices make use of Bluetooth. It connects eight nodes conversely, ZigBee connects 65000 nodes. Wi-Fi based network has size up to 2007 nodes. Range of ZigBee exist from 10 to 100 meters however average range of Wi-Fi up to 100 meters. Data transmission speed of Wi-Fi is in range 11mbps to 54mbps. In our proposed model Wi-Fi technology is used as the communication medium for data transmission.

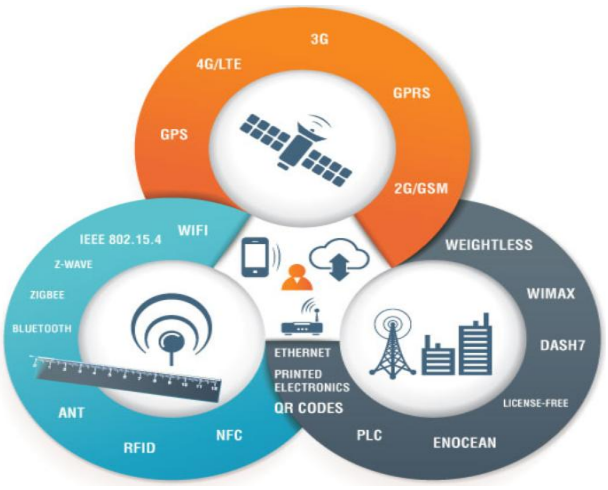


Fig. 2 Communication Technologies used in IoT

System architecture is revealed in Fig. 3. Patients can wear or embed sensors in their body. Each type of sensor measures

doi : 10.17950/ijer/v5i4/029

ISSN:2319-6890)(online),2347-5013(print)
20 May 2016

different health parameters such as temperature, blood pressure, heart beat. These health parameters are passed to sensor gateway via several intermediate nodes. Intruders may act as intermediate node to hack health parameters. To provide data confidentiality, various encryption algorithms are applied. Sensors are connected with sensor gateway to connect WSN with internet.

To provide CIA characteristics of message m encrypt it using secret key kp and bundle it with hash digest hd and session identifier such as time stamp ts.

$$\text{Ciphertext}=\text{hash}(\text{encrypt}(m, kp), ts) \quad (1)$$

An encryption procedure is symmetric, if the encrypting and decrypting keys are the same or it is easy to derive one from the other. It is called as secret key cryptography. The problem with this encrypting scheme is the secret key distribution to all parties. Keys must be updated every now and then. An encrypting function can encrypt the same plaintext to several different crypto texts. They are based on results in number theory or algebra [15].

$$dk(ek(w)) = w \text{ holds for every message (block) } w \text{ and key } k \quad (2)$$

Due to limited resources in sensor networks symmetric key encryption algorithm is used. Working model of symmetric key encryption is shown in Fig. 4. Initially sender converts plain text to cipher text with the help of key and encryption algorithm. Receiver decrypts the cipher text with the help of symmetric key. It makes secret link between two or more parties for share their surreptitious.

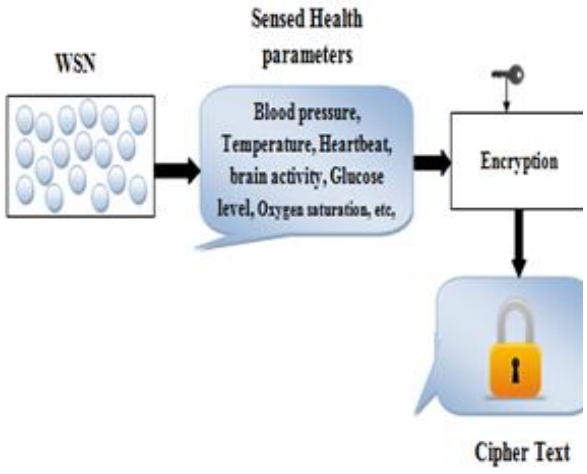


Fig. 3 System model

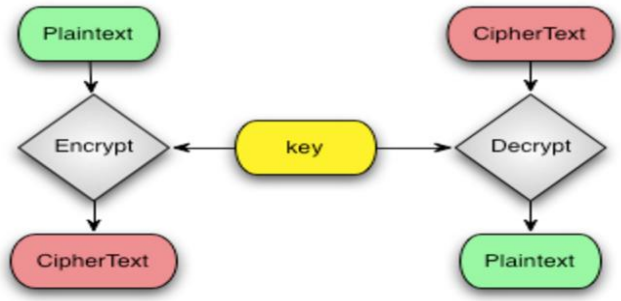


Fig. 4 Symmetric key encryption model

A cryptographic hash function is a hash function which is considered practically impossible to invert, that is, to recreate the input data from its hash value alone. Cryptographic hash functions are used to detect whether a message has been modified by an attacker. However, the use of a cryptographic hash function is not sufficient to detect whether a message has been modified. Fig. 5 demonstrates hash algorithm working model.

Hash function h which satisfies the following properties:

- h is a one-way function - For essentially all pre specified outputs y, it is computationally infeasible to find an x such that $h(x) = y$
- Pre-image resistance - given x it is computationally infeasible to find any second input x' with $x \neq x'$ such that $h(x) = h(x')$
- Collision resistance - it is computationally infeasible to find any pair (x, x') with $x \neq x'$ such that $h(x) = h(x')$

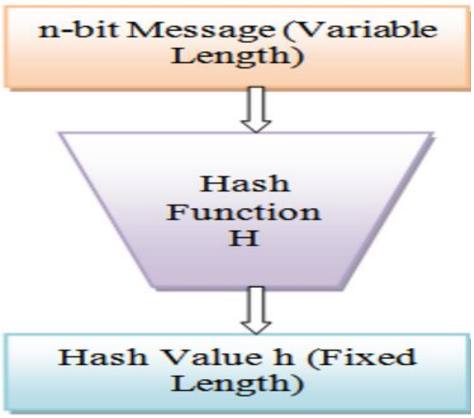


Fig. 5 Hash algorithm model

IV. Experimental Setup and Results

Proposed secure smart healthcare system was evaluated using NS3 simulator. In our proposed model Wi-Fi technology is used as the communication medium for data transmission since it consumes less energy compared to Bluetooth. Average range of Wi-Fi is up to 100 meters and its data transmission speed is 11mbps to 54mbps. Here IPV4 address (class C) is used for device identification. NS3 simulates IoT with the help of adaptation protocol called SixLowPAN. This protocol is used to connect sensors with internet. All the simulations have run more than 50 times and simulation parameters used in our work is illustrated in Table I.

. Source node sends data to border gateway through various intermediate nodes. Since it is a wireless medium the data is overheard by all nodes that are located in the communication range. This network has various intruders. They may access, modify or deny the data packet. Some nodes drop the data packet to do DOS attack. In such cases transmission energy gets dissipated.

doi : 10.17950/ijer/v5i4/029

ISSN:2319-6890)(online),2347-5013(print)
20 May 2016

TABLE I
SIMULATION PARAMETERS

Parameter	Value
Monitoring Area	500 m ×500 m
Number of nodes	250
Packet interval	1 s
Simulation time	1600 s
Transmit Energy	0.20024266 J
Receiving Energy	0.2 J
Idle Energy	0.003 J
MAC layer protocol	IEEE 802.11
Routing Protocol	IP V4 global routing
Adaptation layer protocol	SixLowPAN
Number of packets	100
Length of data packet	16 bytes

In our proposed system various encryption and hashing algorithms are analyzed. Here RC5, XTEA encryption algorithms and SHA 512 and MD5 hashing algorithms are analyzed. It prevents intruders to steal or modifies the health parameters.

Fig. 6 shows memory requirements of RC5 and XTEA algorithms. RAM required for RC5 is 72 bytes nevertheless XTEA uses 11 bytes alone. ROM required for RC5 is 3188 bytes however XTEA requires 1394 bytes. Sensors are resource constrained devices having limited memory. XTEA is suitable for providing security with lower memory requirement.

Fig. 7 shows performance comparison of RC5 and XTEA algorithms. These encryption algorithms has key initialization phase for key setup. This step is the significant task in providing confidentiality. This improves strength of security algorithms. RC5 spent 2.41 milliseconds for initializing key; XTEA takes 0.1 milliseconds for key setup phase. RC5 Encryption algorithm takes 0.829 milliseconds as execution time however XTEA consumes 0.171 milliseconds for encrypting given message. Decryption phase of RC5 takes 0.817 milliseconds; XTEA acquires only 0.174 milliseconds for decryption phase.

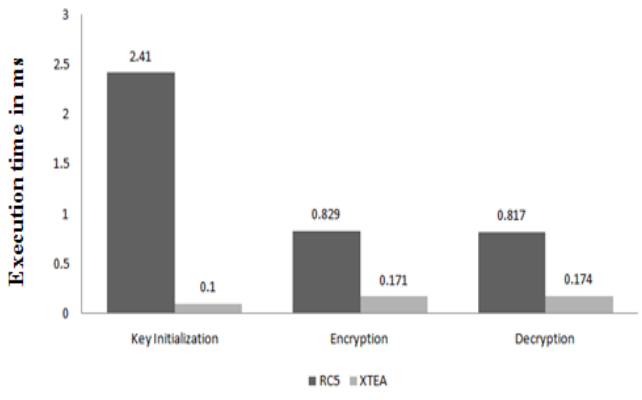
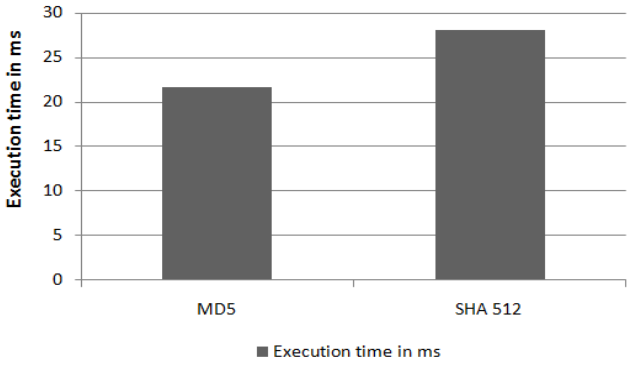


Fig. 7 Performance comparision of RC5 and XTEA

In our work, MD5 and SHA 512 algorithms are analyzed. SHA 1 has lot of security issues than SHA 2 algorithms. However SHA 3 algorithms use complex operations which consume more energy. Hence, SHA 2 family algorithms and MD5 are taken here.

Fig. 8 shows performance comparison of MD5 and SHA 512 algorithms. MD5 consumes 21.723 milliseconds, SHA 512 exhausted 28.076 milliseconds time for execution. Since MD5 spends less time for execution, less number of rounds it consumes less energy than other algorithms. Hence MD5 is chosen for our work.



network which leaks energy of sensor node. As a future enhancement we will overcome such attacks by finding trusted domain in a network and make routing among trusted nodes.

REFERENCES

[1] Nekane Larburu, Richard G. A. Bults, Marten J. Van Sinderen,Ing Widya, and Hermie J. Hermens. (2015, Aug.).An Ontology for Telemedicine Systems Resiliency to Technological Context Variations in Pervasive Healthcare. IEEE journal of Translational Engineering in Health and medicine.Vol. 3. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7163538

[2] Z. Pang, "Technologies and architectures of the Internet-of-Things (IoT) for health and well-being," M.S. thesis, Dept. Electron. Comput. Syst., KTH-Roy. Inst. Technol., Stockholm, Sweden, Jan. 2013.

[3] Healthcare Data Breaches (2015, Jun). Hippa Journal [Online] Available: http://www.hipaajournal.com/2015-healthcare-data-breaches-pass-100-incident-milestone-7052/

[4] Hyman, David A. Health Care Fraud and Abuse. p. 541.

[5] Hileman, Bette. (2008, Feb.) COUNTERFEIT DRUGS: Sophisticated Technologies and Old-Fashioned Fraud Pose Risks to the Prescription Drug Supply in the U.S. Chemical & Engineering News Printed

[6] Y. Wang, G. Attebury, and B. Ramamurthy. (2006, Jun). A survey of security issues in wireless sensor networks. IEEE Commun. Surveys Tuts., vol. 8, no. 2, pp. 2-23

[7] Y. W. Law, "Key management and link-layer security of wireless sensor networks: Energy-efcient attack and defense," M.S. thesis, Inst. Program. Res. Algorithmic, Univ. Twente, Enschede, The Netherlands, 2005.

[8] I. F. Akyildiz,W. Su, Y. Sankarasubramaniam, and E. Cayirci (2002). Wireless sensor networks: A survey. Comput. Netw., vol. 38, no. 4, pp. 393-422

[9] Syed Taha Ali. Vijay Sivaraman. Diethelm Ostry. Gene Tsudik and Sanjay Jha (2014). Securing First-Hop Data Provenance for Bodyworn Devices Using Wireless Link Fingerprints. IEEE TRANSACTIONS ON

 doi : 10.17950/ijer/v5i4/029

INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 12

[10] Mohammad AL-Rousan, A.Rjoub and Ahmad Baset (2009). A low energy security algorithm for exchanging information in wireless sensor networks. Journal of information assurance and security 4, 48-59.

[11] Jongdeog Lee, Krasimira Kapitanova and Sang H. Son (2010). The price of security in wireless sensor networks. Computer Networks, 54, pp.2967–2978.

[12] Afrin Zahra, M. Nizam uddin & Z.A Jaffery (2010). Implementation and Analysis of Security Protocols for Wireless Sensor Network. International journal of Electronics Engineering, 2(1), pp. 111-113.

[13] C. Karlof, N. Sastry, and D. Wagner. TinySec: a link layer security architecture for wireless sensor networks. In SenSys 2004, pages 162–175.

[14] Roger M. Needham, David J. Wheeler (October 1997). Tea extensions (PDF). Computer Laboratory, University of Cambridge (Technical report).

[15] HangRok Lee, YongJe Choi and HoWon Kim (2007). Implementation of TinyHash based on Hash Algorithm for Sensor Network. International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering Vol.1, No.10, pages 1564-1568.