iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** IV **Month of publication:** April 2019

DOI: https://doi.org/10.22214/ijraset.2019.4431

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

Data Integrity Assessment in E-Health Care System using Digital Watermarking

Mr. Abhay Patil[1], Mr. Attamohin Dalal[2], Mr. Parth Shah[3], Mr. Rasesh Bhatt[4], Mr. Rohan Shah[5]
[1]*Assistant Professor,* [2, 3, 4, 5]*Information Technology, Rajiv Gandhi Institute of technology, Mumbai, India, (Affiliated to Mumbai University) Mumbai, India*

Abstract: ***Wireless Sensor Network technology has its potential usage in wide range of applications. One such application is in the field of Healthcare, where wireless medical sensor networks (WMSNs) can be used to monitor patients [1]. Deployment of WMSNs for healthcare monitoring minimizes the need for healthcare professionals and helps the patients and elderly people to survive an easy independent life. However, if new technologies are deployed in healthcare applications without considering data integrity makes patient security vulnerable. Any intruder can send malicious or modified data to the unsuspecting sink, which will be accepted without any checks. One of the essential aspects in E-Health care is Integrity of data. The integrity of collected and transmitted data from medical sensor is critical, whether inside the network, or when stored at central servers. This paper discusses data integrity in the WSN for real-time patient monitoring using hashing mechanism. This paper aims to focus on these critical issues since these issues plays vital role in patient's security.***

Keywords: Wireless Sensor Networks (WSNs), Internet of Things (IOT), Secure Hash Algorithm (SHA), Data Integrity, Healthcare

I. PROBLEM DEFINATION

An E-Health Care System must provide efficient availability of accurate, meaningful, and complete data to assist the physician through the treatment. But one of the serious problems in depending on the networked data is 'rogue data'. Rogue data may include incomplete, missing or inaccurate information. The is a significantly concerning matter in the field of health care as the rogue data may cause medical errors, which can kill or lead to long-term damage to the patient's health. Data should represent the source accurately and also should have internal consistency. Data should stick to the rules based on the logic of the real world. Data integrity is referred as accuracy, internal quality, and reliability of data. Hence, integrity of the medical data to be transferred is a critical security requirement that need to be satisfied, since patient's medical information is extremely sensitive, and sometimes even life-threatening.

II. LITERATURE SURVEY

Owing to the availability of limited resources and privacy concerns, security issues have been major obstacles to the e-health applications that provide support for the people in dire need of these services. [2]. Shi and Xiao [3] suggested an algorithm for authentication of data integrity for WSNs based on reversible digital watermarking. This algorithm effectively applied prediction-error expansion for avoiding the loss of the data that is being sensed due to embedding watermark. However, the algorithm required not only to calculate group size according to the prediction function but also to calculate the hash value of every data item in the group, due to this the computational complexity increases greatly, so it is not suitable for the highly resource-constrained WSNs. In addition, the process of watermark embedding that used the predictions of spread-error expansion might cause data underflow and overflow. Abdelgawad et al. [4] proposed an IOT architecture customized for applications in the healthcare sector. The proposed architecture collects the information and passes it to the cloud where it is processed and analyzed. The user can be provided with the feedback actions based on the data that is analyzed. For collecting the user information that reflects its activity and medical signs, multiple sensors are needed. The proposed system's second module is used for indoor positioning. The signals representing the different sensed phenomena are then conditioned to be ready for input to the microcontroller as it is the core of the system. It is responsible for collecting the data of the different sensors interfaced to it and communicating such a data to the cloud server for further processing, or for retrieving location information. The data of the user is collected and communicated to a cloud server which is responsible for facilitating the accessibility of such a data anywhere through the Internet. However, the proposed system does not involve data security. Sun et al. [5] proposed a lossless digital watermarking strategy which uses redundant data space to embed watermark information. The sensed data collected by the sensor nodes was packaged again; unlike the previous methods, the original sensed data was not modified by embedding of the watermark. However, this strategy still had certain security vulnerability as the initial value of reservation bit for watermark was zero, and the watermark embedding position was relatively fixed which could be used by the attacker to acquire the sensed data.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

III. PROPOSED ARCHITECTURE WITH MODULAR DESCRIPTION

Secure Hash Algorithm (SHA) is a component of an SSL certificate used to ensure that data has not been modified. SHA accomplishes this by computing a cryptographic function and any change to a given piece of data will result in a different hash value. As a result, differing hash values are key to determining if data has been altered.

It is most important entity for providing the security against various data modification attacks. This work introduces secure hash algorithm to real-time monitoring in health application as E-Health Care System. The proposed work includes three processes:

A. Firstly, each client device (or sensing node) collects the data that is being sensed via sensors connected to patients.
B. Secondly, the collected data is given as input to SHA which generates a hash value known as message digest. Predefines rules are used to merge the message digest into the data that is being sensed to form a data packet that is transferred to the server.
C. The packet can suffer from an unreliable transmission and face various kinds of attacks. Thirdly, the server collects the data and then extracts the message digest and restores the sensed data according to the predefined rule. The restored data is used to generate message digest according to the same algorithm.

The figure below shows the block diagram of the proposed work.

The verification of data integrity is achieved by matching the regenerated message digest and the extracted message digest. If the message digest that is regenerated is different from the extracted message digest, the data is proved to be tampered during transmission. Otherwise, the data is proved to be safe. If the data is proved to be tampered, the system generates an alert message to notify the respective personnel of the same. It is difficult to detect the message digest if the predefined method is unknown.

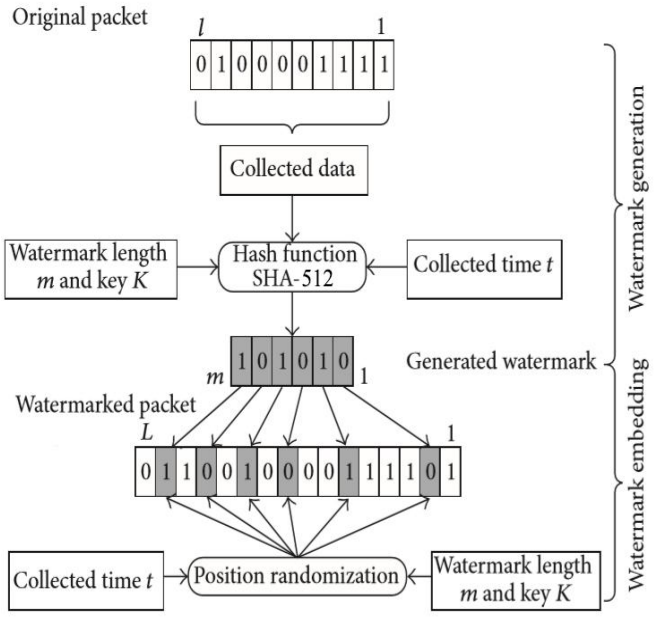
IV. ALGORITHMS

A. Watermark Generation Algorithm

This algorithm uses the SHA-512 hash function for calculating the hash value. SHA-512 hash function guarantees data integrity. It utilizes 65% less memory than other hash algorithms, such as the MD5 algorithm, which is more suitable for resource-constrained WSNs [6] due to a lightweight feature. The secret key K is the discrete information that is only known to the sender and the receiver.

The watermark generation process is described as follows:

1) Concatenate all the sensed data elements, collected time t, and secret key K to data: Data = $data_1$ - $data_2$ - … - $data_n$.
2) Calculate the hash value of the variable data denoted as W_0, based on SHA-512 hash function: W_0 = Hash (Data - t - K).
3) Select m bits from most significant bits of Wo as the watermark W, according to the actual needs. W = MSB (W_0, m).



B. Watermark Embedding Algorithm

The proposed water-mark embedding algorithm improves from the following two aspects:

1) The packet is redesigned and added m bits for water-mark to ensure that the watermark is transparently embedded in the packet. It does not cause any data interference and meets the high-precision requirements.

2) In order to solve the vulnerabilities brought by static embedding location, we introduce a new position random function to dynamically compute the water-mark embedding position which effectively solves likely vulnerabilities and greatly improves the security of the algorithm.

Figure illustrates the generation and embedding mechanism. The watermark embedding process is described as follows:

a) Calculate the watermark information W according to Algorithm 1 and update the packet's payload from l to L.

b) Obtain position arrays P and Q through function rand() with collected time t, secret key K, and number of watermark bits m. P and Q represent the watermark embedding position and the sensed data embedding position, respectively. P and Q need to satisfy the formula

$1 \le P_i \le L, 1 \le i \le m;$

$P_i \ne P_j, i \ne j;$

$P_i < P_j, i < j;$

$1 \le Q_i \le L, 1 \le i \le l;$

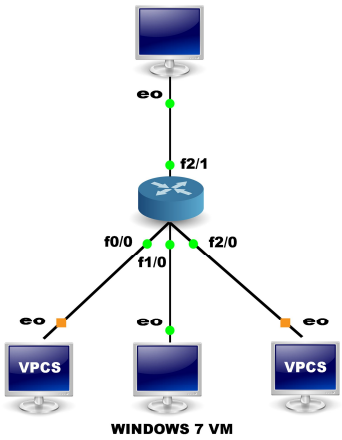
$Q_i \ne Q_j, i \ne j;$

$Q_i < Q_j, 1 < j$

$P \cap Q = \emptyset, P \cup Q = \{1, 2\ldots, L\}$

Length (P) + Length (Q) = L.

c) Insert the watermark W according to the position array P and insert the sensed data according to the position array Q to form a new packet, Packet W.



C. Watermark Extraction Algorithm

When the packet is transferred to the sink node, the sink node extracts the digital watermark information and restores the sensed data. The collected packet is denoted as Packet W'. The sink node and the sensing node share the secret key K. The restored packet is represented as Packet'.

The process of extraction and verification are described as follows:

1) Extract the serial number from collected packet Packet W'.

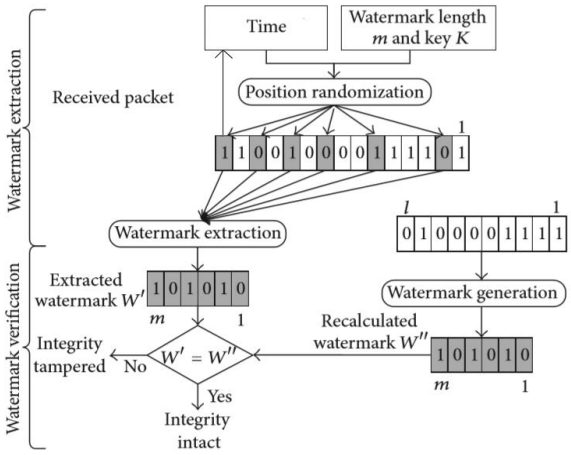
2) Acquire the collected time t from the time queue stored in the sink node.

3) Calculate the arrays P and Q according to the function rand().

4) Obtain the watermark represented as W' and restore the packet represented as Packet'.

5) Recalculate the watermark W" with Packet', t, m, and K.

6) Compare W' with W"; if W' is equal to W"', the data integrity is verified; otherwise the data is tampered.



V. EXPECTED OUTCOME

Our proposed work is expected to have following outcomes:

A. It will be able to provide an efficient way to make sure the message has not been tampered or fabricated over transmission channels.

B. It will offer a great way to achieve data integrity in real-time health care system.

C. It is expected to lessen the workload on the care givers i.e. doctors and nurses in the hospital.

REFERENCES

[1] P. Kumar, H. Lee, "Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey," Sensors, pp. 1-3, 2012.

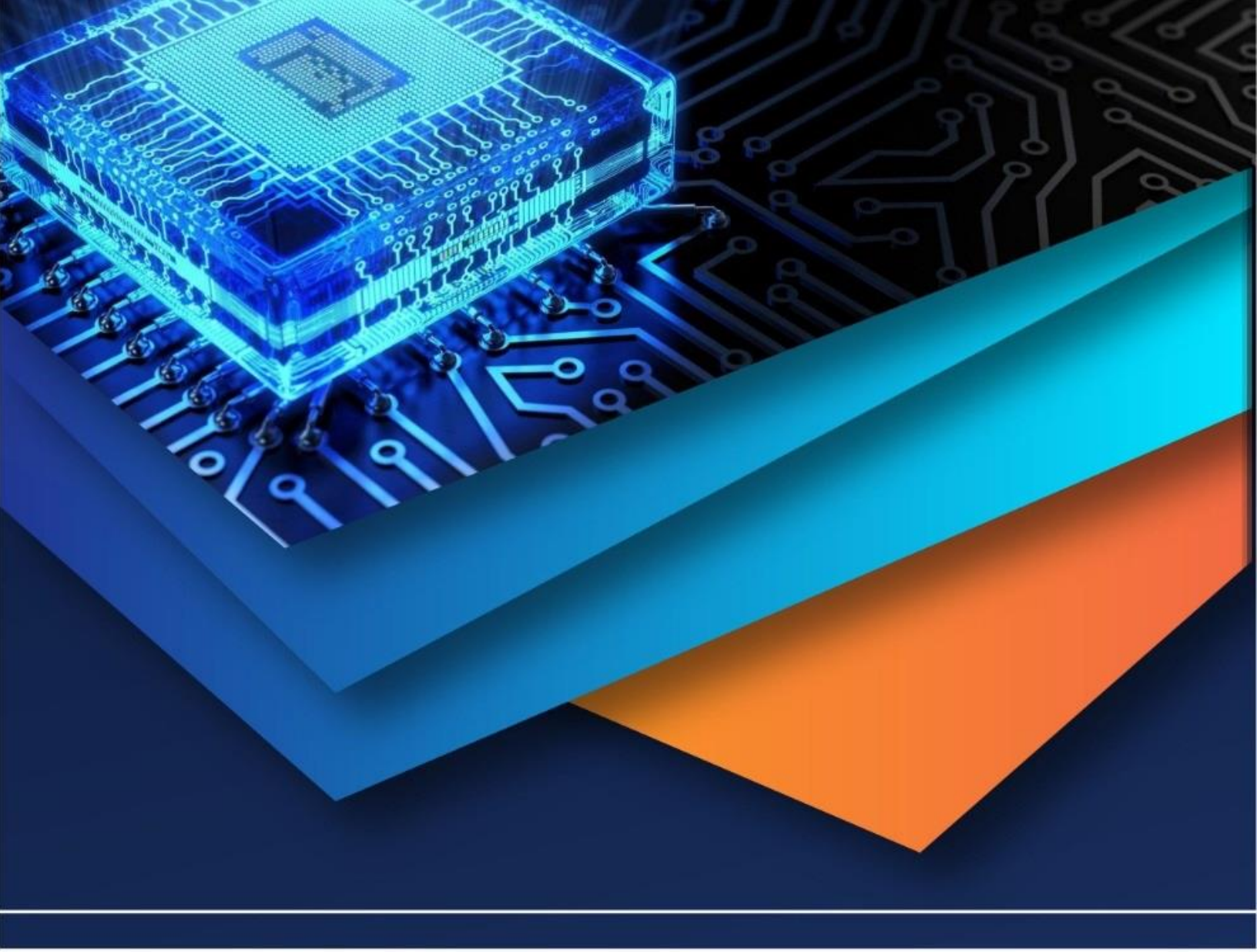
[2] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, G. Wang, "Security and Privacy in the Medical Internet of Things,", Journal of Security and Communication Networks, Hindawi, vol. 2018.

[3] X. Shi and D. Xiao, "A reversible watermarking authentication scheme for wireless sensor networks," Information Sciences, vol. 240, pp.173-183, 2013.

[4] Ahmed Abdelgawad, Kumar Yelmarthi and Ahmed Khattab. "IOT Based Health Monitoring Sytem for Active A and Assisted Living," IEEE, vol. 4, pp.572-582.

[5] X. Sun, J. Su, B. Wang, and Q. Liu, "Digital watermarking method for data integrity protection in wireless sensor networks," International Journal of Security and Its Applications, vol. 7, no. 4, pp. 407-416, 2013.

[6] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller, and M.Sichitiu, "Analyzing and modeling encryption overhead for sensor network nodes," in Proceedings of the Second ACM International Workshop on Wireless Sensor Networks and Applications, WSNA 2003, pp.151–159, September 2003.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY