Hindawi Publishing Corporation
Mobile Information Systems
Volume 2015, Article ID 852173, 9 pages
http://dx.doi.org/10.1155/2015/852173

Research Article

Hadoop-Based Healthcare Information System Design and Wireless Security Communication Implementation

Hongsong Chen[1] and Zhongchuan Fu[2]

[1] *School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China*
[2] *School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150001, China*

Correspondence should be addressed to Hongsong Chen; chenhs@ustb.edu.cn

Received 17 December 2014; Revised 2 May 2015; Accepted 4 May 2015

Academic Editor: Jose Juan Pazos-Arias

Human health information from healthcare system can provide important diagnosis data and reference to doctors. However, continuous monitoring and security storage of human health data are challenging personal privacy and big data storage. To build secure and efficient healthcare application, Hadoop-based healthcare security communication system is proposed. In wireless biosensor network, authentication and key transfer should be lightweight. An ECC (Elliptic Curve Cryptography) based lightweight digital signature and key transmission method are proposed to provide wireless secure communication in healthcare information system. Sunspot wireless sensor nodes are used to build healthcare secure communication network; wireless nodes and base station are assigned different tasks to achieve secure communication goal in healthcare information system. Mysql database is used to store Sunspot security entity table and measure entity table. Hadoop is used to backup and audit the Sunspot security entity table. Sqoop tool is used to import/export data between Mysql database and HDFS (Hadoop distributed file system). Ganglia is used to monitor and measure the performance of Hadoop cluster. Simulation results show that the Hadoop-based healthcare architecture and wireless security communication method are highly effective to build a wireless healthcare information system.

1. Introduction

Since the first biosensor was introduced in 1962 by Clark and Lyons [1], there has been increasing demand for such analytical devices in real applications. Research initially focused mainly on detector principles and recognition elements; however, to obtain a user-friendly and well-performing analytical device, many components have to be considered [1]. Biosensors have been developed for many years and research has become very popular in recent years. Advances in microelectronics, material science, and wireless communication technology have led to the development of micro sensors that can be used for the monitoring of bioinformation objects. So biosensors remain a subject of great popular interest [2].

Wireless sensor networks (WSN) [3, 4] have received significant attentions due to their widespread applications in military and civilian environments. Sensors are low cost, low-power devices which have limited resources. A sensor node typically contains a power unit, a sensing unit, a processing unit, a storage unit, and a wireless transmitter/receiver. Wireless biosensor networks can be used in healthcare system: inside a healthcare system, biosensors are placed or embedded in human body to monitor their blood pressure, body temperature, sugar level, heartbeats, and so forth. Biosensors constitute a wireless network and periodically monitor the health information of their hosts. Health monitoring involves collection of data about vital body parameters and making intelligent decisions. This information is required to be transferred securely. Insecurity information transfer can lead to much risk. So security and privacy [5, 6] issues have become critical research fields in wireless biosensor network. Development of an effective security scheme is challenged by the limited storage, computing ability, and energy. In modern healthcare environment, it is important to design a security scheme based on small biosensor computing devices and big cloud computing resource.

In this paper, a novel Hadoop-based wireless healthcare architecture is proposed to protect data communication

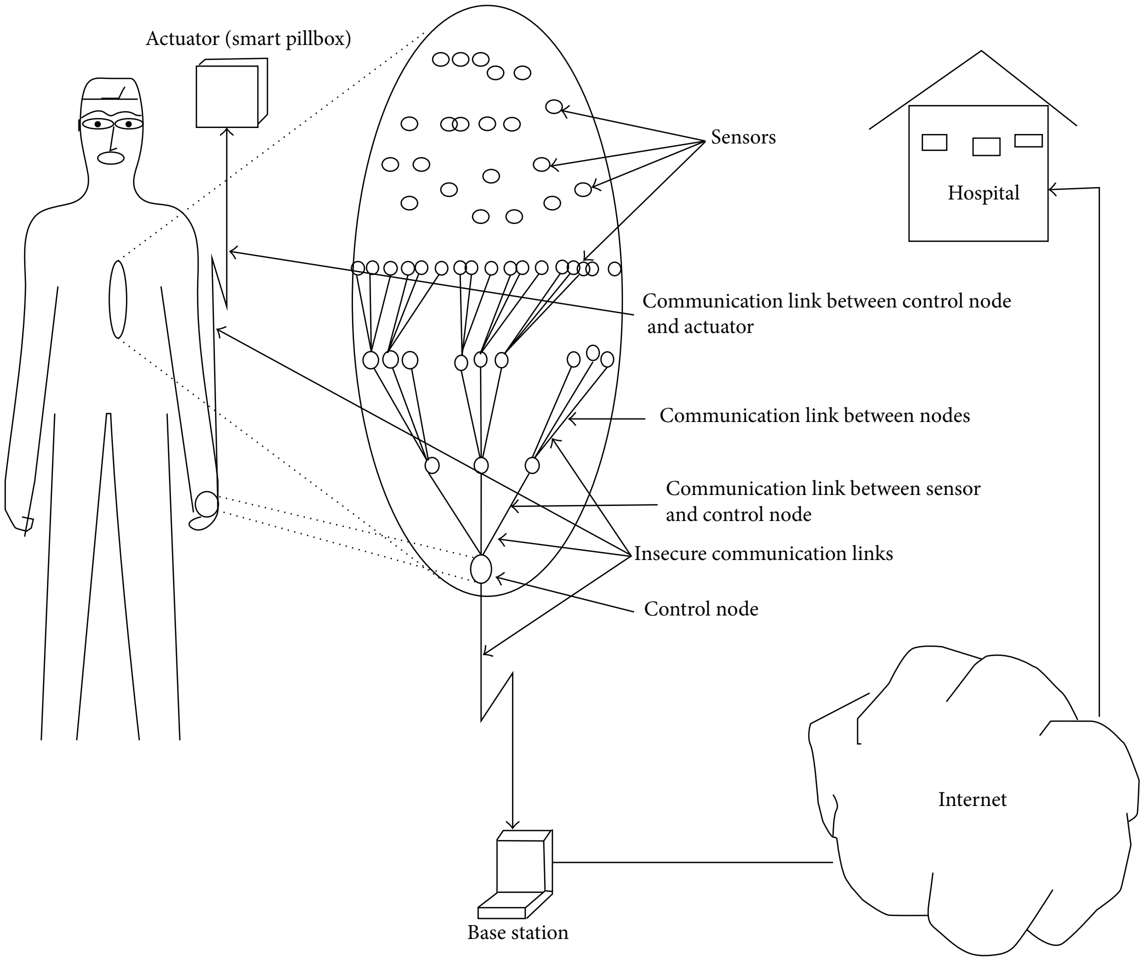

Actuator (smart pillbox)
Sensors
Hospital
Communication link between control node and actuator
Communication link between nodes
Communication link between sensor and control node
Insecure communication links
Control node
Internet
Base station

Figure 1: System model of biosensor network [9].

security in biosensor network. There are two main contributions in the paper. The first is that Hadoop-based biosensor wireless healthcare information system architecture is proposed. The second is that ECC-based digital signature and security communication method are implemented in Sunspot WSN. The rest of this paper is organized as follows: Section 2 reviews some related work on biosensor network and Hadoop-based healthcare system. Section 3 describes the system architecture of Hadoop-based wireless healthcare system. Section 4 describes the security data communication method based on small biosensor node and big cloud resource. Section 5 gives simulation results by Sunspot and Hadoop cloud platform. The conclusion is drawn in Section 6.

2. Related Work Analysis on Biosensor Network and Hadoop-Based Healthcare System

Biosensors, nanosensors, and biochips have become popular as a tool for medical diagnostics due to their noninvasive or minimally invasive nature [7]. A biosensor is a probe that integrates a biological component, such as a whole bacterium or a biological product, with an electronic component to yield a measurable signal. It can detect and measure concentrations of specific bacteria or hazardous chemicals; it can also measure acidity levels (pH). Nanosensors provide new and powerful tools for monitoring in vivo processes within living cells [8]. Biochips are designed by combining integrated circuit elements, an electrooptics excitation/detection system, and bioreceptor probes into a self-contained and integrated micro device.

The rapid improvement in microprocessor and sensing material technology has led to a development of miniature sensors that can be implanted in the human body. The biosensor based approach to healthcare makes it much more effective by reducing the response time [9]. The biosensor network consists of a group of biosensors implanted inside the human body, external device (control node) placed on the human body, and a base station, which are shown in Figure 1.

A network is formed by the biosensors between themselves and the control node. The control node is connected to an external base station, as shown in Figure 1. There are three types of wireless communication links in the biosensor network based health care system. They are the communication links between the biosensors, the communication links between the biosensor and control node, and the link between control node and the base station. All these wireless links are considered to be insecure due to the fact that the data is available on the channel. Therefore, data exchange using any of these communication links has to be secured. The set constraints experienced by the biosensors make existing solutions to sensor network security unsuitable for biosensor security. Hence biosensors security requires novel solutions. The algorithm used is a lightweight encryption algorithm. They use the error correcting codes and the multiple biometrics for securing the key for the problems of measurement errors and randomness problems.

Poon et al. explore the use of this conduit in the security mechanism of BASN (body area sensor network) [10], that is, by a biometrics approach that uses an intrinsic characteristic of the human body as the authentication identity or the means of securing the distribution of a cipher key to secure inter-BASN communications. The method was tested on 99 subjects with 838 segments of simultaneous recordings of electrocardiogram.

Perrig et al. [11] have presented a set of protocols for achieving requirements of security in sensor network. Their architecture consists of two blocks that are SNEP and μTesla. In SNEP they use symmetric keys to encrypt the data. Symmetric keys are also used to compute the Message Authentication Code (MAC). Both of these set of keys are derived from a master key which is shared by the nodes with the base station and are placed in them before being deployed. μTesla is used to achieve authenticated broadcast by delayed key disclosure. The keys are computed from the master predeployed key and the counter which is incremented after each block.

New generations of health care systems generally run on thousands of servers to meet the requirements of millions of users [12]. Traditional health care data analysis systems are difficult in solving the process problems with massive data. They propose a massive data management and analysis solution based on Hadoop. They present data analysis methods based on MapReduce and Hive. Experiment results show that Hadoop-based framework improves the performance of data upload and data query. Hive-based data analysis method is suitable for massive data analysis tasks.

Traditional data storage for patients is not scalable enough for the increasing number of patients and applications [13]. Cloud computing promises low cost, high scalability, and reliability which can be a potential solution for storing patients' medical records. They analyze the impact of cloud computing on improving healthcare services. The architectural design called "MedCloud" which utilizes and integrates services from Hadoop's ecosystem is given for medical systems development.

Kojima and Nagahashi propose the disaster-relief training system using the electronic triage tag [14]. They design the graphical user interfaces to develop the scenarios of injured people information and transport information such as ambulance. They let the electronic triage tag generate vital signs of injured people constantly. By collecting and monitoring those data at regular intervals, they construct disaster-relief training system that enables medical staff to conduct a more practical training considering the change in symptoms of injured people. They use SunSPOT developed by Sun Microsystems as an electronic triage tag.

They propose a method to preserve the privacy and security of patients' portable medical records in portable storage media to avoid any inappropriate or unintentional disclosure [15]. Following HIPAA guidelines, the method is designed to protect, recover, and verify patient's identifiers in portable EHRs.

IBM InfoSphere Guardium provides database activity monitoring and auditing capabilities that enable user to integrate Hadoop data protection into existing enterprise data security strategy [16]. User can configure the system and use InfoSphere Guardium security policies and reports for Hadoop environments. It does not involve wireless sensor network security communication.

HDSM is a Hadoop-based distributed sensor node management system, which uses Hadoop MapReduce framework and distributed file system [17]. Each sensor node imitates DVR (digital video recorder) for sensing video data. All sensor nodes are connected to HDSM manager via gigabit ethernet. So HDSM is not suitable to lightweight sensor node and application.

Cloudwave platform is proposed to access and query large volumes of electrophysiological signal data using the HDFS storage module. Cloudwave allows users to search for clinical events using ontology and semantics reasoning [18]. However, it does not involve biomedical data security communication.

Seen from the above analysis, how to build security healthcare information system with biosensors and cloud computing is a great challenge to current healthcare information system design and implemention.

3. Architecture of Hadoop-Based Wireless Biosensor Healthcare System

To build a biosensor healthcare system, multidiscipline knowledge and techniques are needed, such as electronic engineering, bioinformatics, computer science, software engineering, communication technique, and information security. A novel architecture of Hadoop-based wireless biosensor healthcare information system is shown in Figure 2.

As shown in Figure 2, healthcare information system includes biosensors, Sunspot node, Sunspot base station, Mysql database server, and Hadoop cloud computing cluster server. They cooperate to fulfill healthcare information collection, transfer, storage, and processing. Breathing, heartbeat, pulse, blood pressure, and body temperature are important health parameters, which reflect human health status. Continuous monitoring and storage of the health data can provide important diagnosis references to doctors. Seen from Figure 2, biosensor can measure biological signal and converts it into a value. The health parameters can be collected by different kinds of biosensors; the biosensor circuit boards are connected to Sunspot wireless node by

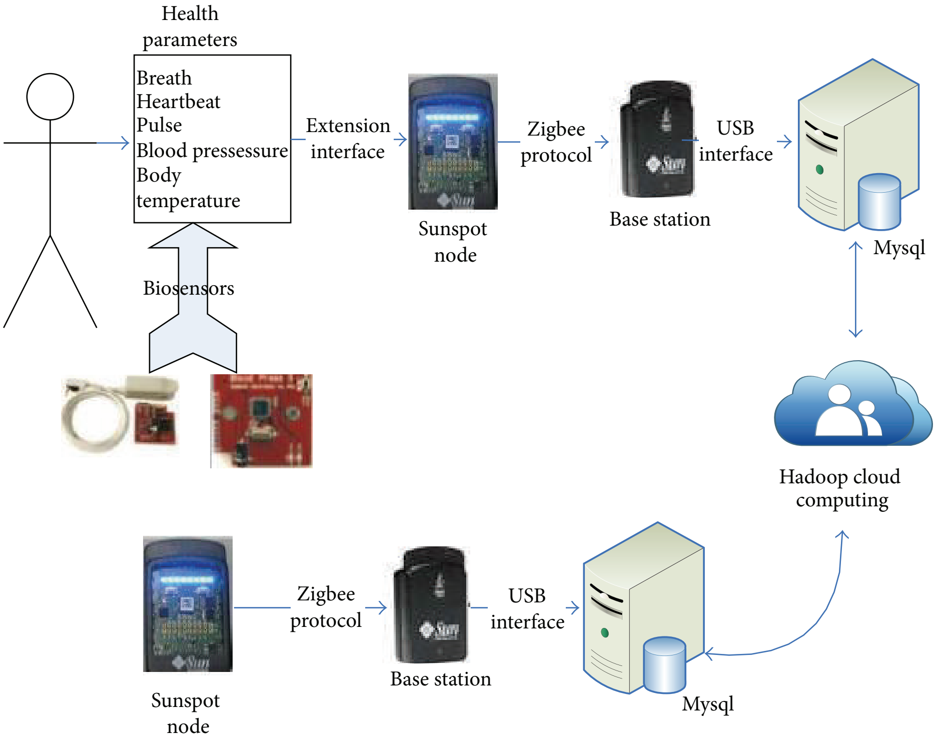


Figure 2: Hadoop-based biosensor wireless healthcare information system architecture.

standard extension interface. In Sunspot node, there is a 20-pin extension interface, in which it supports standard UART (Universal Asynchronous Receiver/Transmitter), I2C, analog signal input, GPIO (General Propose Input Output), Vcc 3V, Vcc 5V, and GND. So different types of biosensors can be connected to Sunspot node; serial port multiplexing technique can be used to connect many biosensors that use serial communication. So the proposed approach has good scalability in case of increase of the number of biosensors.

SunSPOT is a small wireless sensor network device; it is programmable device based on Java. SunSPOT is based on a 32-bit ARM-9 CPU and 11 2.4 GHz radio channels. SunSPOT devices can communicate with each other through the Zigbee protocol. So the measured value can be sent to base station by Zigbee protocol. Then the base station is connected to healthcare Mysql database server by USB interface. All the data received by base station are transferred to the healthcare server and stored in Mysql Database. With the monitor areas enlarging, the number of monitoring nodes will increase greatly. So Hadoop-based big data storage and process are needed.

4. Biosensor Information Secure Communication and Process

From the network security viewpoint, data communication between Sunspot wireless node and Sunspot base station is vulnerable to attack, such as data tampering attack. So we propose a lightweight digital signature and verification method to protect data communication security. As we know, biosensor has limited computing and storage resource; ECC (Elliptic Curve Cryptography) algorithm is a lightweight public key cryptography algorithm which is suitable for WSN. So we use ECC asymmetric cryptography algorithm (supported elliptic curve SECP160R1) to implement digital signature and verification. Biosensor information secure communication is shown in Figure 3.

As shown in Figure 3, biosensor information secure communication is divided into three process steps. The first step is to generate public/private key pair; the wireless node generates its public/private key pair. In Sunspot programming API specification, there are Java class-ECPublicKeyImpl, ECPrivateKeyImpl, and ECKeyImpl to perform ECC public/private key pairs generation; the method genKeyPair (publicKey and privateKey) in ECKeyImpl class is used to generate the public/private key pairs. Then it transfers its public key to the base station, which stores the public key in the background Mysql database server. Because the step is executed before data communication, it is independent of data transmission; attacker finds it difficult to get the key and the biosensor data simultaneously. So data secure delivery is provided in our communication process. To prevent attackers from tampering with the public keys stored in Mysql database, the public keys are backed up to Hadoop cloud storage. Sqoop are used to execute the task of exchanging data between Mysql database and Hadoop file system. The public keys from Mysql database will be backed up to HDFS storage system by Sqoop

Table 1: Execution time of ECC signature and verification on SunSPOT Sensor (ms).

Length of message	Operation type	Number of operations (100)	Number of operations (1000)	Number of operations (5000)	Average execution time (ms)
128 bits	Signature	392	3875	19225	3.865
	Verification	388	3858	19106	3.853
512 bits	Signature	768	7687	38230	7.671
	Verification	759	7697	38012	7.630
1024 bits	Signature	1152	11531	57346	11.507
	Verification	1139	11545	57018	11.446

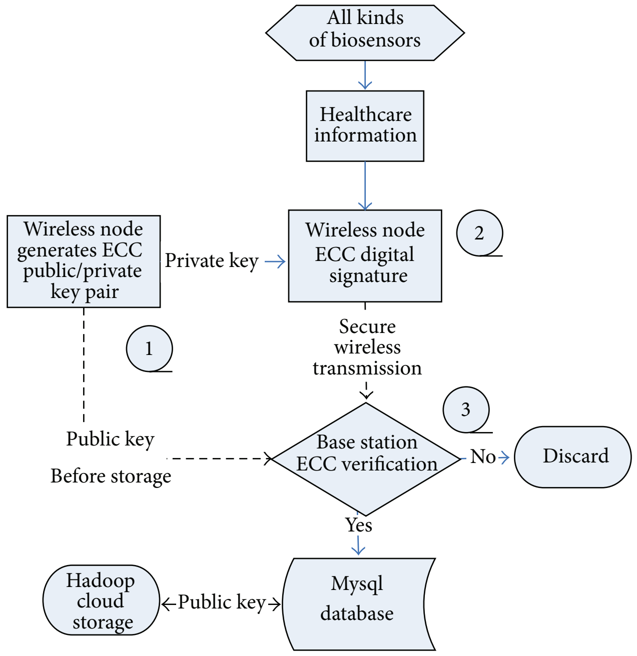

All kinds of biosensors
Healthcare information
Wireless node generates ECC public/private key pair
Private key
Wireless node ECC digital signature
2
1
Secure wireless transmission
3
Public key
Before storage
Base station ECC verification
No
Discard
Yes
Hadoop cloud storage
Public key
Mysql database

Figure 3: Biosensor information secure communication and process.

import instruction. The public key can be recovered from Hadoop to Mysql database by Sqoop export instruction.

In the second step, when the wireless node receives the healthcare information from biosensors, it executes ECC digital signature algorithm to sign and protect the biosensor measure values. In Sunspot programming API specification, there is a Java class-signature to perform ECC signature and verification, which includes initSign, update, sign, and verify methods. A 160-bit standard compliant elliptic curve (secp160r1) is used to implement ECC signature by calling Sunspot programming API.

In the third step, when the base station receives the message which includes measure value, base station queries the Sunspot ID and reads its public key from background Mysql database; then base station uses the public key of Sunspot to verify the message. If the message can be verified successfully, the biosensor measure value will be stored in the background Mysql database. The doctors can check and analyze the health information to do intelligent diagnosis. If the message is tampered with by an attacker, it cannot be verified successfully; the message including measure value will be discarded.

Average execution time in Sunspot node is used to measure the overhead of the ECC signature and verification. The message is computed by SHA1 algorithm to get the Hash value; then the Hash value is signed by ECC signature algorithm. Signature and verification time are used to measure the overhead of ECC signature and verification processes in Sunspot wireless node. The experiment results are shown in Table 1.

We use average execution time as the overhead of ECC signature and verification processes on SunSPOT Sensor. Seen from Table 1, the overhead can be accepted, because the average execution time is millisecond level. The average execution time of ECC signature and verification is close, while the time of signature is a little more than that of verification. With the increase of message length, the average execution time of signature and verification increases simultaneously. To most of signature application in wireless sensor network, the overhead of ECC signature and verification processes can be accepted on the aspect of average execution time.

Two tables are designed in the entity-relationship diagram (ERD) of database; the first table is Sunspot security entity table; it includes the Patient ID, Sunspot ID, and Sunspot public key, in which Patient ID and Sunspot ID are united to be primary key; Sunspot public key can be used to verify biosensor measure value. The security entity table can be backed up to the Hadoop HDFS to prevent public key from tampering attack. The second table is Sunspot measure entity table, which records biosensor health measure values that are measured from the patients. It includes the Sunspot ID, Biosensor ID, measure timestamp, and measure values, in which measure timestamp is the primary key of the Sunspot measure entity table. In every measure time point, the measure value is unique. The entity-relationship model of the two tables is shown is Figure 4. The two entities are connected by verification relation.

Seen from Figure 4, the relation between Sunspot security entity and Sunspot measure entity is verification. Only if the measure value is verified successfully, the measure value can be recorded in the Sunspot measure entity table, otherwise the measure value will be discarded. The integrity of measure values can be protected by the Sunspot security entity. The Sunspot ID of Sunspot security entity is the foreign key of Sunspot measure entity. The two entities can be connected by the Sunspot ID to execute joint query.

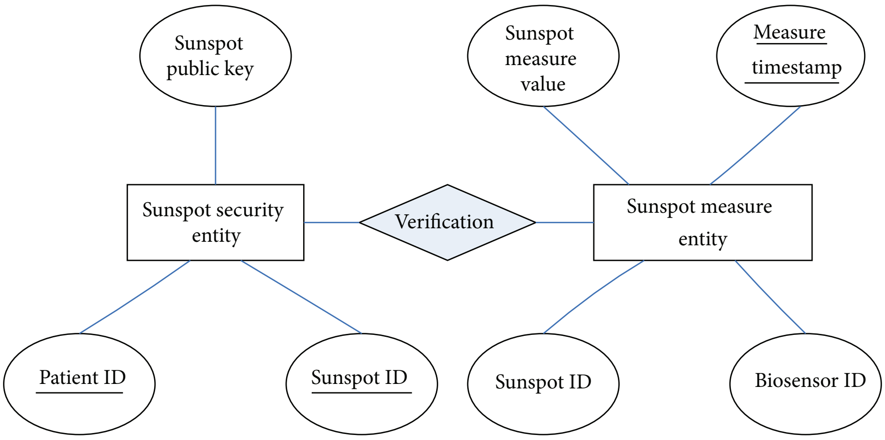
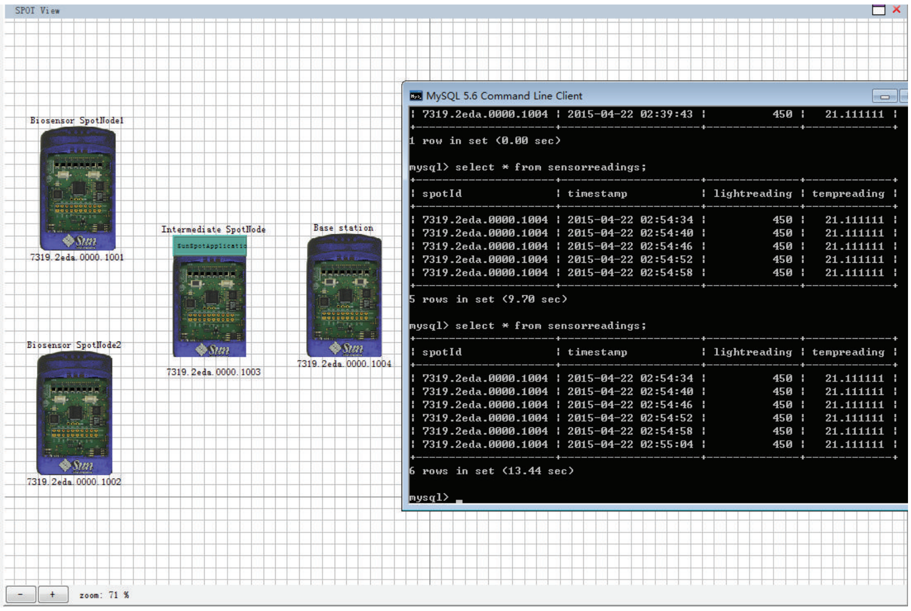


Figure 4: Entity-relationship model of Sunspot security entity and measure entity.



```
| 7319.2eda.0000.1004 | 2015-04-22 02:39:43 |           450 |   21.111111 |
+---------------------+---------------------+---------------+-------------+
1 row in set (0.00 sec)

mysql> select * from sensorreadings;
+---------------------+---------------------+---------------+-------------+
| spotId              | timestamp           | lightreading  | tempreading |
+---------------------+---------------------+---------------+-------------+
| 7319.2eda.0000.1004 | 2015-04-22 02:54:34 |           450 |   21.111111 |
| 7319.2eda.0000.1004 | 2015-04-22 02:54:40 |           450 |   21.111111 |
| 7319.2eda.0000.1004 | 2015-04-22 02:54:46 |           450 |   21.111111 |
| 7319.2eda.0000.1004 | 2015-04-22 02:54:52 |           450 |   21.111111 |
| 7319.2eda.0000.1004 | 2015-04-22 02:54:58 |           450 |   21.111111 |
+---------------------+---------------------+---------------+-------------+
5 rows in set (9.70 sec)

mysql> select * from sensorreadings;
+---------------------+---------------------+---------------+-------------+
| spotId              | timestamp           | lightreading  | tempreading |
+---------------------+---------------------+---------------+-------------+
| 7319.2eda.0000.1004 | 2015-04-22 02:54:34 |           450 |   21.111111 |
| 7319.2eda.0000.1004 | 2015-04-22 02:54:40 |           450 |   21.111111 |
| 7319.2eda.0000.1004 | 2015-04-22 02:54:46 |           450 |   21.111111 |
| 7319.2eda.0000.1004 | 2015-04-22 02:54:52 |           450 |   21.111111 |
| 7319.2eda.0000.1004 | 2015-04-22 02:54:58 |           450 |   21.111111 |
| 7319.2eda.0000.1004 | 2015-04-22 02:55:04 |           450 |   21.111111 |
+---------------------+---------------------+---------------+-------------+
6 rows in set (13.44 sec)

mysql> _
```

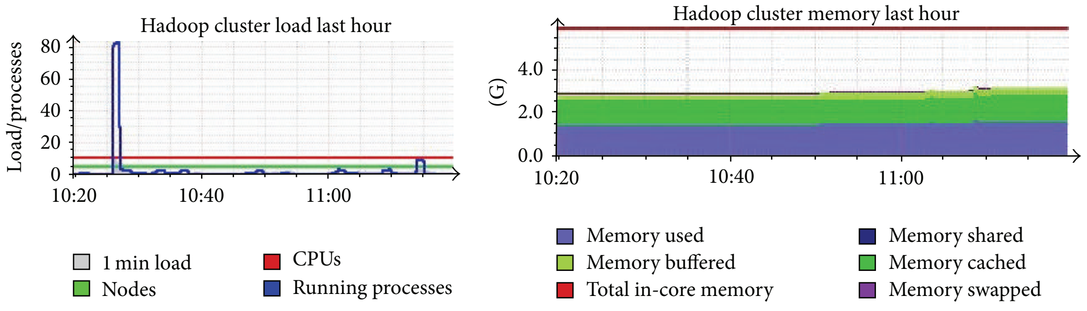
Figure 5: Sunspot based healthcare communication system simulation.

In our scheme, the Sunspot security entity table is backed up to Hadoop HDFS storage to ensure the recovery of public key. One Sunspot node is related to one record in Sunspot security entity table, in which the data types of Patient ID and Sunspot ID are 32-bit unsigned long integer; the data type of Sunspot public key is 160-bit character string. So the storage space of one record in security entity table is 28 Bytes (4 Bytes + 4 Bytes + 20 Bytes), and one Sunspot node needs 28 Bytes in Hadoop HDFS storage. If the cloud storage size is 100 G Bytes, the scale of the biosensor network is $3.571428 * 10^9$.

5. Sunspot Platform Simulation Research

To validate biosensor based healthcare system and information secure communication procedure, we use Sunspot platform to simulate the secure communication process. The simulation scenario is shown in Figure 5.

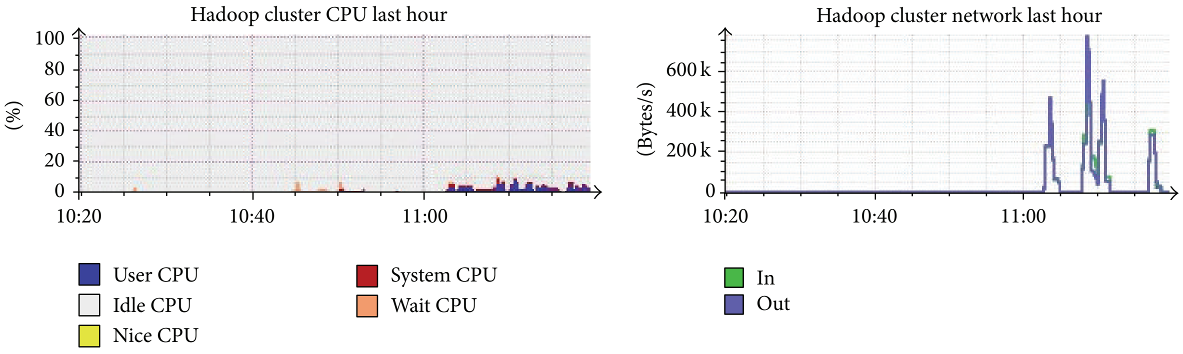
Seen from Figure 5, there are 4 Sunspot nodes in the simulation scenario. Two source nodes collect healthcare information by biosensors and send their data to the intermediate node, the intermediate node transmits the measure value to base station, and base station receives the message. Sunspot node 1 executes ECC digital signature algorithm to protect measure value from biosensors, while Sunspot node 2 does not use ECC algorithm to protect the measure value. We suppose that the intermediate node maybe be attacker, so the intermediate node can tamper with the measure value which is transmitted by it. When the tampered with message is received by base station, if the message is protected by ECC digital signature algorithm, the tampered with message cannot pass the verification; it will be discarded; the tampering attack behaviour can be detected in healthcare secure communication system; otherwise, if Sunspot node 2 cannot execute ECC signature algorithm, base station cannot



(a) Hadoop cluster load last hour.

(b) Hadoop cluster memory last hour.

Figure 6: Hadoop cluster load and memory statistic results.



(a) Hadoop cluster CPU last hour.

(b) Hadoop cluster network last hour.

Figure 7: Hadoop cluster CPU and network statistic.

verify the message; as the tampered with message is not correct, it may misdirect the doctor and harm the patient.

6. Using Hadoop to Store and Audit Data

Hadoop is an open source cloud computing and big data storage platform. It is used to store and audit the data measured by Sunspot in this paper. Sqoop is a software tool which can transfer data between Hadoop HDFS (Hadoop distributed file system) and structured databases such as Mysql.

In our Hadoop storage experiments, five computer nodes are used to build cloud storage system. One of them is namenode; the other four nodes are datanodes. The import instruction of Sqoop is used to periodically import data tables from Mysql database to Hadoop HDFS. The data tables include Sunspot security entity table and Sunspot measure entity table. Only security entity table is exported to Hadoop HDFS. To ensure the secure audit, only security administrators are granted access to the audit data stored in the Hadoop HDFS. If the security administrator doubts that the security entity table is tampered with, he can check the data on the Hadoop HDSF to detect the tampering attack behaviour. Ganglia tool is used to monitor Hadoop's running status, when the table is imported/exported by Sqoop. The monitoring result of Hadoop is shown in Figures 6 and 7. Hadoop load and memory statistics results are shown in Figure 6.

Seen from Figure 6(a), the time range of statistic results is from 10:20 AM to 11:20 AM. When Hadoop cluster sets up at about 10:26, the number of running processes increases quickly when Hadoop initializes the cluster system. When security entity table is imported/exported from 11:05 AM to 11:15 AM, the number of process increases a little. It shows that import/export operations of Sqoop only use less process resource.

Seen from Figure 6(b), when security entity table is imported, the memory usage rate increases a little. It shows that import operation of Sqoop occupies a little memory resource. When Hadoop cluster sets up, the cluster memory almost keeps constant; it implies that the initial process of Hadoop almost occupies less memory resource. The statistics results show the difference between Hadoop initialization and Sqoop import/export operation.

The CPU and Network statistics results are shown in Figure 7.

Seen from Figure 7(a), when data table is imported/exported between Mysql and Hadoop from 11:05 AM to 11:20 AM, there are only small waves in User CPU usage curve; the average User CPU usage is about 10% between 11:05 AM and 11:20 AM. Wait CPU usage curve only waves a little from 10:20 AM to 11:00 AM.

Seen from Figure 7(b), there are 4 peaks from 11:05 AM to 11:20 AM in Hadoop cluster network statistics graph. We execute Sqoop import instruction for three times and Sqoop

Table 2: Comparison with other works.

Healthcare architecture	Technique and method		
	Lightweight digital signature	Big data storage	Interaction with relational database
Our architecture	Support	Support	Support
SNEP and μTesla [11]	Support	No	No
Cloudwave [18]	No	Support	No
MedCloud [13]	No	Support	Support

export instruction only once during 11:05 AM–11:20 AM, and the heights of three peaks are different because the amounts of import data are different. In the second import operation, the amount of import data is maximum. The last peak is the lowest, because data export operation occupies less network bandwidth.

7. Compare the Presented Architecture to Related Works

To show the advantage of our scheme, we compare the presented architecture with related works, which are SNEP and μTesla [11], Cloudwave [18] and MedCloud [13]. We compare them from three aspects: lightweight digital signature, big data storage, and interaction with relational database, which are important in the security of wireless healthcare system. The comparison result is shown in Table 2.

Seen from Table 2, our architecture supports lightweight digital signature, big data storage, and interaction with relation database, which achieved better results than other works. Our architecture can meet the security requirement of wireless communication and big data storage in healthcare information system; at the same time, it can exchange data with traditional database.

8. Conclusion

Recently, biosensor based healthcare information systems attract many researchers and engineers' attentions with the development of microelectronic, Bioinformatics science, embedded computing, wireless communication, and cloud computing. How to use different kinds of biosensors to build an efficient healthcare information system is a challenge problem to current researchers. A novel Hadoop-based wireless healthcare system architecture is proposed in this paper; Sunspot wireless nodes are used to build the wireless biosensor network. A lightweight ECC digital signature algorithm is used to provide secure communication between wireless node and base station. Hadoop cloud platform is used to backup and recover Sunspot security entity table. Sunspot simulation platform and Hadoop cluster are used to validate wireless healthcare system and secure communication method. The main contributions of this paper are the following three aspects:

(1) A novel Hadoop-based biosensor Sunspot wireless network architecture is proposed to build human healthcare information system. Multidiscipline knowledge is used to construct a complex healthcare system, such as bioinformation science, wireless sensor network, cryptograph and information security, security communication, database and information system, human-machine interaction, and cloud computing.

(2) To ensure the data communication security in healthcare system, a lightweight ECC digital signature algorithm and Hadoop-based data backup and recovery method are proposed to authenticate Sunspot wireless node and protect Sunspot key.

(3) Sqoop tool is used to import/export data between Mysql database and Hadoop HDFS cloud storage; security administrator can use it to protect and manage key data.

Simulation and monitoring results show that our healthcare information system architecture and secure communication method are highly effective to counter potential data tampering attacks. In the future, more sensor types, such as Beidou position sensor will be integrated in wireless node to provide patient's precise position information. To ensure the security of measure value, lightweight encryption algorithm will be used to protect the confidentiality of measure value. At the same time, more information will be imported from Mysql database to Hadoop HDFS to improve the security of healthcare information system.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work was supported by Beijing Natural Science Foundation (4142034), China Scholarship Council Foundation, Beijing Higher Education Young Elite Teacher Project (YETP0380), Fundamental Research Funds for the Central Universities (no. FRF-TP-14-042A2), Beijing municipal science and technology plan Project (no. D141100003414002), and Chinese National 863 research Project (no. 2013AA01A209).

References

[1] B. E. Rapp, F. J. Gruhl, and K. Länge, "Biosensors with label-free detection designed for diagnostic applications," *Analytical and Bioanalytical Chemistry*, vol. 398, no. 6, pp. 2403–2412, 2010.

[2] P. T. Kissinger, "Biosensors—a perspective," *Biosensors and Bioelectronics*, vol. 20, no. 12, pp. 2512–2516, 2005.

[3] A. Bharathidasan and V. Ponduru, “Sensor networks: an overview,” in *Proceedings of the 23rd Conference of the IEEE Communications Society (INFOCOM ’04)*, Hong Kong, March 2004.

[4] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, 2002.

[5] A. Perrig, J. Stankovic, and D. Wagner, “Security in wireless sensor networks,” *Proceedings of the Communications of the ACM*, vol. 47, no. 6, pp. 53–57, 2004.

[6] C. Haowen and A. Perrig, “Security and privacy in sensor networks,” *Computer*, vol. 36, no. 10, pp. 103–105, 2003.

[7] T. Vo-Dinh, “Biosensors, nanosensors and biochips: frontiers in environmental and medical diagnostics,” in *Proceedings of the 1st International Symposium on Micro & Nano Technology*, pp. 14–17, Honolulu, Hawaii, USA, 2004.

[8] T. Vo-Dinh, “Nanobiosensors: probing the sanctuary of individual living cells,” *Journal of Cellular Biochemistry*, no. 39, pp. 154–161, 2002.

[9] S. Cherukuri, K. Venkatasubramanian, and S. K. S. Gupta, “Biosec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body,” in *Proceedings of the International Conference on Parallel Processing Workshops*, pp. 432–439, IEEE, October 2003.

[10] C. C. Y. Poon, Y.-T. Zhang, and S.-D. Bao, “A novel biometrics method to secure wireless body area sensor networks for telemedicine and M-health,” *IEEE Communications Magazine*, vol. 44, no. 4, pp. 73–81, 2006.

[11] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, “SPINS: security protocols for sensor networks,” in *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking (MOBICOM ’01)*, pp. 189–199, July 2001.

[12] H. Yu and D. Wang, “Research and implementation of massive health care data management and analysis based on hadoop,” in *Proceedings of the 4th International Conference on Computational and Information Sciences (ICCIS ’12)*, pp. 514–517, IEEE, August 2012.

[13] D. Sobhy, Y. El-Sonbaty, and M. Abou Elnasr, “MedCloud: healthcare cloud computing system,” in *Proceedings of the 7th International Conference for Internet Technology and Secured Transactions (ICITST ’12)*, pp. 161–166, IEEE, London, UK, December 2012.

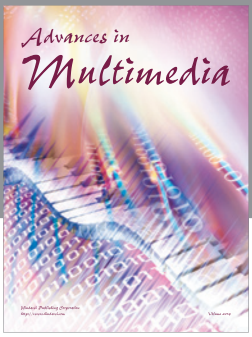
[14] H. Kojima, K. Nagahashi, and K.-I. Okada, “Proposal of the disaster-relief training system using the electronic triage tag,” in *Proceedings of the 25th IEEE International Conference on Advanced Information Networking and Applications (AINA ’11)*, pp. 256–263, March 2011.

[15] L.-C. Huang, H.-C. Chu, C.-Y. Lien, C.-H. Hsiao, and T. Kao, “Privacy preservation and information security protection for patients’ portable electronic health records,” *Computers in Biology and Medicine*, vol. 39, no. 9, pp. 743–750, 2009.

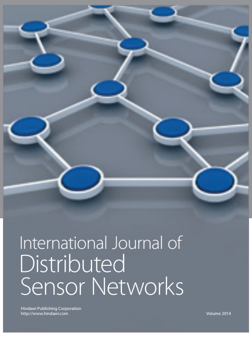
[16] https://developer.ibm.com/hadoop/docs/integration/guardium/big-data-security-auditing-ibm-infosphere-guardium/.

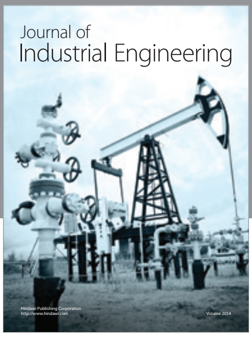
[17] I.-Y. Jung, K.-H. Kim, B.-J. Han, and C.-S. Jeong, “Hadoop-based distributed sensor node management system,” *International Journal of Distributed Sensor Networks*, vol. 2014, Article ID 601868, 7 pages, 2014.

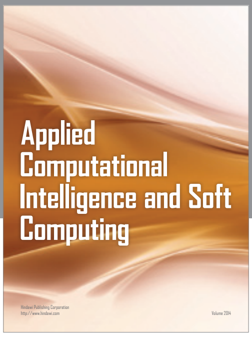
[18] S. S. Sahoo, “Biomedical big data for clinical research and patient care: role of semantic computing,” in *Proceedings of the IEEE International Conference on Semantic Computing (ICSC ’14)*, pp. 3–5, June 2014.

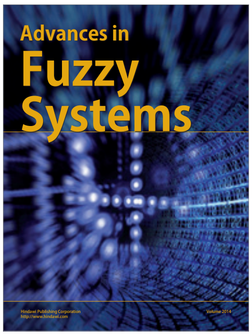

Advances in
Multimedia

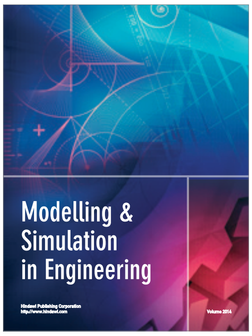
The Scientific
World Journal

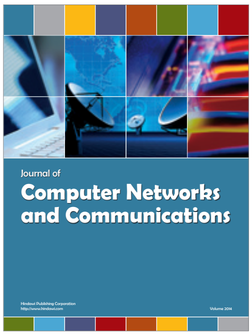

International Journal of
Distributed
Sensor Networks

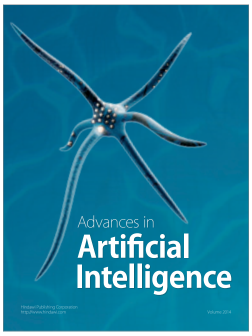

Journal of
Industrial Engineering

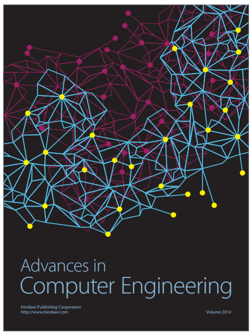

Applied
Computational
Intelligence and Soft
Computing


Advances in
Fuzzy
Systems

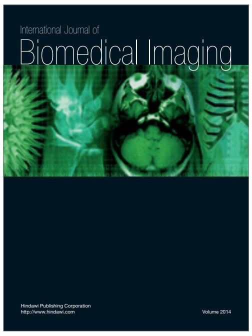

Modelling &
Simulation
in Engineering

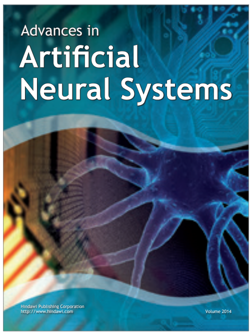

Journal of
Computer Networks
and Communications

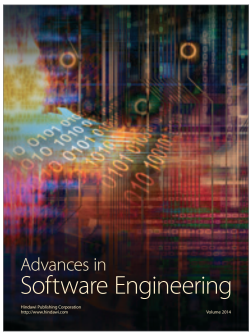

Advances in
Artificial
Intelligence


Advances in
Computer Engineering

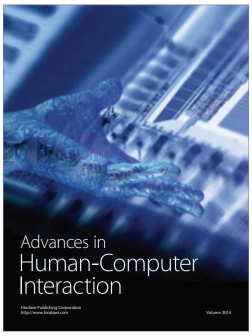
International Journal of
Computer Games
Technology

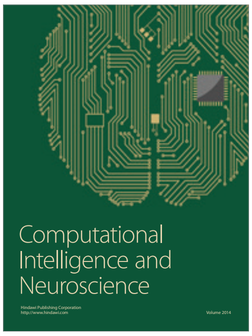

International Journal of
Biomedical Imaging


Advances in
Artificial
Neural Systems


Advances in
Software Engineering

Journal of
Robotics


Advances in
Human-Computer
Interaction


Computational
Intelligence and
Neuroscience

International Journal of
Reconfigurable
Computing

Journal of
Electrical and Computer
Engineering