International Journal of Cryptology Research 4(1): 84 - 101 (2013)

Design and Implementation of Key-Policy Attribute-Based Encryption in Body Sensor Network

[1]Yar-Ling Tan, [2*] Bok-Min Goi, [3]Ryoichi Komiya, and [4]Raphael Phan

[1]Universiti Tunku Abdul Rahman,
Building PD No.9, Jalan Bersatu 13/4,
46200 Petaling Jaya, Selangor, Malaysia

[4]Multimedia University, Jalan Ayer Keroh Lama,
75450, Ayer Keroh, Melaka, Malaysia

E-mail: yarling@1utar.my, goibm@utar.edu.my, ryoichi@utar.edu.my and raphael@mmu.edu.my

*Corresponding author

ABSTRACT

Body sensor network (BSN) is a set of sensors attached to patients' body to collect vital signs. The vital signs will be sent from patients' smart phone or personal computer via BSN coordinator to the remote healthcare provider's server. This will enable patients' vital signs to be monitored by healthcare people via internet. However, security is necessary for the patients' personal data including vital signs. The patients' personal data and vital signs are referred to as medical information. Therefore, encryption needs to be applied to patient's medical information. In this paper, we propose an implementation of key-policy attribute-based encryption (KP-ABE) in order to encrypt the medical information and present an encryption/decryption prototype system of KP-ABE in BSN. KP-ABE allows fine-grained sharing of encrypted data. It is able to provide differential access rights for different users. Thus, the encryption allows flexibility in changing access rights of individual users over the encrypted data.

1. INTRODUCTION

The current technology has brought remarkable contribution and advancement to the electronic healthcare devices today. The advancement of electronic healthcare devices is essential for monitoring and early prevention of various diseases such as heart diseases, diabetes, hypertension, chronic obstructive pulmonary disease (COPD), and other chronic diseases.

Body sensor network [1-4], is one of the smallest personal electronic healthcare networks which has been studied and tested its availability all over the world. Body sensor network (BSN) is composed of wearable computing device with a set of sensors attached to different parts of human body to collect vital signs. The vital signs to be collected are body temperature, blood pressure, pulse rate (or heart rate), respiratory rate and etc. BSN is a wireless network that enables sensors to send the vital signs to mobile computing device (e.g. smart phone) or a computing unit via BSN coordinator. Then they will be sent to the third party remote server to be stored. In this way, patient can be monitored in real time or non-real time basis remotely from the hospital [5].

The medical information stored at the remote server will be shared among different users (e.g. doctors, nurses, pharmacies, patient and etc.). Thus, privacy, confidentiality and security issues for the medical informationshould be a major concern in this topic. Therefore, it is important for the medical information to be encrypted before sending to the third party remote server. Encryption is one of the potent approaches to secure medical information. Many research works have been done in order to secure the medical information of the BSN [6-10].

Attribute-based encryption (ABE) [11-14], is a fine-grained access control system, which enables a set of users to have differential access rights. On the other hand, ABE is also flexible in defining the access rights of each user. There are two major types of ABE; key-policy attribute-based encryption (KP-ABE)[15-16], and ciphertext-policy attribute-based encryption (CP-ABE) [17-19]. In this paper, we propose an implementation of KP-ABE scheme to apply the encryption to patient's medical information. KP-ABE encryption time is shorter than CP-ABE. Besides that, KP-ABE has less restriction and limitation on the authorized users who are able to apply decryption to the encrypted medical information. Authorized user (e.g. medical operator) is able to perform decryption if his/her access policy matches the attributes assigned to the encrypted vital signs. In hardware implementation, KP-ABE is also advantageous. KP-ABE scheme is able to realize the lightweight encryption and producing smaller ciphertext size than CP-ABE in a resource constraint device [20]. We have implemented a prototype which is composed of BSN to collect vital signs from human body and a laptop to perform the encryption/decryption of patient's medical information.

2. BACKGROUND

In 1984, Shamir introduced a novel type of public encryption scheme called Identity-Based Encryption scheme (IBE) [21], which enable users to securely communicate, verify and exchange each other's signatures without any exchange of private or public keys. Thus, eliminates the need to keep key directories. Instead of generating a random pair of public/secret key and made the public key known to everyone, the public key can be in a form of any arbitrary string. For example, names, home address, phone number, e-mail address and etc. provided that the user can be uniquely identified which he cannot later deny. In year 2001, Boneh and Franklin proposed the first secure and practical IBE [22] from the Weil pairing on elliptic curves.

In 2005, Sahai and Waters introduced a new type of IBE scheme called Fuzzy Identity-Based Encryption (FIBE) [23]. In IBE, identities are viewed as arbitrary strings. While in FIBE, identities are being viewed as a set of descriptive attributes. FIBE scheme allows a user with private key corresponding to a set of identity, *ID* to decrypt a ciphertext encrypted with the public key, *ID'* if and only if *ID* and *ID'* overlap each other by some distance metric, *d*. Therefore, FIBE system allows a certain amount of error-tolerance in the identities. The authors also mentioned on the application of FIBE termed as Attribute-Based Encryption (ABE). In an ABE system, a user's private key and ciphertext are labeled with a set of attributes. A particular private key can decrypt a particular ciphertext only if there is a match between the attributes of the user's private key and ciphertext.

After ABE was first introduced in the work of Sahai and Waters, in year 2006, Goyal et al. proposed the Key-Policy Attribute Based Encryption (KP-ABE) for fine-grained sharing of encrypted data [15]. Encryption of data usually limits the ability of encrypted data to be shared among different users. In other words, the encrypted data can only be selectively shared at a coarse-grained level. For example, in order to perform data decryption, user needs to give his/her private key to another party. This somehow allows another party to have all the access of the user's data. Another alternative, user can act as an intermediary to perform decryption on the relevant data but this method is arduous. Both approaches are not appealing as they are impractical and inefficient.

In KP-ABE, each ciphertext is labeled with a set of descriptive attributes, while the access structure is embedded in the user's private key. User is able to decrypt a ciphertext if the access structure embedded in the private key matches the descriptive attributes labeled in the ciphertext. Fine-grained sharing of encrypted data enables different authorized users to retrieve and decrypt ciphertext based on their access structure. KP-ABE scheme is able to grant different access rights to different users.

In year 2007, Bethen court et al. provides the first construction of a ciphertext-policy attribute-based encryption (CP-ABE) scheme [17]. In

CP-ABE scheme, access structure is use in data encryption while the descriptive attributes are embedded in the user's private key. A user is able to decrypt the ciphertext if his descriptive attributes satisfy the access structure associated to the ciphertext. Table 1 summarizes the terminology definition in this section.

TABLE 1: Terminology List

Terminology	Definition	Example
Attributes	Identities of a person	Name, home address, e-mail address, identity number, phone number
Access Structure	A policy/structure to define an authorized person	{("Dept of Medical Services" **AND** "Specialist") **AND** ("Kuala Lumpur" OR "Penang") **OR** "Name: Dr. Jehovah"}
Private Key Generator	A trusted third party that handles the issuance of private keys	

3. IMPLEMENTATION

This section shows the implementation of our work. This section is divided into a few subsections; body sensor network, attribute-based encryption scheme, and our prototype setup.

3.1 Body Sensor Network

BSN is applicable to healthcare, well-being monitoring, sports and entertainment [24-26]. Different activities require different set of sensors. In our work, we focus on the healthcare applications by using BSN. The needs of healthcare applications are emanate from the increase of chronic diseases, aging population and early diseases prevention and detection.

BSN for healthcare application is dynamic. It can be used at anytime, anywhere and for anybody. It provides continuous medical information collections and transmissions on real time or non-real time basis to hospital server which helps the hospital personnel to diagnose the patients outside the hospital.

The BSN which we have implemented has four major components which are the processor, radio frequency transceiver, battery and sensor. It is designed to have three modules. The three modules are battery, sensor and BSN node. The BSN node consists of processor and radio frequency transceiver. The BSN is a stackable design to connect and interface between the modules. We have implemented two types of body sensor nodes which measure temperature and 3D motion. The BSN node can transmit and receive vital signs within the range of approximately 50 meters indoor. Figure 1 shows the body sensor node manufactured by Sensixa Ltd. Company[27].

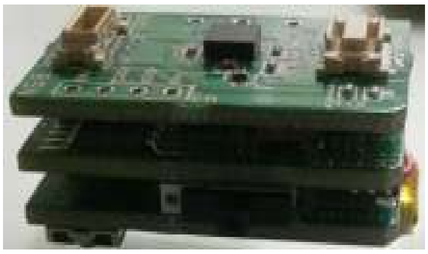


Figure 1: Body Sensor Node

3.2 Attribute-Based Encryption Scheme (ABE)

Comparisons between KP-ABE and CP-ABE schemes are studied and analysed to determine their propriety in BSN [11]. Comparisons were conducted in terms of encryption efficiency/time, attribute and access structure's assignment, access control and hardware implementation.

In our work, we have intended to achieve a lightweight and secure encryption. In KP-ABE, encryption is performed by using descriptive attributes. Access structure is embedded in the private key which is issued by private key generator (PKG). In CP-ABE, encryption is performed by using the access structure. Descriptive attributes are embedded in the private key issued by PKG.

Encryption performs by using descriptive attributes has lower encryption complexity and shorter computation time than encryption to be performed by using access structure. Moreover, medical information is being encrypted at a continuous basis, while key generation for each authorized users is being generated once. Therefore, KP-ABE encryption scheme is more appropriate to be implemented in our work.

Patients are involved in the assignment of descriptive attributes or access structure with the assistance from medical agents. Assignment of descriptive attributes in KP-ABE for encryption purpose is much simpler and less time consuming than assignment of access structure in CP-ABE encryption. This is because a slight update mistake in the access structure would cause a complication in the entire encryption and decryption system.

Furthermore, in terms of access control, KP-ABE allows higher flexibility and efficiency in the modification of access control towards any authorized personnel compared to CP-ABE. This is because the updates made on the descriptive attributes are much simpler than updates made on access structure.

In KP-ABE, the encryption time is shorter and ciphertext size is smaller than CP-ABE. This is because the high complexity and processing work to embed the access structure in private keys are done by the PKG. However, for CP-ABE, the encryption computation time is longer and the ciphertext size is larger. Therefore, in terms of hardware implementation, KP-ABE is advantageous.

For our prototype, we have implemented the KP-ABE scheme as this scheme is more suitable than CP-ABE in terms of light weight and less power consumption [11]. In KP-ABE scheme as shown in Figure 2, attributes are labeled in the encrypted medical information (vital signs and patient’s personal data). Access structure is embedded in the private key. The private key is issued by a trusted private key generator (PKG). This is an advantage of KP-ABE scheme where attributes label in the encrypted medical information can be easily created and altered. The tedious task of access structure creation and alteration is handled by professional PKG creator.

The KP-ABE scheme consists of four algorithms [15].

- Setup (1^k): The setup algorithm takes as input a security parameter, 1^k and outputs the public parameters, *PK* and a master key, *msk* which is known only to the private key generator (PKG).

- Encrypt (*m, PK, γ*): The encryption algorithm takes as input a message, *m*, a set of attributes, γ and the public parameters, *PK.* It outputs the ciphertext, *c*.

- Key Generation (*PK*, msk,): The key generation algorithm takes as input the public parameters, *PK*, the master key, *msk* and an access policy, . It outputs the private key, *D* .

- Decrypt (*c*, *PK*, *D*): The decryption algorithm takes as input the ciphertext, *c* which was encrypted under the set of attributes, *γ*, the public key parameter, *PK* and the private key, *D* for access control structure, . It outputs the message *m* if *γ*∈ .

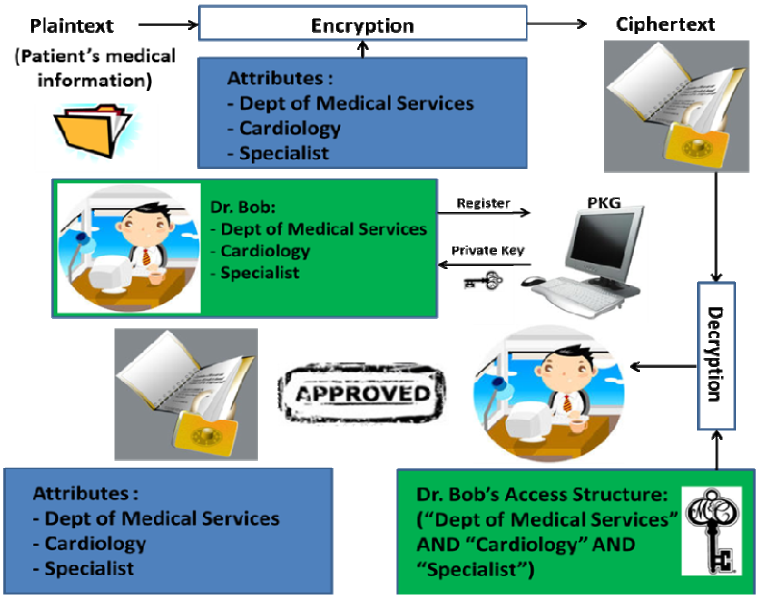

Plaintext
(Patient's medical information)
Encryption
Ciphertext
Attributes :
- Dept of Medical Services
- Cardiology
- Specialist
Dr. Bob:
- Dept of Medical Services
- Cardiology
- Specialist
Register
PKG
Private Key
Decryption
APPROVED
Attributes :
- Dept of Medical Services
- Cardiology
- Specialist
Dr. Bob's Access Structure:
("Dept of Medical Services" AND "Cardiology" AND "Specialist")

Figure 2: Key-Policy Attribute-Based Encryption and Decryption

3.3 Prototype Setup

We have attached the sensor nodes to the human body as shown in Figure 3 to collect temperature and 3D motion readings. The readings are transmitted to the BSN coordinator which is connected to a personal computer (PC). In the PC, KP-ABE encryption and decryption is performed.

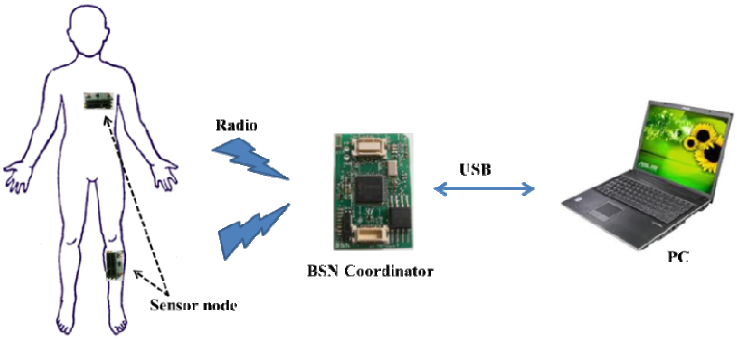


Figure 3: Prototype configuration

PC:
Send commands to, and receives vital signs from the BSN-network. Encrypt the vital signs using KP-ABE encryption.

BSN-coordinator:
Receives commands from, and sends vital signs to the laptop.

(i) Connection between BSN nodes and BSN coordinator

Vital signs are sent from sensor nodes to the BSN coordinator via radio transceiver – CC2420, as shown in Figure 4. The CC2420 is a single-chip 2.4 GHz IEEE 802.15.4 compliant RF transceiver with an effective data transfer rate of 250 kbps. It is designed for low-voltage and low-power wireless RF applications. The CC2420 provides hardware support for AES-128 based data encryption and data authentication.

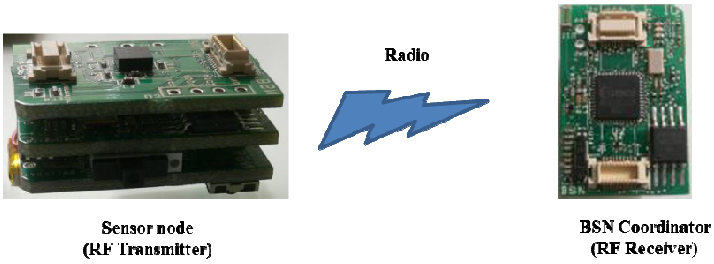


Figure 4: BSN-Network

RF Transmitter:
Toggles the red LED and send the vital signs in packet. Each packet contains a sequence number in the packet header, which increases by one after a packet is sent out.

RF Receiver:
Toggles the red LED and receives data packets sent from RF Transmitter and check their sequence numbers in the packet header.

(ii) Connection between BSN coordinator and PC

Vital signs sent from the sensor nodes will then be received by the BSN coordinator and be transmitted to the PC via universal serial bus (USB) as shown in Figure 5. In order to collect the vital signs, PC first sends out a request. The BSN coordinator will then transmit a message to all the BSN sensor nodes or only to the selected sensor nodes. When the BSN sensor nodes receive the message, they will then transmit the vital signs to the BSN coordinator. After that, through the USB connection, the PC will receive the vital signs. The number of nodes can be altered accordingly to accommodate the number of vital signs types require to be collected.

In our work, BSN sensor node 1 will retrieve the human body temperature, and BSN sensor node 2 retrieves the 3D motion of human body.

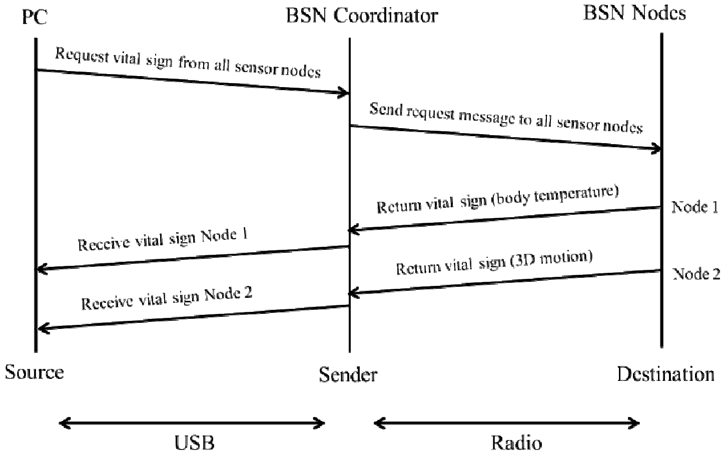

PC
BSN Coordinator
BSN Nodes
Request vital sign from all sensor nodes
Send request message to all sensor nodes
Return vital sign (body temperature)
Node 1
Receive vital sign Node 1
Return vital sign (3D motion)
Node 2
Receive vital sign Node 2
Source
Sender
Destination
USB
Radio

Figure 5: Connection between PC, BSN coordinator and sensornodes

3.4 KP-ABE Encryption in PC

Once the vital signs are sent to the PC, the PC will perform the KP-ABE encryption on the vital signs. In our implementation, we used the key-policy attribute-based encryption library (*libcelia*). It is a subroutine library implementing KP-ABE scheme and kpa be toolkit created by Yao Zheng [28].

Figure 6 illustrates the process flow of the encryption and decryption. Figure 9shows the screenshot of correct encryption and decryption.

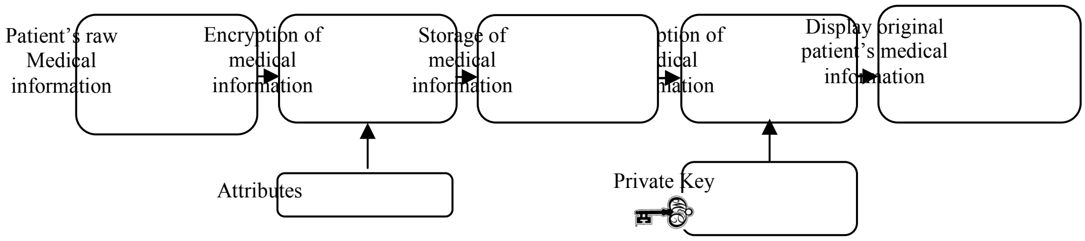

Patient's raw Medical information
Encryption of medical information
Storage of medical information
ption of dical mation
Display original patient's medical information
Attributes
Private Key

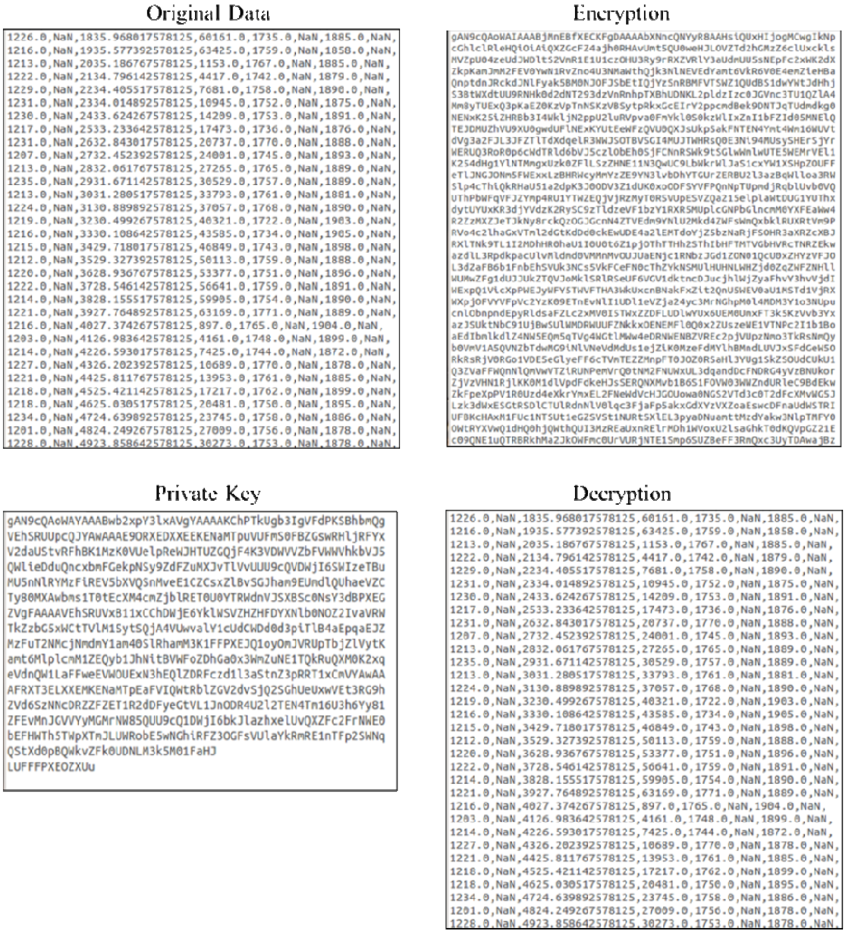
Figure 6: Diagram of Process Flow of Encryption and Decryption

- *kpabe-setup* : The setup algorithm generates system parameters, a public key, and a master secret key under set of attributes.
- *kpabe-enc*: Encryption algorithm encrypt medical information of patient under a set of attributes.
- *kpabe-keygen*: The key generation algorithm generates a private key and sends to the authorized medical operators.
- *kpabe-dec*: The decryption algorithm takes as input the encrypted medical information under a set of attributes, the public key parameters and the private key generated by kpabe-keygen. It then outputs the message original file if access structure embedded in the private key matched the attributes.

4. RESULTS OF EXPERIMENT

Section 4 shows the results of the experiment. The results shown are correct encryption and decryption as well as the incorrect encryption and decryption. We show 2 types of incorrect encryption and decryption; decryption using incorrect key and decryption using incorrect wording.

4.1 Correct Encryption and Decryption



Original Data

```
1226.0,NaN,1835.968017578125,60161.0,1735.0,NaN,1885.0,NaN,
1216.0,NaN,1935.577392578125,63425.0,1759.0,NaN,1858.0,NaN,
1213.0,NaN,2035.186767578125,1153.0,1767.0,NaN,1885.0,NaN,
1222.0,NaN,2134.796142578125,4417.0,1742.0,NaN,1879.0,NaN,
1229.0,NaN,2234.405517578125,7681.0,1758.0,NaN,1890.0,NaN,
1231.0,NaN,2334.014892578125,10945.0,1752.0,NaN,1875.0,NaN,
1230.0,NaN,2433.624267578125,14209.0,1753.0,NaN,1891.0,NaN,
1217.0,NaN,2533.233642578125,17473.0,1736.0,NaN,1876.0,NaN,
1231.0,NaN,2632.843017578125,20737.0,1770.0,NaN,1888.0,NaN,
1207.0,NaN,2732.452392578125,24001.0,1745.0,NaN,1893.0,NaN,
1213.0,NaN,2832.061767578125,27265.0,1765.0,NaN,1889.0,NaN,
1235.0,NaN,2931.671142578125,30529.0,1757.0,NaN,1889.0,NaN,
1213.0,NaN,3031.280517578125,33793.0,1761.0,NaN,1881.0,NaN,
1224.0,NaN,3130.889892578125,37057.0,1768.0,NaN,1890.0,NaN,
1219.0,NaN,3230.499267578125,40321.0,1722.0,NaN,1903.0,NaN,
1216.0,NaN,3330.108642578125,43585.0,1734.0,NaN,1905.0,NaN,
1215.0,NaN,3429.718017578125,46849.0,1743.0,NaN,1898.0,NaN,
1212.0,NaN,3529.327392578125,50113.0,1759.0,NaN,1888.0,NaN,
1220.0,NaN,3628.936767578125,53377.0,1751.0,NaN,1896.0,NaN,
1222.0,NaN,3728.546142578125,56641.0,1759.0,NaN,1891.0,NaN,
1214.0,NaN,3828.155517578125,59905.0,1754.0,NaN,1890.0,NaN,
1221.0,NaN,3927.764892578125,63169.0,1771.0,NaN,1889.0,NaN,
1216.0,NaN,4027.374267578125,897.0,1765.0,NaN,1904.0,NaN,
1203.0,NaN,4126.983642578125,4161.0,1748.0,NaN,1899.0,NaN,
1214.0,NaN,4226.593017578125,7425.0,1744.0,NaN,1872.0,NaN,
1227.0,NaN,4326.202392578125,10689.0,1770.0,NaN,1878.0,NaN,
1221.0,NaN,4425.811767578125,13953.0,1761.0,NaN,1885.0,NaN,
1218.0,NaN,4525.421142578125,17217.0,1762.0,NaN,1899.0,NaN,
1218.0,NaN,4625.030517578125,20481.0,1750.0,NaN,1895.0,NaN,
1234.0,NaN,4724.639892578125,23745.0,1758.0,NaN,1886.0,NaN,
1201.0,NaN,4824.249267578125,27009.0,1756.0,NaN,1878.0,NaN,
1228.0,NaN,4923.858642578125,30273.0,1753.0,NaN,1878.0,NaN,
```

Encryption

```
gAN9cQAoWAIAAABjMnEBfXECKFgDAAAAbXNncQNYyR8AAHsiQUxHIjogMCwgIkNp
cGhlclRleHQiOiAiQXZGcFZ4ajh0RHAvUmt5QU0weHJLOVZTd2hGMzZ6clUxckls
MVZpU04zeUdJWDltS2VnR1E1U1czOHU3Ry9rRXZVRlY3aUdmUU5sNEpFc2xWK2dX
ZkpKamJmM2FEV0YwN1RvZno4U3NMawthQjk3NlNEVEdYamt6VkR6V0E4emZ1eHBa
QnptdnJRckdJNlFyak5BM0NJOFJSbEtIQjYzSnRBMFVTSWZ1QUdBS1dwYWtJdHhj
S3BtWXdtUU9RNHk0d2dNT293dzVnRnhpTXBhUDNKL2pldzIzc0JGVnc3TU1QZlA4
Mm8yTUExQ3pKaEZ0KzVpTnNSKzVBSytpRkxGcEIrY2ppcmdBek9DNTJqTUdmdkg0
NENxK2SiZHRBb3I4WkljN2ppU2luRVpva0FmYkl0S0kzWlIxZnI1bFZId0SMNElQ
TEJDMUZhVU9XU0gwdUFlNExKYUtEeWFzQVU0QXJsUkpSakFNTEN4Ymt4Wn16WUVt
dVg3a2FJL3JFZTlTdXdqelR3WWJSOTBVSGI4MUJTWHRSQ0E3Ni94MUsySHErSjYr
WERUQ3RoR0p6cWdTRld6bVJ5czlObEh0SjFCNnRSWk9tSGlwWnlwUTE5WEMrVEl1
K2S4dHg1YlNTMmgxUzk0ZFlLSzZHNE11N3QwUC9LbWkrWlJaS1cxYW1XSHpZOUFF
eTlJNGJONm5FWExxLzBHRWcyMmYzZE9YN3lvbDhYTGUrZERBU2l3azBqWlloa3RW
Slp4cThiQkRHaU51a2dpK3J0ODV3Z1dUK0xoODFSYVFPQnNpTUpndjRqblUvb0VQ
UThPbWFqVFJZYmp4RU1YTWZEQjVjRzMyT0RSVUpESVZQaz15elplaWtDUG1YUThx
dytUYUxKR3djYVdzK2RySC9zTldzeVF1bzY1RXRSMUplcGNPbGlncmM0YXFEaWw4
R2ZzMXZJeTJkNy8rckQzOGJGcnN4ZTVEdm9YNlU2Mkd4ZWFsWmQxbklRUXRtVm9P
RVo4c2lhaGxVTml2dGtKdDd0ckEwUDE4a2lEMTdoYjZ5bzNaRjFSOHR3aXRZcXBJ
RXlTNk9TL1I2MDhHR0haU1I0U0toZ1pjOThTTHh2SThIbHFTMTVGbHVRcTNRZEkw
azdlL3RpdkpacUlvMldndDVMMnMvOUJUaENjc1RNbzJGd1ZON01QcUUxZHYzVFJO
L3dZaFB6b1FnbEhSVUk3NCs5VkFCeFN0cThZYkNSMUlHUHNLWHZjd0ZqZWFZNHll
WUMwZFg1dUJJUk2TQVJoMklSRlRSeUF6VCV1dktncDJucjhlWjZyaFhvV3hvVjdI
WExpQ1VlcXpPWEJyWFY5THVFTHA3WkUxcnBNakFxZlt2QnU5WEV0aU1MSTd1VjRX
WXpjOFVYVFpVc2YzK09ETnEvNlI1UDl1eVZja24yc3MrNGhpM0l4MDM3Y1o3NUpu
cnlObnpndEpyRldsaFZLc2xMV0I5TWxZZDFLUDlWYUx6UEM0UmxFT3k5KzVvb3Yx
azJSUktNbC91UjBwSUlWMDRWUUFZNkkxOENEMFl0Q0x2ZUszeWE1VTNPc2I1b1Bo
aEdIbmlkdlZ4NW5EQm5qTVg4WGtlMWw4eDRNWENNBZVREc2pjVUpzNmo3TkRsNmQy
b0VmV1A5QVN2bTdwMG9iNlVNeVdMdUs1ejZlK0MzeFdMYlhBMmdLUVJxSFdGeW5O
RkRsRjVORGo1VDE5eGlyeFF6cTVnTEZZMnpFT0JOZ0RSaHlJYUg1SkZSOUdCUkU1
Q3ZVaFFWQnNlQmVwYTZiRUNPemVrQ0tNM2FNUWxUL3dqandDcFNDRG4yVzBNUkor
ZjVzVHN1RjlKK0M1dlVpdFdkeHJsSERQNXMvb1B6S1FOVW03WWZndURleC9CdEkw
ZkFpeXpPV1R0Uzd4eXkrYmxxEL2FNeWdVcHJGGOUowa0NGS2VTd3c0T2dFcXMvWGSJ
Lzk3dWxESGtRSDlCTUlRdnNlV0lqc3FjaFpGakxGdXYzVXZoaEswcDFnaUdWSTRI
UF0KcHAxM1FUc1NTSUtieGZSVStiNURtSXlEL3B5aDNuamttMzdYakw3NlpTMFY0
OWtRYXVwQ1dhQ0hjQWthQUI3MzREaUxnRElrMDh1WVoxU2lsaGhkT0dKQVpGZ21E
c09QNE1uQTRBRkhMa2JkOWFmc0UrVURjNTE1Smp6SUZBeFF3RmQxc3UyTDAwajBz
```

Private Key

```
gAN9cQAoWAYAAABwb2xpY3lxAVgYAAAAKChPTkUgb3IgVFdPKSBhbmQg
VEhSRUUpcQJYAWAAAE9ORXEDXXEEKENaMTpuVUFmS0FBZGSWRHljRFYX
V2daUStvRFhBK1MzK0VUelpReWJHTUZGQjF4K3VDWVVZbFVWWVhkbVJ5
QWlieDduQncxbmFGekpNSy9ZdFZuMXJvTlVvUUU9cQVDWjI6SWIzeTBu
MU5nNlRYMzFiREV5bXVQSnMveE1CZCsxZlBvSGJham9EUndlQUhaeVZC
Ty80MXAwbms1T0tEcXM4cmZjblRET0U0YTRWdnVJSXBSc0NsY3dBPXEG
ZVgFAAAAVEhSRUVxB11xCChDWjE6YklWSVZHZHFDYXNlb0NOZ2IvaVRW
TkZzbGSxWCtTVlM1SytSQjA4VUwvalY1cUdCWDd0d3piTlB4aEpqaEJZ
MzFuT2NMcjNmdmY1am40SlRhamM3K1FFPXEJQ1oyOmJVRUpTbjZlVytK
amt6MlplcmM1ZEQyb1JhNitBVWFoZDhGa0x3WmZuNE1TQkRuQXM0K2xq
eVdnQW1LaFFweEVWOUExN3hEQlZDRFczd1l3aStnZ3pRRT1xCmVYAwAA
AFRXT3ELXXEMKENaMTpEaFVIQWtRblZGV2dvSjQ2SGhUeUxwVEt3RG9h
ZVd6SzNNcDRZZFZET1R2dDFyeGtVL1JnODR4U2l2TEN4Tm16U3h6Yy81
ZFEvMnJGVVYyMGMrNW85QUU9cQ1DWjI6bkJlazhxelUvQXZFc2FrNWE0
bEFHWTh5TWpXTmJLUWRobE5wNGhiRFZ3OGFsVUlaYkRmRE1nTFp2SWNq
QStXd0pBQWkvZFk0UDNLM3k5M01FaHJ
LUFFFPXEOZXUu
```

Decryption

```
1226.0,NaN,1835.968017578125,60161.0,1735.0,NaN,1885.0,NaN,
1216.0,NaN,1935.577392578125,63425.0,1759.0,NaN,1858.0,NaN,
1213.0,NaN,2035.186767578125,1153.0,1767.0,NaN,1885.0,NaN,
1222.0,NaN,2134.796142578125,4417.0,1742.0,NaN,1879.0,NaN,
1229.0,NaN,2234.405517578125,7681.0,1758.0,NaN,1890.0,NaN,
1231.0,NaN,2334.014892578125,10945.0,1752.0,NaN,1875.0,NaN,
1230.0,NaN,2433.624267578125,14209.0,1753.0,NaN,1891.0,NaN,
1217.0,NaN,2533.233642578125,17473.0,1736.0,NaN,1876.0,NaN,
1231.0,NaN,2632.843017578125,20737.0,1770.0,NaN,1888.0,NaN,
1207.0,NaN,2732.452392578125,24001.0,1745.0,NaN,1893.0,NaN,
1213.0,NaN,2832.061767578125,27265.0,1765.0,NaN,1889.0,NaN,
1235.0,NaN,2931.671142578125,30529.0,1757.0,NaN,1889.0,NaN,
1213.0,NaN,3031.280517578125,33793.0,1761.0,NaN,1881.0,NaN,
1224.0,NaN,3130.889892578125,37057.0,1768.0,NaN,1890.0,NaN,
1219.0,NaN,3230.499267578125,40321.0,1722.0,NaN,1903.0,NaN,
1216.0,NaN,3330.108642578125,43585.0,1734.0,NaN,1905.0,NaN,
1215.0,NaN,3429.718017578125,46849.0,1743.0,NaN,1898.0,NaN,
1212.0,NaN,3529.327392578125,50113.0,1759.0,NaN,1888.0,NaN,
1220.0,NaN,3628.936767578125,53377.0,1751.0,NaN,1896.0,NaN,
1222.0,NaN,3728.546142578125,56641.0,1759.0,NaN,1891.0,NaN,
1214.0,NaN,3828.155517578125,59905.0,1754.0,NaN,1890.0,NaN,
1221.0,NaN,3927.764892578125,63169.0,1771.0,NaN,1889.0,NaN,
1216.0,NaN,4027.374267578125,897.0,1765.0,NaN,1904.0,NaN,
1203.0,NaN,4126.983642578125,4161.0,1748.0,NaN,1899.0,NaN,
1214.0,NaN,4226.593017578125,7425.0,1744.0,NaN,1872.0,NaN,
1227.0,NaN,4326.202392578125,10689.0,1770.0,NaN,1878.0,NaN,
1221.0,NaN,4425.811767578125,13953.0,1761.0,NaN,1885.0,NaN,
1218.0,NaN,4525.421142578125,17217.0,1762.0,NaN,1899.0,NaN,
1218.0,NaN,4625.030517578125,20481.0,1750.0,NaN,1895.0,NaN,
1234.0,NaN,4724.639892578125,23745.0,1758.0,NaN,1886.0,NaN,
1201.0,NaN,4824.249267578125,27009.0,1756.0,NaN,1878.0,NaN,
1228.0,NaN,4923.858642578125,30273.0,1753.0,NaN,1878.0,NaN,
```

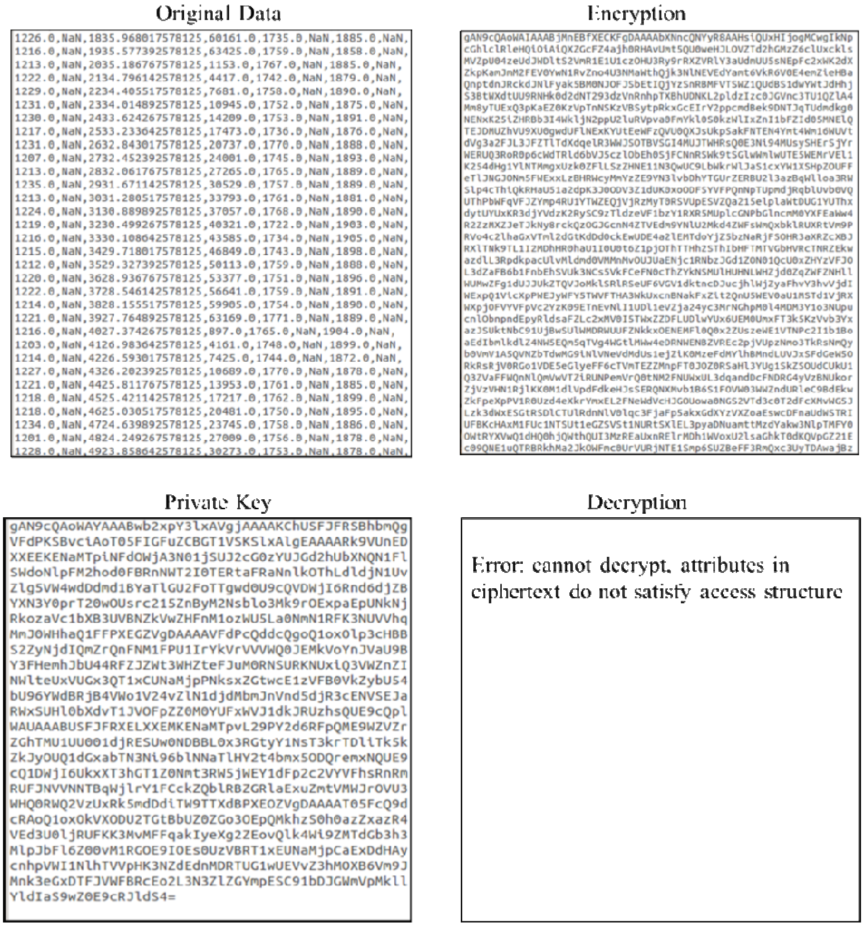
Figure 7: Screenshot of correct encryption and decryption

Figure 7 shows the screenshot of the work. The vital signs are being encrypted with a set of attributes at the patient's site and then sent to remote server site. In order to decrypt the encrypted vital signs, the access policy embedded in the private key must match the attributes encrypted inthe vital signs.

4.2 Incorrect Encryption and Decryption

In this section, we show 2 results of incorrect encryption and decryption; decryption using incorrect private key and decryption using incorrect wording.

4.2.1 Decryption using incorrect private key



Original Data

```
1226.0,NaN,1835.968017578125,60161.0,1735.0,NaN,1885.0,NaN,
1216.0,NaN,1935.577392578125,63425.0,1759.0,NaN,1858.0,NaN,
1213.0,NaN,2035.186767578125,1153.0,1767.0,NaN,1885.0,NaN,
1222.0,NaN,2134.796142578125,4417.0,1742.0,NaN,1879.0,NaN,
1229.0,NaN,2234.405517578125,7681.0,1758.0,NaN,1890.0,NaN,
1231.0,NaN,2334.014892578125,10945.0,1752.0,NaN,1875.0,NaN,
1230.0,NaN,2433.624267578125,14209.0,1753.0,NaN,1891.0,NaN,
1217.0,NaN,2533.233642578125,17473.0,1736.0,NaN,1876.0,NaN,
1231.0,NaN,2632.843017578125,20737.0,1770.0,NaN,1888.0,NaN,
1207.0,NaN,2732.452392578125,24001.0,1745.0,NaN,1893.0,NaN,
1213.0,NaN,2832.061767578125,27265.0,1765.0,NaN,1889.0,NaN,
1235.0,NaN,2931.671142578125,30529.0,1757.0,NaN,1889.0,NaN,
1213.0,NaN,3031.280517578125,33793.0,1761.0,NaN,1881.0,NaN,
1224.0,NaN,3130.889892578125,37057.0,1768.0,NaN,1890.0,NaN,
1219.0,NaN,3230.499267578125,40321.0,1722.0,NaN,1903.0,NaN,
1216.0,NaN,3330.108642578125,43585.0,1734.0,NaN,1905.0,NaN,
1215.0,NaN,3429.718017578125,46849.0,1743.0,NaN,1898.0,NaN,
1212.0,NaN,3529.327392578125,50113.0,1759.0,NaN,1888.0,NaN,
1220.0,NaN,3628.936767578125,53377.0,1751.0,NaN,1896.0,NaN,
1222.0,NaN,3728.546142578125,56641.0,1759.0,NaN,1891.0,NaN,
1214.0,NaN,3828.155517578125,59905.0,1754.0,NaN,1890.0,NaN,
1221.0,NaN,3927.764892578125,63169.0,1771.0,NaN,1889.0,NaN,
1216.0,NaN,4027.374267578125,897.0,1765.0,NaN,1904.0,NaN,
1203.0,NaN,4126.983642578125,4161.0,1748.0,NaN,1899.0,NaN,
1214.0,NaN,4226.593017578125,7425.0,1744.0,NaN,1872.0,NaN,
1227.0,NaN,4326.202392578125,10689.0,1770.0,NaN,1878.0,NaN,
1221.0,NaN,4425.811767578125,13953.0,1761.0,NaN,1885.0,NaN,
1218.0,NaN,4525.421142578125,17217.0,1762.0,NaN,1899.0,NaN,
1218.0,NaN,4625.030517578125,20481.0,1750.0,NaN,1895.0,NaN,
1234.0,NaN,4724.639892578125,23745.0,1758.0,NaN,1886.0,NaN,
1201.0,NaN,4824.249267578125,27009.0,1756.0,NaN,1878.0,NaN,
1228.0,NaN,4923.858642578125,30273.0,1753.0,NaN,1878.0,NaN,
```

Encryption

gAN9cQAoWAIAAABjMnEBfXECKFgDAAAAbXNncQNYyR8AAHsiQUxHIjogMCwgIkNp
cGhlclRleHQiOiAiQXZGcFZ4ajh0RHAvUmt5QU0weHJLOVZTd2hGMzZ6clUxckls
MVZpU04zeUdJWDltS2VmR1E1U1czOHU3Ry9rRXZVRlY3aUdmUU5sNEpFc2xWK2dX
ZkpKamJnM2FEV0YwN1RvZno4U3NMaWthQjk3NlNEVEdYamt6VkR6V0E4emZieHBa
QnptdnJRckdJNlFyak5BM0NJOFJSbEtIQjYzSnRBMFVTSWZ1QUdBS1dWYWtJdHhj
S3BtWXdtUU9RNHk0d2dNT293dzVnRnhpTXBhUDNKL2pldzIzc0JGVnc3TU1QZlA4
Mm8yTUExQ3pKaEZ0KzVpTnNSKzVBSytpRkxGcEIrY2ppcmd8ek9DNTJqTUdmdkg0
NENxK25iZHRBb3I4WkljN2ppU2luRVpva0FmYkl0S0kzWlIxZnI1bFZId05MNElQ
TEJDMUZhVU9XU0gwdUFlNExKYUtEeWFzQVU0QXJsUkpSakFNTEN4Ymt4Wm16WUVt
dVg3a2FJL3JFZTlTdKdqelR3WWJSOTBVSGI4MUJTWHRsQ0E3Ni94MUsySHErSjYr
WERUQ3RoR0p6cWdTRld6bVJ5czlObEh0SjFCNnRSWk9tSGlwWmlwUTE5WEMrVEl1
K254dHg1YlNTMmgxUzk0ZFlLSzZHNE11N3QwUC9LbWkrWlJaS1cxYW1XSHpZOUFF
eTlJNGJONm5FWExxLzBHRWcyMmYzZE9YN3lvbDhYTGUrZERBU2l3azBqWlloa3RW
Slp4cThiQkRMaU51a2dpK3J0ODV3Z1dUK0xoOOFSYVFPQnNpTUpmdjRqbluvb0VQ
UThPbWFqVFJZYmp4RU1YTWZEQjVjRzMyT0RSVUpESVZQa215elplaWtDUG1YUThx
dytUYUxKR3djYVdzK2RySC9zTldzeVF1bzY1RXR5MUplcGNPbGlncmM0YXFEaWw4
R2ZzMXZJeTJkNy8rckQzOGJGcnN4ZTVEdm9YNlU2Mkd4ZWFsWmQxbklRUXRtVm9P
RVo4c2lhaGxVTml2dGtKdDd0ckEwUDE4a2lEMTdoYjZ5bzNaRjFSOHR3aXRZcXBJ
RKlTNk9TL1IZMDhHR0haU1I0UDt6Z1pjOThTTHhZSTh1bHFTMTVGbHVRcTNRZEkw
azdlL3RpdkpacUlvMldmd0VMMnMvOUJUaENjc1RNbzJGd1Z0N01QcU0xZHYzVFJO
L3dZaFB6b1FnbEhSVUk3NCs5VkFCeFN0cThZYkNSMUlHUHNLWHZjd0ZqZWFZNHll
WUMwZFg1dUJJUkZTQVJoMklSRlRSeUF6VGV1dktncDJucjhlWjZyaFhvY3hvVjdI
WExpQ1VlcXpPHEJyWFY5TWVFTHA3WkUxcnBNakFxZlt2QnU5WEV0aU1MSTd1VjRX
WKpjOFVYVFpVc2YzK09ETnEvNlI1UDl1eVZja24yc3MrNGhpM0l4MDM3Y1o3NUpu
cnlObnpndEpyRldsaFZLc2xMV0I5TWxZZDFLUDlwYUx6UEM0UmxFT3k5KzVvb3Yx
azJSUktNbC91UjBwSUlWMDRWUUFZNkkxOENENEFl0Q0x2ZUszeWE1VTNPc2I1b1Bo
aEdIbmlkdlZ4NW5EQm5qTVg4WGtlMWw4eDRNWENBZVREc2pjVUpzNmo3TkRsNmQy
b0VmV1A5QVNZbTdwMG9iNlVNeVdMdUs1ejZiK0MzeFdMYlh8MndLUVJxSFdGeW5O
RkRsRjV0RGo1VDE5eGlyeFF6cTVmTEZZMnpFT0J0Z0RSaHl3YUg1SkZ5OUdCUkU1
Q3ZVaFFWQnNlQmVwVT2iRUNPemVrQ0tNM2FNUWxUL3dqandDcFNDRG4yVzBNUkor
ZjVzVHN1RjlKK0M1dlVpdFdkeHJsSERQNKMvb1B6S1FOVW03WW2ndURleC9BdEkw
ZkFpeXpPV1R0Uzd4eKkrYmxEL2FNeWdVcHJGOUowa0NGS2VTd2c0T2dGcXMvWG5J
Lzk3dWxESGtRSDlCTUlRdnNlV0lqc3FjaFp5akxGdXYzVXZoaEswcDFnaUdWSTRI
UFBKcHAxM1FUc1NTSUt1eGZSVSt1NURtSXlEL3pyaDNuamttMzdYakw3NlpTMFY0
OWtRYXVwQ1dHQ0hjQWthQUI3MzREaUxnREJrMDh1WVoxU2lsaGhkT0dKQVpGZ21E
c09QNE1uQTRBRkhhMa2JkOWFmc0UrVURjNTE1Smp6SUZBeFF3RmQxc3UyTDAwajBz

Private Key

gAN9cQAoWAYAAABwb2xpY3lxAVgjAAAAKChUSFJFRSBhbmQg
VFdPKSBvciAoT05FIGFuZCBGT1VSKSlxAlgEAAAARk9VUnED
XXEEKENaMTpiNFdOWjA3N01jSUJ2cG0zYUJGd2hUbXNQN1Fl
SWdoNlpFM2hod0FBRnNWT2I0TERtaFRaNnlkOThLdldjN1Uv
Zlg5VW4wdDdmd1BYaTlGU2FoTTgwd0U9cQVDWjI6Rnd6djZB
YXN3Y0prT20wOUsrc215ZnByM2Nsblo3Mk9rOExpaEpUNkNj
RkozaVc1bXB3UVBNZkVwZHFnM1ozWU5La0NmN1RFK3NUVVhq
MmJ0WHhaQ1FFPXEGZVgDAAAAVFdPcQddcQgoQ1ox0lp3cHBB
S2ZyNjdIQmZrQnFNM1FPU1IrYkVrVVVWQ0JEMkVoYnJVaU9B
Y3FHemhJbU44RFZJZWt3WHZteFJuM0RNSURKNUxiQ3VWZnZI
NWlteUxVUGx3QT1xCUNaMjpPNksxZGtwcE1zVFB0VkZybU54
bU96YWdBRjB4VWo1V24vZlN1djdMbmJnVnd5djR3cENNVSEJa
RWxSUHl0bXdvT1JVOFpZZ0M0YUFxWVJ1dkJRUzhsQUE9cQpl
WAUAAABUSFJFRXELXXEMKENaMTpvL29PY2d6RFpQME9WZVZr
ZGhTMU1UU001djRESUw0NDBBL0x3RGtyY1NsT3krTDliTk5k
ZkJyOUQ1dGxabTN3Ni96blNNaTlHY2t4bmx5ODQremxNQUE9
cQ1DWjI6UkxXT3hGT1Z0Nmt3RW5jWEY1dFp2c2VYVFhsRnRm
RUFJNVVNNTBqWjlrY1FCckZQblRBZGRlaExuZmtVMWJrOVU3
WHQ0RWQ2VzUxRk5mdDdiTW9TTXdBPXEOZVgDAAAAT05FcQ9d
cRAoQ1oxOkVXODU2TGtBbUZ0ZGo3OEpQMkhzS0h0azZxazR4
VEd3U0ljRUFKK3MvMFFqakIyeXg2ZEovQlk4Wi9ZMTdGb3h3
MlpJbFl6Z00vM1RGOE9IOEs0UzVBRT1xEUNaMjpCaExDdHAy
cnhpVWI1NlhTVVpHK3NZdEdnMDRTUG1wUEVvZ3hMOXB6Vm9J
Mnk3eGxDTFJVWFBRcEo2L3N3ZlZGYmpESC91bDJGWmVpMkll
YldIaS9wZ0E9cRJldS4=

Decryption

Error: cannot decrypt, attributes in ciphertext do not satisfy access structure

Figure 8: Screenshot of encryption and decryption using incorrect private key

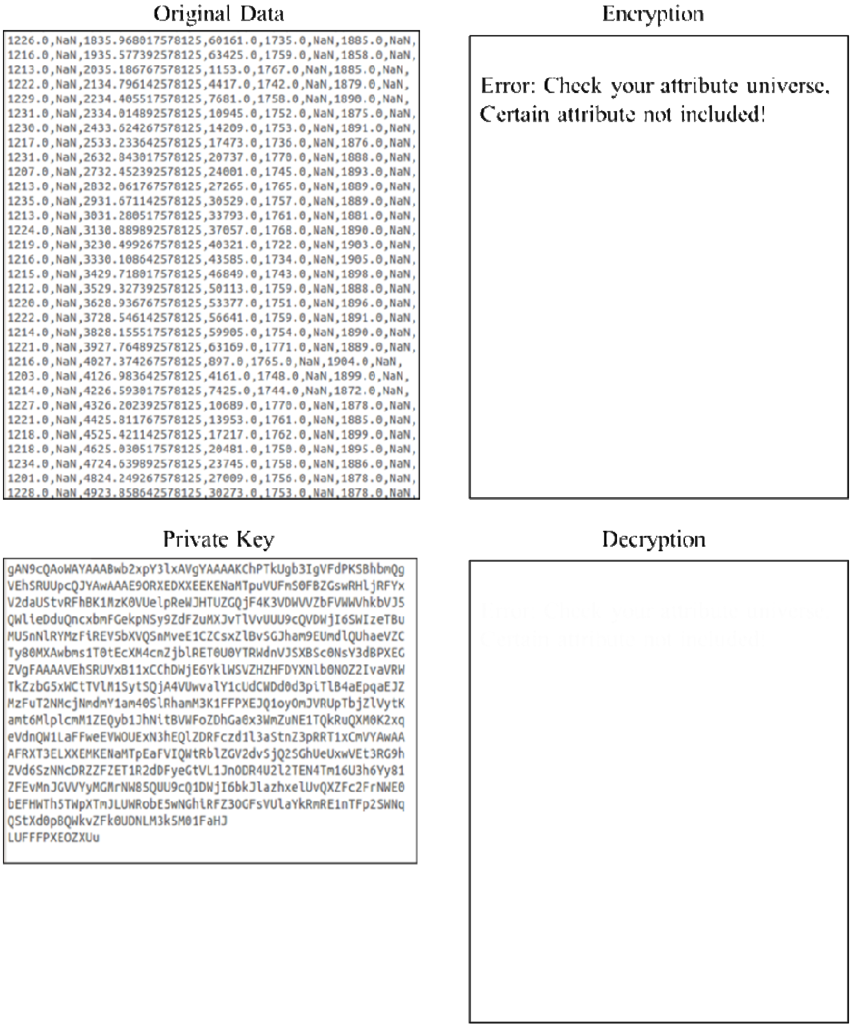
From the screenshot shown in Figure 8, the encrypted vital signs are being decrypted with an incorrect private key. The encrypted vital signs cannot be decrypted and the original vital signs cannot be reconstructed as the embedded access policy in the private key does not satisfy the attributes encrypted in the vital signs.

4.2.2 Decryption using incorrect wording

TABLE 2: KP-ABE Performance test results with incorrect wording

Correct attributes		Wrong attributes	Test results
Name of Doctor	Simon Peter	Sim**e**on Peter	X
Expertise	Cardiology	Cardilo**j**y	X
Department of medical service	Department of heart disease	Department of hear**d** Disease	X
Name of hospital	Columbia	Colum**p**ia	X

X: original text was not reconstructed



Original Data

```
1226.0,NaN,1835.968017578125,60161.0,1735.0,NaN,1885.0,NaN,
1216.0,NaN,1935.577392578125,63425.0,1759.0,NaN,1858.0,NaN,
1213.0,NaN,2035.186767578125,1153.0,1767.0,NaN,1885.0,NaN,
1222.0,NaN,2134.796142578125,4417.0,1742.0,NaN,1879.0,NaN,
1229.0,NaN,2234.405517578125,7681.0,1758.0,NaN,1890.0,NaN,
1231.0,NaN,2334.014892578125,10945.0,1752.0,NaN,1875.0,NaN,
1230.0,NaN,2433.624267578125,14209.0,1753.0,NaN,1891.0,NaN,
1217.0,NaN,2533.233642578125,17473.0,1736.0,NaN,1876.0,NaN,
1231.0,NaN,2632.843017578125,20737.0,1770.0,NaN,1888.0,NaN,
1207.0,NaN,2732.452392578125,24001.0,1745.0,NaN,1893.0,NaN,
1213.0,NaN,2832.061767578125,27265.0,1765.0,NaN,1889.0,NaN,
1235.0,NaN,2931.671142578125,30529.0,1757.0,NaN,1889.0,NaN,
1213.0,NaN,3031.280517578125,33793.0,1761.0,NaN,1881.0,NaN,
1224.0,NaN,3130.889892578125,37057.0,1768.0,NaN,1890.0,NaN,
1219.0,NaN,3230.499267578125,40321.0,1722.0,NaN,1903.0,NaN,
1216.0,NaN,3330.108642578125,43585.0,1734.0,NaN,1905.0,NaN,
1215.0,NaN,3429.718017578125,46849.0,1743.0,NaN,1898.0,NaN,
1212.0,NaN,3529.327392578125,50113.0,1759.0,NaN,1888.0,NaN,
1220.0,NaN,3628.936767578125,53377.0,1751.0,NaN,1896.0,NaN,
1222.0,NaN,3728.546142578125,56641.0,1759.0,NaN,1891.0,NaN,
1214.0,NaN,3828.155517578125,59905.0,1754.0,NaN,1890.0,NaN,
1221.0,NaN,3927.764892578125,63169.0,1771.0,NaN,1889.0,NaN,
1216.0,NaN,4027.374267578125,897.0,1765.0,NaN,1904.0,NaN,
1203.0,NaN,4126.983642578125,4161.0,1748.0,NaN,1899.0,NaN,
1214.0,NaN,4226.593017578125,7425.0,1744.0,NaN,1872.0,NaN,
1227.0,NaN,4326.202392578125,10689.0,1770.0,NaN,1878.0,NaN,
1221.0,NaN,4425.811767578125,13953.0,1761.0,NaN,1885.0,NaN,
1218.0,NaN,4525.421142578125,17217.0,1762.0,NaN,1899.0,NaN,
1218.0,NaN,4625.030517578125,20481.0,1750.0,NaN,1895.0,NaN,
1234.0,NaN,4724.639892578125,23745.0,1758.0,NaN,1886.0,NaN,
1201.0,NaN,4824.249267578125,27009.0,1756.0,NaN,1878.0,NaN,
1228.0,NaN,4923.858642578125,30273.0,1753.0,NaN,1878.0,NaN,
```

Encryption

Error: Check your attribute universe.
Certain attribute not included!

Private Key

```
gAN9cQAoWAYAAABwb2xpY3lxAVgYAAAAKChPTkUgb3IgVFdPKSBhbmQg
VEhSRUUpcQJYAwAAAE9ORXEDXXEEKENaMTpuVUFmS0FBZGswRHljRFYx
V2daUStvRFhBK1MzK0VUelpReWJHTUZGQjF4K3VDWVVZbFVWWVhkbVJ5
QWlieDduQncxbmFGekpNSy9ZdFZuMXJvTlVvUUU9cQVDWjI6SWIzeTBu
MU5nNlRYMzFiREV5bXVQSnMveE1CZCsxZlBvSGJham9EUmdlQUhaeVZC
Ty80MXAwbms1T0tEcXM4cmZjblRET0U0YTRWdnVJSXBSc0NsY3dBPXEG
ZVgFAAAAVEhSRUVxB11xCChDWjE6YklWSVZHZHFDYXNlb0NOZ2IvaVRW
TkZzbG5xWCtTVlM1SytSQjA4VUwvalY1cUdCWDd0d3piTlB4aEpqaEJZ
MzFuT2NMcjNmdmY1am40SlRhamM3K1FFPXEJQ1oyOmJVRUpTbjZlVytK
amt6MlplcmM1ZEQyb1JhNitBVWFoZDhGa0x3WmZuNE1TQkRuQXM0K2xq
eVdnQW1LaFFweEVWOUExN3hEQlZDRFczd1l3aStnZ3pRRT1xCmVYAwAA
AFRXT3ELXXEMKENaMTpEaFVIQWtRblZGV2dvSjQ2SGhUeUxwVEt3RG9h
ZVd6SzNNcDRZZFZET1R2dDFyeGtVL1JnODR4U2l2TEN4Tm16U3h6Vy81
ZFEvMnJGVVYyMGMrNW85QUU9cQ1DWjI6bkJlazhxelUvQXZFc2FrNWE0
bEFHWTh5TWpXTmJLUWRobE5wNGhiRFZ3OGFsVUlaYkRmRE1nTFp2SWNq
QStXd0pBQWkvZFk0UDNLM3k5M01FaHJ
LUFFFPXEOZXUu
```

Decryption

Error: Check your attribute universe.
Certain attribute not included!

Figure 9: Screenshot of private key generation failure due to incorrect wording

From the results shown in Table 2, the encryption will not be granted because of incorrect wording. Figure 9 shows the screenshot of encryption failure due to the incorrect wording usage. This is to ensure the correct descriptive attributes are used to perform the encryption.

5. CONCLUSION

We present the encryption/decryption prototype system to protect the captured vital signs and personal information of patients. This enables patients' medical data to be remotely monitored from the hospital insecured manner. Body sensor nodes are used in the system to capture vital signs from the human body. We demonstrate that, by using key-policy attribute-based encryption (KP-ABE), patients' medical information can be protected and be shared among different medical operators. Our work is a non-real time application. However, we are going to extend our system to real-time application for ubiquitous healthcare purposes. It provides flexibility for patients to collect their vital signs and perform encrypt at any time of the day and at any places according to their preferences.

Future work of this project is to connect the current system to a personal health record service provider (PHR). PHR will enable patients to store their encrypted vital signs from home and allow the medical information retrieval of healthcare providers in hospitals.

REFERENCES

[1] B. Lo, S. Thiemjarus, R. King and G.Z. Yang (2005). Body Sensor Network - A Wireless Sensor Platform for Pervasive Healthcare Monitoring. *Adjunct Proceedings of the 3rd InternationalConference on Pervasive Computing, pp.77-80.*

[2] B. Lo and G.Z. Yang (2005). Architecture for Body Sensor Networks. *IEEE Proceedings of thePerspective in Pervasive Computing, pp.23-28.*

[3] B. Lo and G.Z. Yang (2005). Key Technical Challenges and Current Implementations of Body Sensor Networks. *IEEE Proceedings of the 2nd International Workshop on Body Sensor Networks, pp. 1-5.*

[4] Otto, C., Milenkovic, A., Sanders, C., &Jovanov, E. (2006). System architecture of a wireless body area sensor network for ubiquitous health monitoring. *Journal of Mobile Multimedia, 1*(4): 307-326.

[5] R. S. H. Istepanian, E. Jovanov, and Y.T. Zhang (2004). Introduction to the Special Section on M-Health: Beyond Seamless Mobility

and Global Wireless Health-Care Connectivity. *IEEE Transactions on Information Technology in Biomedicine,8*(2).

[6] Cherukuri, S., Venkatasubramanian, K. K., & Gupta, S. K. (2003). BioSec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body. In *Parallel Processing Workshops, 2003. Proceedings. 2003 International Conference on* (pp. 432-439). IEEE.

[7] Bao, S. D., & Zhang, Y. T. (2006). A design proposal of security architecture for medical body sensor networks. In *Wearable and Implantable Body Sensor Networks, 2006. BSN 2006. International Workshop on* (pp. 4-pp). IEEE.

[8] Poon, C. C., Zhang, Y. T., &Bao, S. D. (2006). A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health.*Communications Magazine, IEEE*, *44*(4), 73-81.

[9] Singh, K., &Muthukkumarasamy, V. (2007). Authenticated key establishment protocols for a home health care system. In *Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference on* (pp. 353-358). IEEE.

[10] Tan, C. C., Wang, H., Zhong, S., & Li, Q. (2008). Body sensor network security: an identity-based cryptography approach. In *Proceedings of the first ACM conference on Wireless network security* (pp. 148-153). ACM.

[11] Sahai and B. Waters (2005). Fuzzy Identity Based Encryption. In *Advances of cryptology – Eurocrypt 2005, LNCS 3494, pp. 457-473.*

[12] Ostrovsky, R., Sahai, A., & Waters, B. (2007). Attribute-based encryption with non-monotonic access structures. In *Proceedings of the 14th ACM conference on Computer and communications security* (pp. 195-203). ACM.

[13] Chase, M. (2007). Multi-authority attribute based encryption. *Theory of Cryptography*, 515-534.

[14] Lewko, A., Okamoto, T., Sahai, A., Takashima, K., & Waters, B. (2010). Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. *Advances in Cryptology–EUROCRYPT 2010*, 62-91.

[15] V. Goyal, O. Pandey, A. Sahai and B. Waters (2006). Attribute Based Encryption for Fine-Grained Access Control of Encrypted Data. *ACM conference on Computer and Communications Security, pp. 89–98.*

[16] Attrapadung, N., Libert, B., & De Panafieu, E. (2011). Expressive key-policy attribute-based encryption with constant-size ciphertexts. *Public Key Cryptography–PKC 2011*, 90-108.

[17] J. Bethencourt, A. Sahai and B. Waters (2007). Ciphertext-policy attribute-based encryption. *IEEE Symposium on Security & Privacy, pp.321-334.*

[18] Goyal, V., Jain, A., Pandey, O., &Sahai, A. (2008). Bounded ciphertext policy attribute based encryption. *Automata, Languages and Programming*, 579-591.

[19] Waters, B. (2011). Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. *Public Key Cryptography–PKC 2011*, 53-70.

[20] Y.L. Tan, B.M. Goi, R. Komiya, S.Y. Tan (2011). A Study of Attribute-Based Encryption for Body Sensor Networks. *Communications in Computer and Information Science, 251(2), pp.238-247.*

[21] Shamir (1984). Identity-based cryptosystems and signature schemes. *Advances in Cryptology - Crypto '84, LNCS 0196, pp. 47-53.*

[22] D. Boneh and M. Franklin (2001). Identity-based Encryption from the Weil pairing.*Advances in Cryptology- CRYPTO'01, LNCS 2139, pp. 213–229.*

[23] Sahai and B. Waters (2005). Fuzzy Identity Based Encryption. *EUROCRYPT 2005, LNCS 3494, pp. 457–473.*

[24] Hao, Y., & Foster, R. (2008). Wireless body sensor networks for health-monitoring applications. *Physiological measurement*, *29* (11), R27.

[25] Ghasemzadeh, H., Loseu, V., Guenterberg, E., &Jafari, R. (2009). Sport training using body sensor networks: a statistical approach to measure wrist rotation for golf swing. In *Proceedings of the Fourth International Conference on Body Area Networks* (p. 2). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[26] Kim, S., Beckmann, L., Pistor, M., Cousin, L., Walter, M., &Leonhardt, S. (2009). A versatile body sensor network for health care applications. In *Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2009 5th International Conference on* (pp. 175-180). IEEE.

[27] Sensixa Ltd. http://www.sensixa.com.

[28] Yao Zheng (2011). Privacy-preserving personal health record system using attribute-based encryption. *Master's thesis*. *Worcester Polytechnic Institute*.

]