International Journal of Smart Home
Vol.7, No.5 (2013), pp.225-238
http://dx.doi.org/10.14257/ijsh.2013.7.5.23

A Study on the Realization of Mobile Homecare Nursing Service Based on Effective Security

Eun-Young Jung[1], Sung-Jong Eun[2], Byoung-Hui Jeong[3] and Dong Kyun Park[*]

[1,*] *u-Healthcare Center Gachon University, Gil Medical center, Incheon, Korea,*
[2]*Department of Computer Science Gachon University, Seongnam, Gyunggi-Do, Korea*
[3]*Bio Research Complex, BRC Co.,Ltd. Incheon, Korea*
[1]*eyjung@gilhospital.com,* [2]*asclephios@hotmail.com,* [3]*buxbany@gmail.com,*
[*]*pdk66@gilhospital.com*

Abstract

Demands on homecare nursing are on the rise due to increase of medical demand for the aged; however, as the homecare nursing should provide service by visiting home, there are limits in the IT infra that manages and inquires the medical information of patients in current situations. This paper developed an application for inquiring about the information of patients and homecare nursing patient clients in the middle of medical services thanks to the recent development of mobile service, and improved the safety of service by applying an effective security method suitable for mobile platform. As homecare nurses can confirm the details of homecare nursing requests, inquiries by reserved patients, progress records, etc. at home in real time, it is likely possible that a good quality of homecare nursing service that provides tailored information according to the patients' status is realized.

Keywords: *component; homecare nursing service, mobile-healthcare, mobile-device, smart phone, healthcare data security*

1. Introduction

The nation's health promotion project in South Korea is directly influenced by information for ageing, gentrification in medical demands, increases of medical costs due to the developments of medical and treatment technologies, medical cost restrictions due to resource limits, and also prompted by the citizen's efforts; thus, the demand on homecare nursing becomes an issue. Accordingly, many studies have been made on the computerization on such an issue as concerns on homecare nursing rose, rather the service that uses a mobile device in managing patients [1]. The homecare nursing service is a hospital substitution service scheme that a special homecare nurse visits patients' home to provide necessary treatments and cares according to doctor's prescription for patients who require continuous treatments and nursing after retiring from a hospital [2]. Therefore, as the demands for homecare nursing service increase, the homecare nursing service providers intend to provide the service in more convenient environments; however, due to the current shortage of service using mobile devices, the homecare nurse depends the patient treatment and prescription information on the telephone [3]. This study compensated such problems by using a mobile device, made it possible to manage the patients by saving the information and progresses about homecare nursing at the application and to provide the tailored homecare nursing service to the patients through the real time inquiries on the treatments and prescription information for the patients. To differentiate from the conventional medical information-linked application, this study

ISSN: 1975-4094 IJSH

realized an effective mobile homecare nursing service suitable for the mobile platforms considering the medical information securities.

2. Related Works

The homecare nursing service is the service that a homecare nurse visits home of the care subject, and helps the patient to recover faster and to retire from a hospital earlier by providing a psychological stability [4]. The typical examples are the hospital's homecare nursing, health center's homecare nursing, long-term care for the elderly, visiting care, *etc*.

The homecare nursing has extended nationwide since February 2001 after being operated as a demonstration project from Sep. 1994, and is currently being implemented over 150 places in South Korea. Thus, whilst the homecare nursing conducted by the hospital and health center has increased every year, researches and developments on the diversification of IT infra and services necessary for the homecare nursing remain minor [5].

The recent developments of mobile communication technologies and mobile devices have triggered the developments of the services that use mobile devices for the efficient medical services through many companies and medical institutions.

The mobile device, Smartphone is on the rise on its market share in the entire mobile phone markets, and becomes popular thanks to its various functions [6]. On the other hand, in the treatment programs, many patient management applications including the verification of treatment details, patient status, etc. are also being developed. The Seoul National University Bundang Hospital operates a representative cloud-based treatment information system, the Ministry of Food and Drug Safety services a Mobile Picture Archiving Communication System (PACS), and such systems provide the medical data like X-ray, Computer Tomography (CT), *etc.*, at the treatment sites using medical equipment in real time [7]

The 'Smart Doctor' developed by Chunneung IT is a smart chart that interworks with the Electronic Medical Record System (EMR) and enhances the efficiency of treatment through readings and corrections. In addition, that includes the hospital search function that shows the nearest hospitals.

SK Telecom built an information communication-based medical service environment, the 'Smart-Hospital' application to provide the best medical services to patients. If a hospital agreed to use the 'Smart-Hospital' application, the hospital can process the existing information including EMR, Order Communication System (OCS), PCS, *etc.*, through a mobile phone, and increase the operation efficiencies [8].

The mobile device can be used at any time anywhere regardless the locations, uses the built-in wireless internet; therefore, the device is widely utilized in the medical services and treatments in many places thanks to its efficiency in treatment and management services. However, the device carries problems in its aggressive utilization in homecare nursing due to the lower efficiencies in communication costs, security issues, interworking with the existing systems, *etc.*, as such device should be used by a homecare nurse.

Currently the homecare nurse prints out or works manually the related information of patients, and brings to patients' home to carry out home care [9]. Therefore, there are problems that the nurse is unable to inquire the patient information and process records in real time, and is difficult to check the information of homecare nursing patients in the hospital in real time. In terms of the security of medical information, some studies have been made on the security technologies suitable for the mobile platforms; however, the services that are improved in its safety by applying such studies to the health care applications are minor.

Therefore, in this paper, such a mobile high security in the field of health care for the ECC (Elliptic Curve Cryptosystem) encryption algorithm using the mobile home care services is designed and implemented.

1985 N. ECC algorithms Koblitz and V. Algorithm proposed by Miller elliptic curve algorithm, also called elliptic curves defined over finite groups (Group) from the difficulty of the discrete logarithm problem is based on the encryption algorithm.

Elliptic Curve about 150 years ago, a wide range of mathematical research have been or Andrew Wiles recent proof of Fermat's Last Theorem has been used in the important. ECC algorithms safety 10 years ago, the other per-bit public key encryption algorithm that is more efficient alryeojyeotgo The ECM (Elliptic Curve Method) is the foundation of the RSA encryption algorithm factoring problem and hydrophobic test may provide an efficient algorithm was.

In general, a 160-bit key size of ECC algorithm with 1024-bit key size RSA algorithm has been said to have a comparable safety, especially 160-bit key size and 193-bit ECC algorithm with a key size from 10 to 20, respectively, above the safety is estimated with the efficiency compared to other cryptographic algorithms have been recognized

This method combined with randomness ECC algorithms (*e g.*, P + P + P. .. = kP) public key shared by the sending and receiving devices, the attacker cannot infer motives secure secret key and a secret key motivation used in conjunction with message encryption and authentication data are conducted in order to. In order to implement such a system password and message encryption algorithm key distribution algorithm must consist of two ECC-based key distribution algorithm ECDH (Elliptic Curve Diffie-Hellman) is representative. ECDH algorithm in finite positions as the elliptic curve Diffie-Hellman algorithm to convert on the Diffie-Hellman algorithm is essentially the same, and operation method. Figure 1 is an operation of the ECDH algorithm.

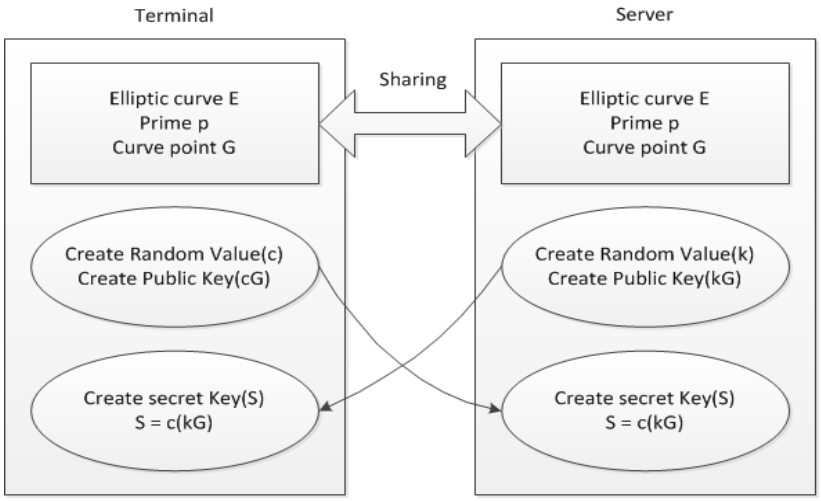

Figure 1. ECDH Operation Process

3. Design of the System

The block diagram of the system, as shown in Figure 2, displays the functions that the home-care nurse can inquire and manage the details including the reservation information, home care request, homecare nursing process, etc. that are necessary for the homecare nursing after the nurse logged in the application. The easier accessibility thanks to the interoperability of the web service makes the importance of the web service security to be more significant.

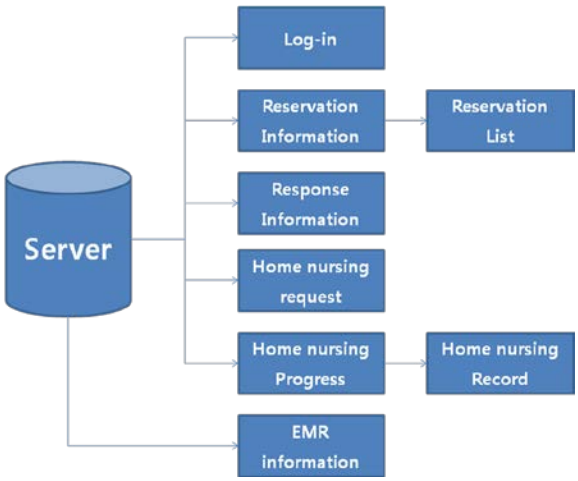

Figure 2. System Schema

The security of the web service is divided into the transmission hierarchy of communication protocol, message (SOAP or XML), and service security level. The communication protocols for the web service are used with the internet protocols such as HTTP, HTTPS, SMTP (Simple Mail Transfer Protocol) and FTP. The XML encryption provides the confidentialness of documents, and applicable to the encryption in a part or the whole of the documents according to the conventional encryption standard [10]. The encryption expresses the encoded result by using the XML. That is, the encoded results stand for the data encrypted in the XML type. Therefore, it uses the encryption function while maintaining the merits of the XML. Moreover, it has an advantage that can be encoded based on the XML without changing the application due to various encryption algorithms. The medical information security system proposed in this paper receives through an EMR Integrated Gateway the transmitted data related to diseases, diets, exercises, *etc.*, that are basically linked with the hospital. Then, the system defines the basic information to extract the contents at the personal health information management module and daily life information management module. Then, the system transmits to the outside such data through the personal health information management module or clinical information management module in connection with the ECC encryption algorithm module that can be used with HL7/CCD or HL7/CCR, and these data are processed in the standardized XML documents.

CCR and certain personal information associated with the patient's medical information at the point represents. ASTM and other standards development organizations established in cooperation with the XML schema to use, if properly designed electronic medical records system for all CCR data to be able to import, export business of health care workers in the delivery of medical information while minimizing confusion is possible. CCR standard for health information exchange using the same procedure as in Figure 3 was designed.

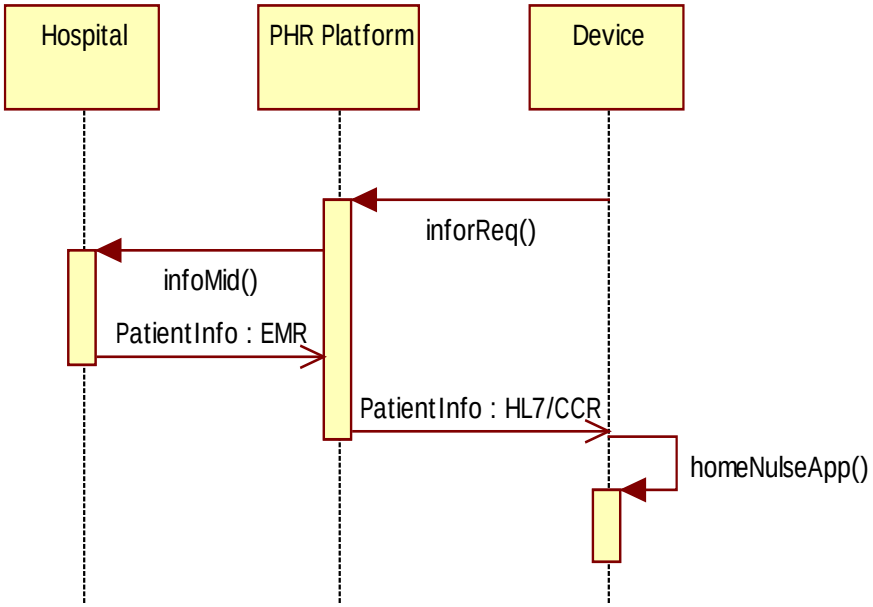

Figure 3. Health Information Exchange Procedures

The proposed patient data in XML format contains a wealth of information of the patient. It also has a standardized structure, so the standard is suitable for a variety of external services, the same services can be provided. Mainly used in home care services to the patient's personal data basic/Function to search medical information, medical information measure query/input functions, information functions Nursing, Nursing progress functions can be called the essential functions. The following table lists these patient data in XML format is the structure of the request and response messages.

Table 1. Patient Query Schema Structure

I/O	Depth	Name	Value
Request	1	Type	Patient-Search
	1	ResidentID	
Response	1	PersonalInformation	
	2	PatientName	
	2	Gender	
	2	Age	
	2	ResidentID	
	2	Address	
	2	HomePhoneNumber	
	3	OfficePhoneNumber	
	2	CellPhoneNumber	
	2	Email	
	1	Allergy	

Table 2. Vital Signs Schema Structure

I/O	Depth	Name	Value
Request	1	Type	VitalSign
	1	LoginID	
	1	PatientID	
	1	StartDate	
	1	EndDate	
Response	1	Vitalsigns	
	2	Vitalsign	
	3	Date	
	3	Time	
	3	BPDiastolic	
	3	BPSystolic	
	3	Pulse	
	3	BodyTemperature	
	3	Height	
	3	Weight	
	3	BloodSugar	

If the message is an XML request from the device to the hospital, or in the hospital for a particular task to a device that includes the ability to request services. Therefore, the request shall be separated by parsing the type, the request type, two minutes if the response message is transmitted.

However, this type of CCR medical information only used to send data because the encryption and decryption process because it operates independent of the medical and security services should be designed and implemented in a different perspective. To solve this problem, in this paper, as shown in Table 1 and Table 2 of the CCR XML format using the same type of structure-related messages were designed encryption and decryption.

Table 3. Send Public Key Message Structure

I/O	Depth	Name	Value
Request	1	Type	SendPublicKey
	1	DeviceID	
	1	Key	
	1	Parameter	
Response	1	Server Info	
	2	Key	

Table 3, the Public key as a way to transfer the request type "Public Key Transfer" includes the value. The server decrypts it is appropriate for the encryption and decryption operations are running, the response by generating a response message is transmitted.The XML message encoding ciphering in this paper is applied with an encryption method using the ECC encryption algorithm in the fields of the XML documents where require the security in a part. The XML message applied with ECC extracts the service data from the Uniform Resource Identifier (URI) of the web service and generates the SOAP messages. The XML message uses the signature of the SOAP message and ECC algorithm, encrypts the message, and protects the web service. The service data of the original URI copy is used as a file for the web service accessible at remote through the HTTP protocol. The XML encryption using the

ECC encryption algorithm is differentiated from the existing encryption processes on its structural characteristics of the XML document that encodes only the parts necessary for the security and that the final encryption process result shows the XML message form other than the binary code. Figure 4 shows the algorithm of the ECC encryption process of the XML message.

```
Procedure Encrytion()
{    Accept XML message;
 Parsing well-formed XML message;
 Whlie(parsing result valid) then
    {   Extract the element to be encryted
        If (extract result = exit) then
        {
        Encrypt using private key;
        Encode;
        Create Encryptiom Information element;
        Replace the element;
      }
     else {
            encrypted XML message;
            end;
          }
  }
  Exception error;
}
```

Figure 4. Encription Procedure

It is applied with an encryption algorithm that the web service data is extracted according to the client's request, the SOAP message is generated by the SOAP message processor, and an encoded XML type message is generated. The message encryption module compares a message with the document structure of the XML type message; if it is found as an effective (well-formed) XML document, the module extracts the partial elements with which the module conducts the encoding operation, and encrypts using the secret key encryption algorithm. The secret key in the encryption represents the session key for the relevant group. When the encryptions of the elements are completed, it encodes such encrypted elements to exchange with the elements in the XML message. Lastly, it attaches the necessary information required for deciphering the encrypted contents on the encrypted contents. Through the aforementioned process, the parts only require the security are composed to the encrypted XML message.

The decryption process of the XML message is similar to the encryption process. Figure 5 shows the process order at the XML message decryption module. The message decryption module examines the XML message whether it has effective (well-formed) XML document structure; if it is found effective, it extracts the elements to be deciphered, and decodes the extracted elements. The module uses the session key to decipher the elements in the encoded XML message. After the decryption is completed, the module replaces the encrypted information and its related information with the deciphered elements.

```
Procedure Decrytion()
{  Accept encryted XML message;
Parsing well-formed XML message;
Whlie(parsing result valid) then
   {  Extract the element to be decryted
      If (extract result = exit) then
      {
      Decode;
      Decrypt
      Delete Encryptiom Information element;
      Replace the element;
    }
    else
    {
       Decrypted XML message;
       end;
     }
}
Exception error;
}
```

Figure 5. Decription Procedure

In this paper, an ECC algorithm is proposed by applying the protocol ECDH key management includes a module. ECDH algorithm in the case of default, the hospital and the external services to use when connecting to the authentication server is normal. ECDH key management procedures of the algorithm was designed, as shown in Figure 6.

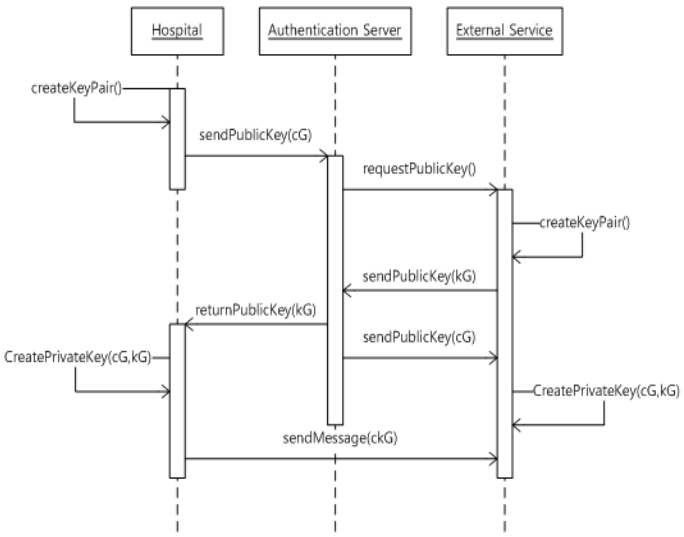

Figure 6. The Proposed ECDH Key Management Procedures

According to Figure 6, in the middle of the hospital and outside services to each other by the authentication server share a secret key that goes through the procedure. At this time, the procedure is as follows:

① hospital (or services) using his private key c to generate Public key pair.

② generated Public key is sent to the authentication server, cG is as a form of release.

③ received public key authentication server opponents Service (or hospital) to request the public key (Request) is.

④ requested service (or hospital) immediately using the secret key k to generate Public key pair.

⑤ generated Public key is sent to the authentication server, kG is as a form of release.

⑥ Now, the authentication server and the service received from both the hospital and kG respectively cG is transmitted.

⑦ opponent's public key received two hospitals and each have their own private key and public key combination to generate ckG.

⑧ When sending a message to encrypt and transmit ckG.

According to the above procedure to initiate communication between agencies and services in order to be each other's public key, and then using the public key of their own to share a secret key can be seen.

4. Implementation of Mobile Platform UI

After the development of the operation program based on HTML5, CSS and JavaScript is completed, the UI packaging operation is conducted on the relevant script-based contents through the native mobile platform. The relevant contents are processed as shown in Figure 7, and developed to support various users with the service regardless the platforms.

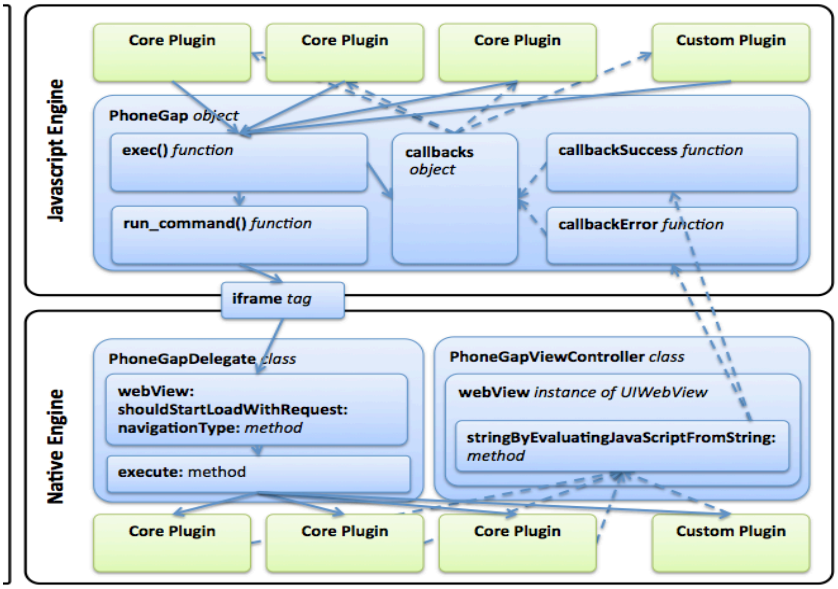

Figure 7. Mobile App Architecture

This service is developed for a Smartphone application based on the Android operation system. The homecare nurse can use the clinical information of patients at the system that receives the EMR-based patient information.

If the homecare nurse logs in using the Smartphone application, the main screen shows the schedules. The schedule function identifies the numbers of patients to visit, and can connect the nurse to the home care request and homecare nursing reservation. The home care request functions the detail inquiry according to the response by the nurse. The detail inquiry can be searched by the starting date, completion date, patient number or patient name. The searched patients are inquired about homecare nursing reservation time, patient number, patient name, gender and age. To receive the information of patients from the homecare nurse, it is necessary to collect the personal information of the patient; therefore, the hospital's EMR information is linked with the system. Such information is consisted of the patient inquiry and request details. In addition, the patient names, treatment department, gender and age appear on the nurse's Smartphone in the order of the reservation for the home care, so the nurse can find the information about the home care reservation in a single page. By selecting patients presented in order, the nurse can extract the detailed patient information. The nurse can update the hospital information in real time by loading the homecare nursing process record and information search record through the Smartphone application, observe the progress of the patient, and investigate quickly the information and status of the patient. Figure 8 verifies the results of each realization respectively.

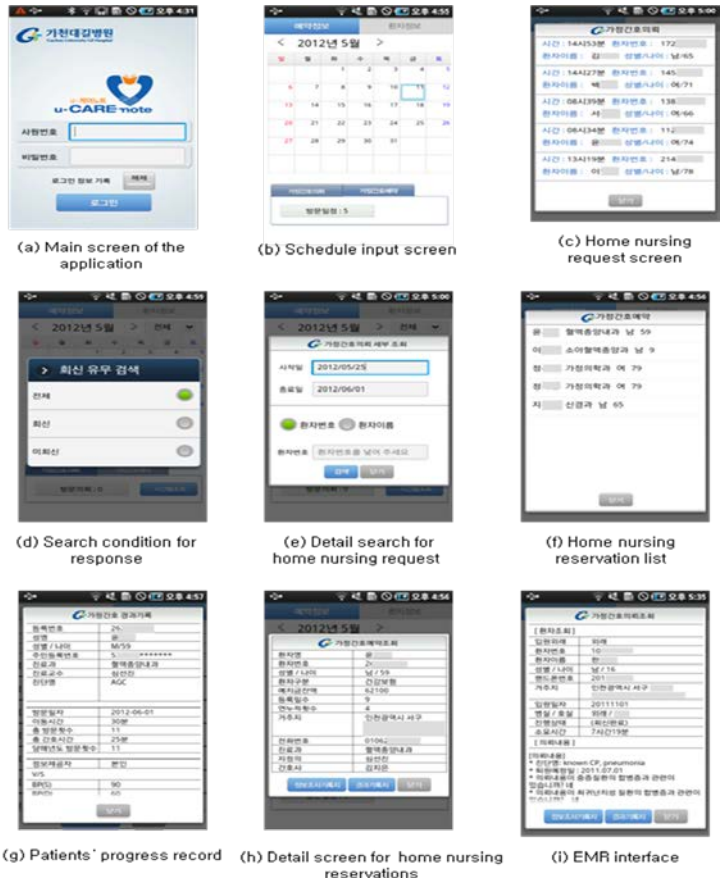

Figure 8. System Implementation

5. Evaluation of Mobile Platform UI

In this paper, we design and implement a mobile home care services did not apply the security system, the load on the system is greater than. It also requires the use of real-time services in an environment where time delays of data transfer can occur. Therefore, the proposed system is to determine whether the services of the following scenarios are being tested.

① to encrypt the data Send from the hospital to increase the size of the patient's data should be encrypted. The time is measured and compared.

② 1 scenario in the same environment as the load on the server is measured. For this purpose, the amount of memory used by the server is measured and compared.

Figure 9 is a graph of the ECC algorithm, the speed measurement data. ECC encryption algorithm in the case of very ginde the time it takes to initialize, the initialization process, the county created the curve, and the encryption and decryption procedures for computing the minimum means. In other words, the size of the data to be encrypted, regardless of the number of hours it takes similar. However, relative to the initialization than the data encryption and decryption time is very short.

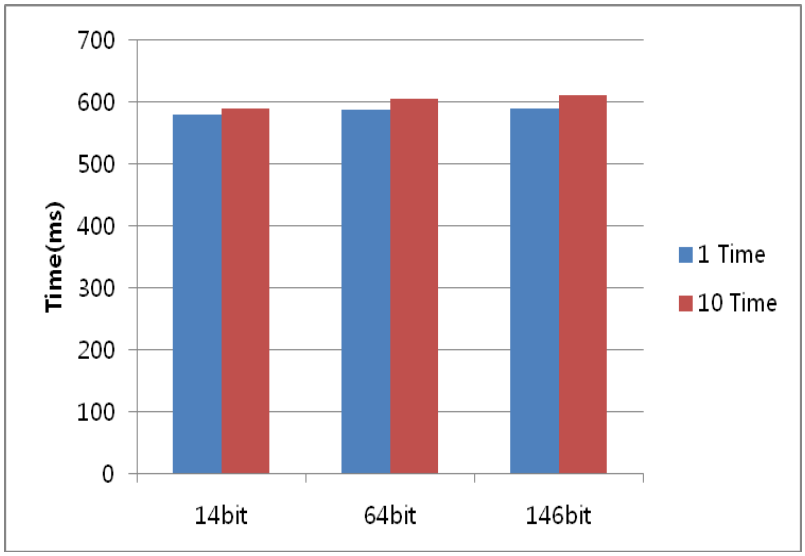

Figure 9. ECC Algorithm Speed Measurement Data Graphs

Figure 10 is a graph of the data to measure ECC Memory. Test scenarios, a variety of input data to be encrypted by the server takes the actual amount of memory that is measured. The larger the size of the data you enter, the more the number of iterations increases the amount of memory occupied. However, the difference is relatively mild, and not to determine the actual load operation the [147bit / 1 times] because it consumes only about 1680kb based encryption and decryption require large amounts of server enough to accommodate even confirmed.

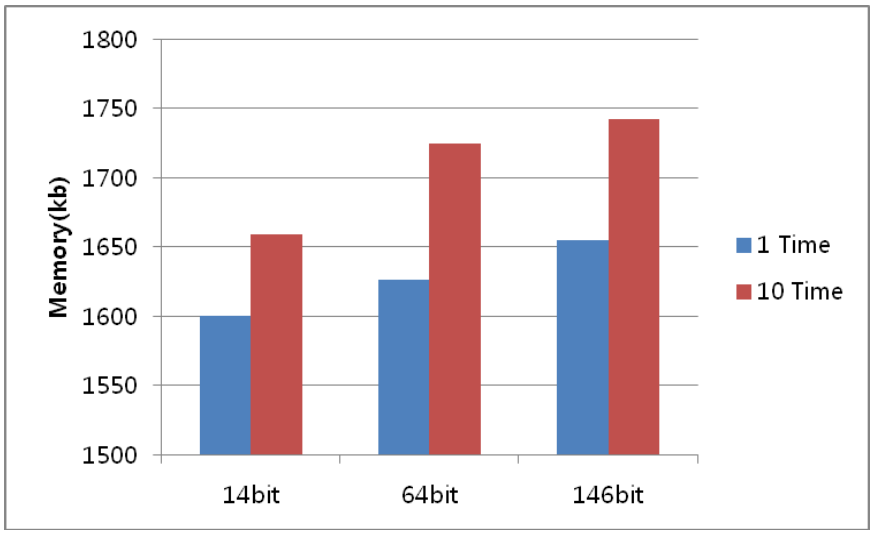

Figure 10. ECC Memory Measurement Data Graph

6. Conclusion

This study developed an effective homecare nursing Smartphone application by applying the security technology suitable for the mobile platform, using the Smartphone that is linked with the EMR and carried by the homecare nurse. Among many menus for homecare nursing OCS, the system, consisted of the most needed menus only for the homecare nursing according to the needs of the homecare nurse, provides a mobile service to conduct an effective homecare nursing. The homecare nurse does not need to carry the documents as she/he receives information about the patients' status in real time, can provide a tailored homecare nursing information to the patient after verifying the patient status; therefore, both the patient and the homecare nurse can enjoy the benefits of the differentiated service. However, this study found a limit that the homecare nurses are only authorized to use the service, and the doctors who are authorized for the prescription can only verify the records of the homecare nursing processes through the EMR. If the application is modified so the doctors can access to mobile for correcting the prescriptions or represcriptions in the future, its utilization is likely to be more popularized. Further, investigations will be conducted on the method for providing more tailored homecare nursing service linked with the personal

Acknowledgements

This research was supported by MSIP (the Ministry of Science, ICT and Future Planning), Korea, under the IT-CRSP(IT Convergence Research Support Program) (NIPA-2013-H0401-13-1001) supervised by the NIPA(National IT Industry Promotion Agency).

References

[1] W. A. Dombi, "Home care & Hospice Financial Manager Association: It Work for You With the transformation in health care in the United States that raised the importance of home care and hospice in both acute and chronic care settings, the financial management of the sectors has grown in importance and complexity",. HHFMA is recognition that financial managers are essential to the future success of home care and hospoce. Caring-Washington DC-, vol. 27, no. 9, **(2008)**, pp. 6-7.
[2] S. J. Kim, H. J. Kim, K. J. Lee and S. O. Lee, "Focus Group Method". Seoul. Hyun Moon Sa, **(2000)**.
[3] Y. Y. Jung, "A Study on the Effects of EMR on Nursing Efficiency", CJKMI, **(2000)**.

[4] D. Kimberly and S. Vicki, "Decision-Making and Nurse Care Management", Advanced in Nursing Science, vol. 27, no. 1, **(2004)**, pp. 32-34.
[5] http://www.kpha.or.kr/.
[6] H. Verkasalo, C. Lopez-Nicolas, F. MolinaCastillo and H. Bouwman, "Analysis of users and non-users of smartphone applications", Telematics and Informatics, vol. 27, **(2010)**, pp. 242-255.
[7] http://www.kfda.go.kr/
[8] Smart Doctor, http://www.smartdoctor.kr/.
[9] SKtelecom, http://www.sktelecom.com/.
[10] Y. L.Yeap and W. T. H. O'Brien, "Securing XML Web Services with Elliptic Curve Cryptography", Electrical and Computer Engineering, 2007. CCECE 2007, **(2007)**, pp.974-977.

Authors

Eun-Young Jung received M.S. degree in Health Informatics, Gachon University, Korea, in 2001. She received Ph.D. degree of Medical Informatics from Ajou University, Korea, in 2012. She is currently manager of U-Healthcare Center, Gachon University Gil Medical Center, Korea. Her research interests include u-healthcare, Telecare and Health IT, Virtual Reality simulation.

Sung-Jong Eun received the M.S. degree from Gachon University of South Korea in 2009 and the Ph.D candidate both in Computer Science from Gachon University in 2012. His research areas include Computer Graphics, Medical image processing, Healthcare service, BCI, AR.

Byoung-Hui Jeong received the M.S. degree from Incheon University of South Korea in 2010 and the Ph.D candidate both in Computer Science from Incheon University in 2013. His research areas include Artificial Intelligence, Software Architecture, Database design

Dong Kyun Park received B.S. degree from College of Medicine, Chungbuk National University, Korea, in 1992. He received M.S. and Ph.D. degree in College of Medicine from Inha University, Korea, in 2000 and 2003. He is currently Director of U-Healthcare Center and Medical Specialist of Gastroenterology in Gachon University Gil Medical Center, Korea. His research interests include u-healthcare, RFID, and Big data analysis.