Original Article

Healthc Inform Res. 2019 April;25(2):106-114.
https://doi.org/10.4258/hir.2019.25.2.106
pISSN 2093-3681 • eISSN 2093-369X

HIR
Healthcare Informatics Research

Privacy Enhanced Healthcare Information Sharing System for Home-Based Care Environments

Daniel Agbesi Dzissah[1], **Joong-Sun Lee**[1], **Hiroyuki Suzuki**[1], **Mie Nakamura**[2], **Takashi Obi**[1]

[1]Tokyo Institute of Technology, Yokohama, Japan
[2]Tokyo Medical and Dental University, Tokyo, Japan

Objectives: Home-based nursing care services have increased over the past decade. However, accountability and privacy issues as well as security concerns become more challenging during care provider visits. Because of the heterogeneous combination of mobile and stationary assistive medical care devices, conventional systems lack architectural consistency, which leads to inherent time delays and inaccuracies in sharing information. The goal of our study is to develop an architecture that meets the competing goals of accountability and privacy and enhances security in distributed home-based care systems. **Methods:** We realized this by using a context-aware approach to manage access to remote data. Our architecture uses a public certification service for individuals, the Japanese Public Key Infrastructure and Health Informatics-PKI to identify and validate the attributes of medical personnel. Both PKI mechanisms are provided by using separate smart cards issued by the government. **Results:** Context-awareness enables users to have appropriate data access in home-based nursing environments. Our architecture ensures that healthcare providers perform the needed home care services by accessing patient data online and recording transactions. **Conclusions:** The proposed method aims to enhance healthcare data access and secure information delivery to preserve user's privacy. We implemented a prototype system and confirmed its feasibility by experimental evaluation. Our research can contribute to reducing patient neglect and wrongful treatment, and thus reduce health insurance costs by ensuring correct insurance claims. Our study can provide a baseline towards building distinctive intelligent treatment options to clinicians and serve as a model for home-based nursing care.

Keywords: Home Health Nursing, Medical Information Exchange, Electronic Health Records, Privacy, Computer Security

Submitted: February 22, 2019
Revised: March 27, 2019
Accepted: April 3, 2019

Corresponding Author
Joong-Sun Lee
Tokyo Institute of Technology, R2-60 Yokohama-shi, Yokohama 226-8503, Japan. Tel: +81-0459245482, E-mail: j-lee@isl.titech.ac.jp (https://orcid.org/0000-0002-6976-6472)

I. Introduction

The Japanese government is aiming to reduce the burden of medical health insurance costs as the number of elderly patients with chronic diseases, such as cardiovascular problems, diabetes, and dementia, has been increasing rapidly [1]. These chronic diseases should be managed by promoting efficiency in home-based care [2,3]. This can be an alternative to increasing hospital-based medical care for senior citizens living alone [4]. The Japanese Ministry of Health, Labour, and Welfare issued guidelines for the secure management of medical information network systems [5]. It includes mobile access but does not mention home-based nursing care environments. As such, it remains an ambiguous topic for home-based nursing care.

It is becoming common for home care nurses to use smart devices and IoT connected equipment to monitor patient vital signs [6,7]. This interconnection results in a myriad of types of sensitive patient information, which are prone to data breaches [8]. It is a challenge to balance the competing goals of efficiency against security through trustworthy transactions and accessibility.

In this paper, we present a healthcare information sharing system for home-based nursing care environments. Our system uses the Japanese Public Key Infrastructure (JPKI) embedded in the Japanese National Individual Card so-called 'My Number Card'. The Japanese government announced that health insurance validation will also use the JPKI platform starting in 2020 [9,10]. As of July 2018, 14 million cards have already been issued with the JPKI platform [11]. Primary home-based care provides a level of independence at home and improves elderly quality of life. The use of smart devices and applications with body sensors has increased [12]. Cloud computing technologies and context-aware systems have been used for ambient assisted living [13] and remote healthcare [14,15]. Context-aware information monitoring is a key to home-based nursing care systems because it covers the situational context of the accumulated data and provides real-time personalized healthcare services suited to user needs [16]. Context awareness is widely used in modern big data analytics [17]. Sensors generate large amounts of data; however, they lack the processing power to perform essential monitoring and secure data transmission. The Japanese Public Key (JPKI) in the 'My Number Card' is used to verify the card owner's identity on the internet. The government is also considering issuing a second JPKI certificate for a user's mobile device which links a phone to its owner.

Our system also uses the Healthcare PKI (HPKI) to identify and validate the status of medical personnel through the *hcRole* included in the HPKI certificate. The *hcRole* attribute represents one of the twenty-four types of healthcare and welfare qualifications or one of the five types of administrative functions so far. The HPKI already is a global standard, ISO 17090, which defines the standard for Health Informatics-PKI [18,19]. From interviews with nurses, we gained insight into the specific challenges to security and privacy in home-based nursing care environments. We briefly discuss each of these concerns below.

(1) Leakage of private information: Privacy leakage is a critical issue in home-based nursing environments [20]. This may hinder the processing and exchange of health data for diagnosis and treatment.

(2) Unintentional errors and malicious attacks [21]: Based on interviews, we realized that physicians might often forget to log out of terminals or smart equipment in a patient's home, which leads to the risk of unauthorized parties gaining access to sensitive health information.

(3) Health data access control: IoT devices, such as wearables and sensors, using cloud services offer numerous advantages, including significant storage and computation capabilities. However, managing access control on these devices is challenging. Moreover, outsourcing third-party services would also introduce security concerns [22].

The objective of this study is to develop an architecture that achieves the competing goals of providing accountabil-

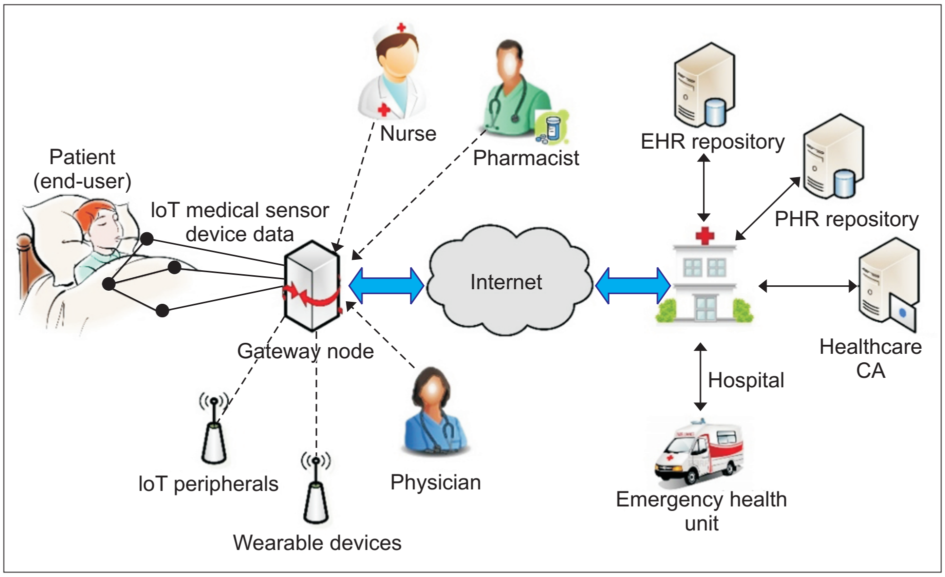


Figure 1. Overview of a distributed home-based healthcare environment.

ity and privacy and enhancing security in distributed home-based care systems. To accomplish our purpose, we designed an architecture that improves the reliability of data exchange between healthcare personnel. To generate a trustworthy source of visit records, we use a system that supplies concrete evidence that healthcare personnel visited a patient's residence. Our system provides a security layer that supports accountability by leveraging context-aware services so that it can react intelligently according to the physical and logical environment.

II. Methods

Doctors and medical care providers (often nurses or licenced caregivers) take risks rooted in data transmission and access to sensitive medical data across institutions in a distributed home-based healthcare environment (Figure 1). To address this situation, we propose a home-based information-sharing architecture (Figure 2) in which context awareness is introduced in the system.

1. Privacy-Enhancing Trust Levels

User authentication is the first step in protecting sensitive medical data. We employ the state-run JPKI to serve as a trusted mechanism with high reliability in our system. The second step is user authorization, which employs user access roles based on the HPKI. Thus, we leverage the JPKI and HPKI robust security features. The third step entails data resource processing, which is managed by a context-aware system built on a gateway to enhance privacy protection and data security as depicted in Figure 3. The gateway securely connects a patient's home to a remote service provider through the virtual private network (VPN). To accomplish the steps correctly, all the users have the JPKI and medical personnel the HPKI certificates. The mobile devices used in this system have to be linked to registered medical staff members. This is done by installing a PKI certificate in the trust execution environment of the devices. The primary function of registration allows the system to associate a device with its owner's identity. It also ensures that the gateway node is linked to a secure near-field communication (NFC) tag with the JPKI holder's account. The government is con-

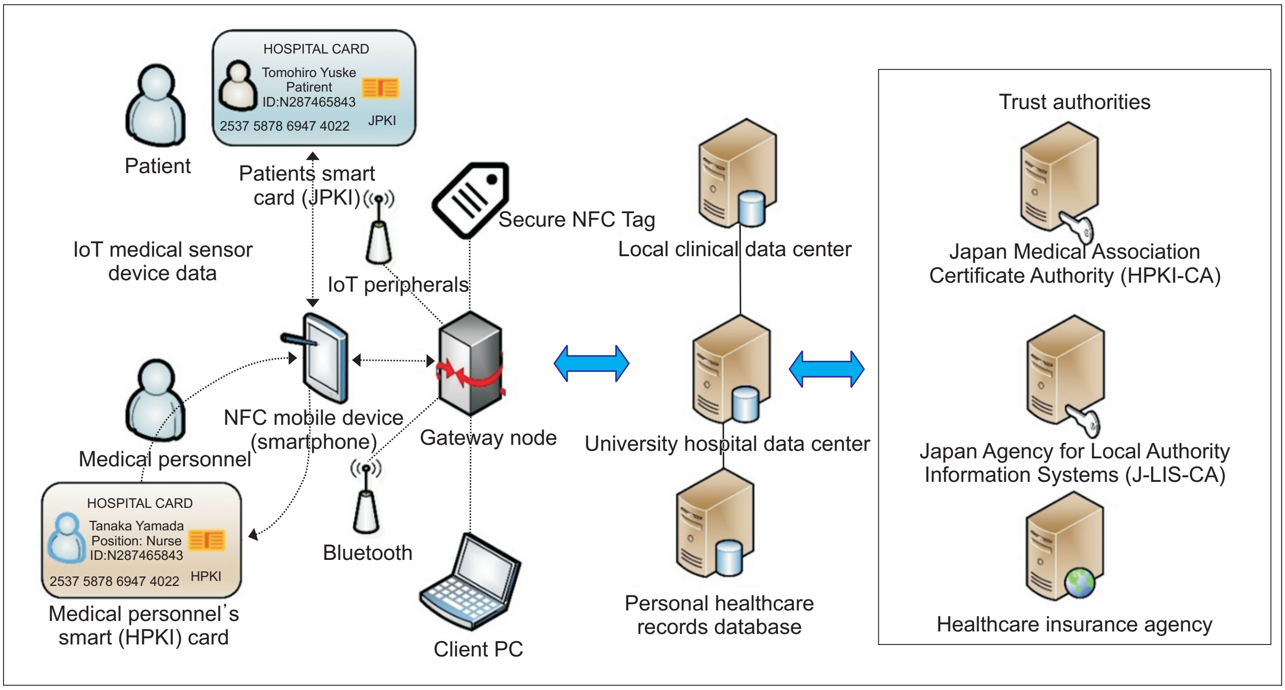

HOSPITAL CARD
Tomohiro Yuske
Patirent
ID:N287465843
2537 5878 6947 4022
JPKI
Patient
Patients smart card (JPKI)
Secure NFC Tag
IoT medical sensor device data
IoT peripherals
Local clinical data center
Trust authorities
Japan Medical Association Certificate Authority (HPKI-CA)
NFC mobile device (smartphone)
Gateway node
University hospital data center
Medical personnel
HOSPITAL CARD
Tanaka Yamada
Position: Nurse
ID:N287465843
2537 5878 6947 4022
HPKI
Bluetooth
Japan Agency for Local Authority Information Systems (J-LIS-CA)
Medical personnel's smart (HPKI) card
Client PC
Personal healthcare records database
Healthcare insurance agency

Figure 2. Proposed home-based information-sharing architecture.

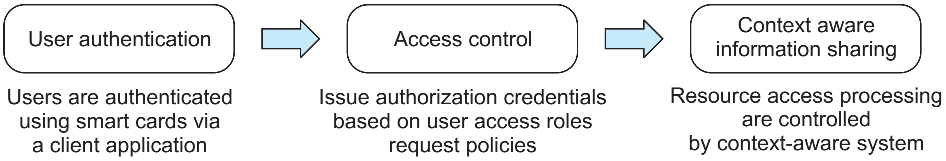

User authentication
Users are authenticated using smart cards via a client application
Access control
Issue authorization credentials based on user access roles request policies
Context aware information sharing
Resource access processing are controlled by context-aware system

Figure 3. Context-aware authentication trust levels.

sidering issuing JPKI certificates for mobile device owners soon.

2. Context-Aware Management

When healthcare information service is accessed from home-based environments, user access is provided by a context-aware system that constrains access to services. The system uses context resources and data to provide relevant information and services to the users (medical personnel). The context-aware middleware comprises two modules: the client context manager (client CM) and the gateway context manager (gateway CM). The client CM comes wrapped in the Android application. It acquires and processes data from sensory networks in the user's domain and transmits it to the gateway CM. The gateway CM processes context information based on pre-defined context policies for each user as described later in this section. It also handles alert management and context instances for each session. The process is summarized here and is presented in Figure 4, where the numbering corresponds to the flow.

- Resource access request (1): A user (U) sends an access request based on context policy to authenticate to the service provider. If the user can meet the context policy requirements, then he or she can obtain a session from the session manager.
- Attribute and credential authentication (2)-(3): Otherwise, user attributes need to be authenticated and validated with the service provider access control as described later regarding the general authentication flow (see Section III-3). The system requests user credential verification based on the privacy-enhancing trust levels, in this case using the PKI card. Policy-enforcement module definitions are based on the *hcRole* coded into the HPKI cardholder's policy settings. The remote authentication service issues authenticated attribute credentials based on the *hcRole* and authorization from patient credentials.
- Assigning client sessions (4): The access manager (AM) maintains each session by assigning a temporary client session token. It assign tokens to the client CM for each user session-based access rights until ended by users or the policy-enforcement module.
- Context processing (5)-(6): It enforces policies based on information supplied by the context provider module, which uses metrics to establish the device's context types. Context collection is determined by the access policy. Context type may vary depending on its source, from a verified user's device context providers. The collected context is time stamped and digitally signed in to identify the context source.
- Context validation (7): The gateway node confirms and validates pre-defined context and runtime contextual information gathered from the user's smartphone. The context verifier (CV) accumulates all the contextual data to confirm whether the context satisfies the conditions of the policy. The CV sends an encoded time-stamp and challenge response to the context provider (CP) after validation. Thus, engineers examining the system security requirements can appropriately decide which context types will be used to define access.
- Policy validation (8): The policy verifier processes the predefined context policies provided by the policy decision point (PDP). The context data filter characterizes a policy

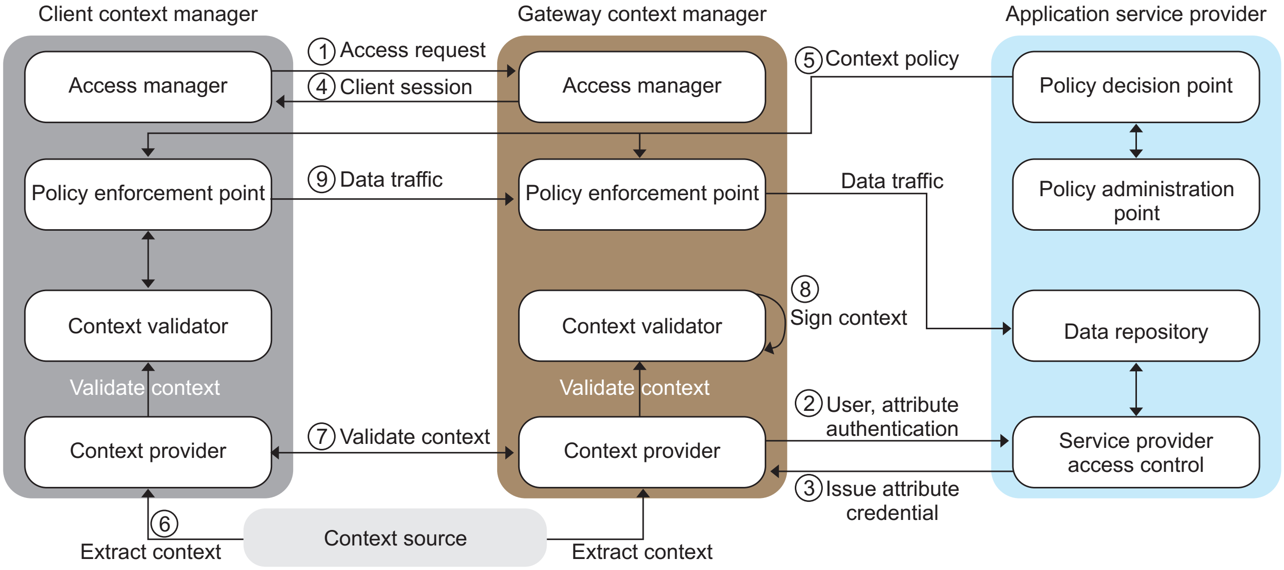


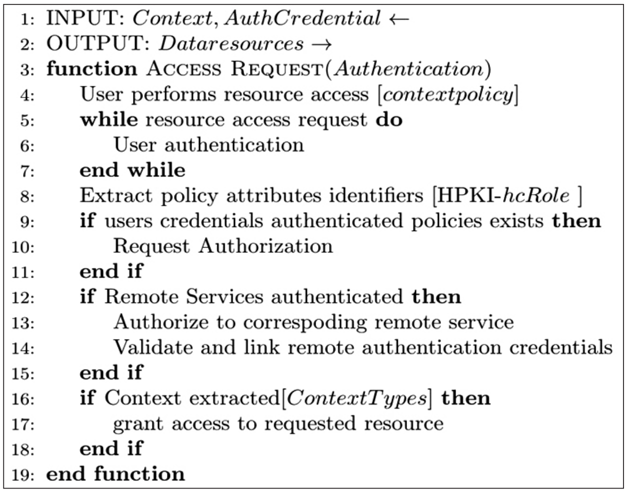
Figure 4. Overview of the context-aware modules.

enforcement point (PEP). It evaluates context data from the CP against the compiled policy rules, and the calls to request services are executed as user actions. Actions may include downloading files, updating healthcare information, and accessing limited data resources from other care providers. Context-aware policies are applied at user-end points of the client CM. These policies are maintained for every active user session to enable or reject access for a user to specific healthcare information resources. Further steps involve ordinary authorization, which is described in Section III-3 in relation to trust-level credential authentication and authorization. The corresponding context policy is based on Figure 5.

For example, we will consider a policy that ensures that nursing care staff receive notifications on a mobile app to validate the current session associated with a particular patient. Whenever a change in location occurs based on the predefined context type (Table 1), the policy makes each information session end by logging the user off. The status of an information session changes with every variation in context metrics. For example, the policy prevents a caregiver leaving a residence and forgetting to sign out of active sessions. Thus, exposure of vital medical information or inconsistent logging of access control data can be avoided.

3. Trust-Level Credential Authentication and Authorization

To initiate any transaction through the gateway, users must also establish a secure connection between the mobile device and the gateway. Figure 6 presents the authentication and authorization process between mobile devices in our system using context management. This process validates credential information provided by the user (U) against the repository of enrolled users. This process is based on authorization information, such as a user's identity, services being requested, and the attributes of the requester. If all checks are passed, an authentication token is issued, and the trust-level credential used (HPKI/JPKI) is digitally signed. Upon establishing a connection via the gateway, the CP in the client application (Section III-2) requests that context information be synchronized through the trusted gateway node. Once verification is securely completed, the healthcare provider has permission to access medical data and records. However, the broadness of their access is determined by the attributes of their assigned *hcRole* and the authorization based on the patient JPKI. The patient presents his or her smart card and enters the smart card personal identification number (PIN) code to sign the authentication challenge. If deemed necessary in special cases, the secure internal PIN-less authentication mechanism, which was introduced for JPKI cards, allows cardholders (here, patients or next of kin) to execute the authentication process that is employed in secure IC card transactions [20]. By executing the authentication process, the patient allows medical personnel to access the relevant medical information and verifies the status of his or her health insurance.



```
INPUT: $Context, AuthCredential \leftarrow$
OUTPUT: $Dataresources \rightarrow$
function ACCESS REQUEST($Authentication$)
    User performs resource access [$contextpolicy$]
    while resource access request do
        User authentication
    end while
    Extract policy attributes identifiers [HPKI-$hcRole$ ]
    if users credentials authenticated policies exists then
        Request Authorization
    end if
    if Remote Services authenticated then
        Authorize to correspoding remote service
        Validate and link remote authentication credentials
    end if
    if Context extracted[$ContextTypes$] then
        grant access to requested resource
    end if
end function
```

Figure 5. Context-aware policy management algorithm.

III. Results

1. System Prototype

A prototype of the system was deployed for testing on a local network with an Android smartphone as the medical personnel terminal, and a Raspberry Pi as the gateway node. Figure 7 depicts a screenshot of a 'request for action' notification. The trust-authentication services were emulated by Linux machines functioning as the CA's of HPKI and JPKI separately besides the health insurance agency. Moreover, data center repositories were established on the same machines. Context-aware middleware modules were implemented in both the client devices and the gateway node. In the prototype, client applications were developed

Table 1. Context types and operation values

Context type	Value
Close proximity (Wi-Fi, Bluetooth, NFC)	Device identifiers, unique address
Location (GPS, Wi-Fi)	Coordinates, fine coordinates
Time (*PTP, NTP)	Time (high accuracy)
User credentials (smart card PKI certificates)	User identifier

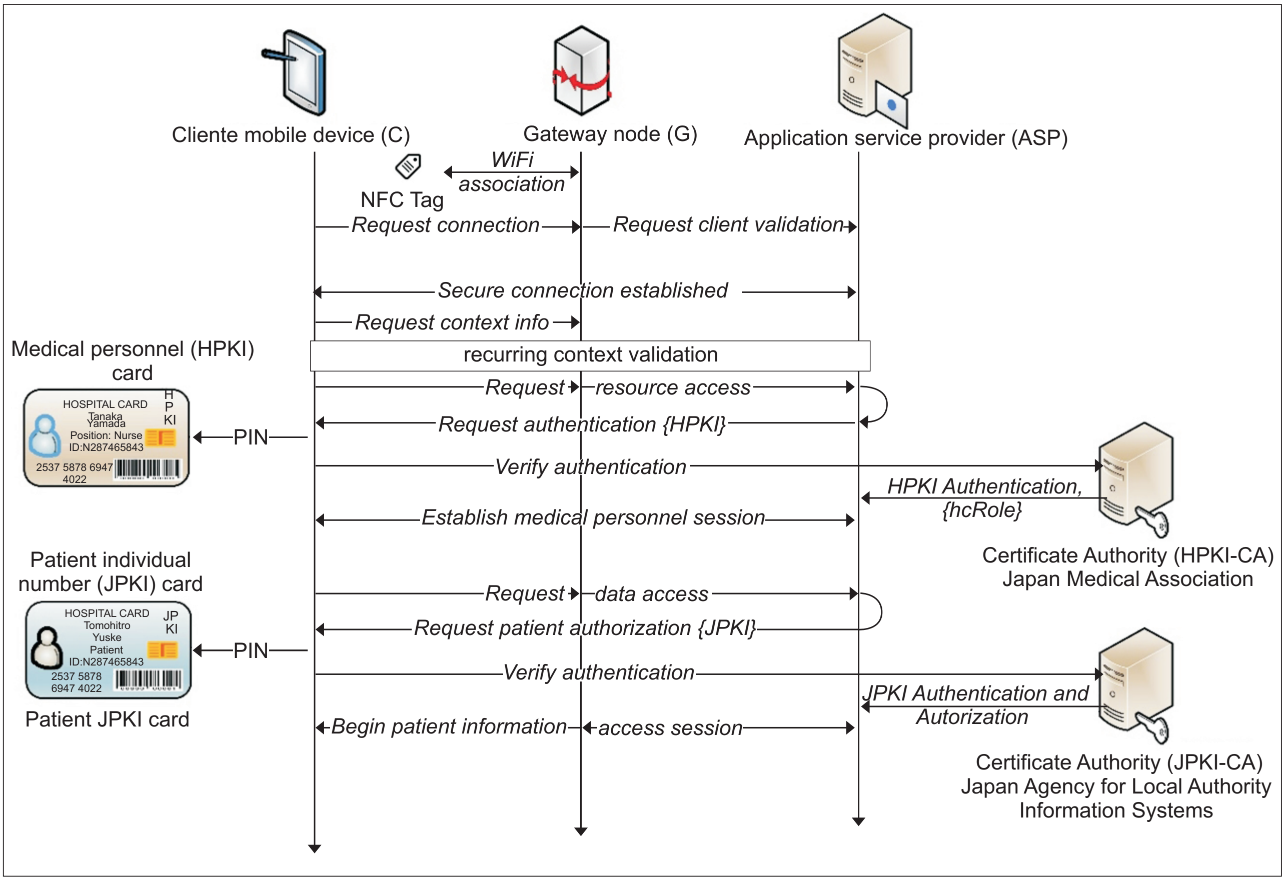
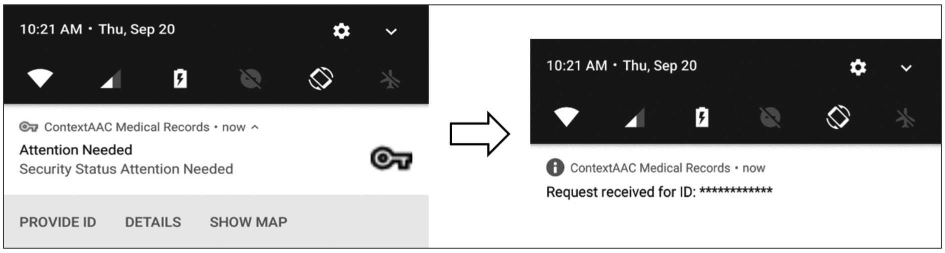

Cliente mobile device (C)
Gateway node (G)
Application service provider (ASP)
NFC Tag
WiFi association
Request connection
Request client validation
Secure connection established
Request context info
recurring context validation
Medical personnel (HPKI) card
HOSPITAL CARD
Tanaka Yamada
Position: Nurse
ID:N287465843
2537 5878 6947 4022
HPKI
PIN
Request
resource access
Request authentication {HPKI}
Verify authentication
HPKI Authentication, {hcRole}
Establish medical personnel session
Certificate Authority (HPKI-CA)
Japan Medical Association
Patient individual number (JPKI) card
HOSPITAL CARD
Tomohitro
Yuske
Patient
ID:N287465843
2537 5878 6947 4022
JPKI
PIN
Request
data access
Request patient authorization {JPKI}
Verify authentication
JPKI Authentication and Autorization
Patient JPKI card
Begin patient information
access session
Certificate Authority (JPKI-CA)
Japan Agency for Local Authority Information Systems

Figure 6. Overall authentication and authorization flow.


10:21 AM • Thu, Sep 20

ContextAAC Medical Records • now

Attention Needed

Security Status Attention Needed

10:21 AM • Thu, Sep 20

ContextAAC Medical Records • now

Request received for ID: ************

Figure 7. Request for action notification.

for an Android platform, which gave physicians, nurses, or medical caregivers remote access to the healthcare information system. The patient platform was implemented with the gateway using a Raspberry Pi, which was connected to the Internet and the patient's TV via a set-top box. This smart TV-like solution is intended to be usable by the elderly who may not be adept with technology. This also supports the concept of a personal electronic health journal (health diary) to enable patients to communicate and interact with doctors, nurses, and caregivers.

2. Prototype Analysis

We evaluated the prototype system with the following aims: (1) to investigate whether the system satisfies the policy of the access control and privacy enhancement which permits access from authorized users and restricts unauthorized users; (2) to check whether the actual surrounding environment context, such as the geo-location, through the mobile devices is trustworthy and then the context-aware decision is accurately made in collaboration with the PEP; (3) to examine how the context-aware manager processes the PEP in case of policy changes by the policy administration point through the PDP; and (4) to simulate a situation using the two PKI cards (HPKI and JPKI) in our experimental setting to predict real situations to improve usability.

Tests were conducted in a closed environment with six users, including two patients, a registered nurse who was also a licenced home care giver, and general care staff. The results will not wholly reflect those of an actual working environment. The system functionality may require specific modification to suit organizational privacy policies and the legal requirements set by the governing authority.

Processing times for provider authentication and patient authorization need to be shorter. In our system, the average time for the client-gateway association is nearly 6.42 seconds, including user's (patient and care provider) PIN inputs and the initial NFC tag handover to the Wi-Fi connection. In actual situations, this may take longer but not intolerable lengths of time because user PIN inputs take time and remote services perform the authentication and authorization. The latency of NFC tag read-write is about 5.34 seconds during the initial connection of the mobile device to the nearest gateway. Using the NFC tag enhances the workflow of users and integrates it into a seamless access control process. It also helps improve user interaction by eliminating user input tasks.

IV. Discussion

We developed a context-aware architecture for supporting nursing care providers in home-based nursing environments. We use a secure NFC authentication mechanism that implements a secure channel by encrypting sensitive context data during transmission in the network. This architecture conducts authentication and authorization to access a specified patient's data using a context-aware gateway node. Thus, when a nurse or doctor visits the wrong patient's home, it rejects authorization based on the context sources of the geo-location, such as GPS data and Wi-Fi access point. Even where contextual information for the client is being spoofed or is misleading, the context verifier periodically justifies contextual sources and performs validation by comparing context data from the gateway and the mobile devices of the medical care giver. If the client's location varies significantly from the gateway in use, it requests the access manager to end the session by automatically logging off. By utilizing the JPKI and HPKI mechanisms, the identities of patients and medical personnel can be confirmed, satisfying the government requirement regarding security and privacy protection. Patients' use of their JPKI cards expresses explicit permission to access their data. This also serves as the granting of informed consent before medical procedures. Patient privacy is guaranteed by allowing access to information only by medical personnel with authorized roles according to the HPKI *hcRole*. Lee et al. [7] proposed a service-oriented framework for remote medical services focused on the IoT environment using a similar method of context awareness. However, our research systematically approaches the introduction of context awareness in home-based nursing care environments. Some preliminary work was carried out in which the HPKI was introduced for access control of web-based clinical information in combination with the policy control of personal computers [19]. Users are authenticated using device IDs and passwords. Although this method is practical, our approach is stronger and is expected to resist common attacks, such as user impersonation password guessing and stolen verifier attacks.

In our research, we introduced context-awareness in home-based nursing environments. The proposed system generates electronic evidence of a medical visit to a patient's home through authentication and authorization using the JPKI and the HPKI, respectively. The authentication process employs digital signatures for all patients and healthcare professionals, which is essential during insurance claims verification. Our approach ensures on-the-spot authorization through the patient's consent to access their data, while maintaining the patient's privacy. In our system design, we focused on the user-friendly validation of the context without the leaking of sensitive user information. Our proposed approach complies with the Japanese Act on Protection of Personal Information and the Health Insurance Portability and Accountability Act (HIPPA). This approach makes the system extensible to other global regulatory requirements for home-based nursing care systems. Our experimental results show that the authentication and authorization architecture is feasible to deploy in IoT network environments. However, the main limitation of our work is that the architecture is based on the premise that patients can use the JPKI and medical personnel the HPKI. The JPKI can be replaced with PKI-based ID cards. The HPKI is already standardized by the ISO, but it is only available in Japan so far.

To make our system user-friendly through BYOD, we apply a method that filters malformed context information from user's devices. The home gateway serves as a trusted source for gathering information for monitoring a patient's vital signs through wearable devices. Our study can provide a baseline towards building distinctive intelligent treatment options to clinicians and serve as a model for home-based nursing care. We believe that our research will contribute to reducing patient neglect and wrongful treatment. It also can reduces health insurance costs by ensuring correct insurance claims. We are confident that the proposed system will enhance patient and medical care provider privacy by enforcing access control.

https://doi.org/10.4258/hir.2019.25.2.106

Conflict of Interest

No potential conflict of interest relevant to this article was reported.

ORCID

Daniel Agbesi Dzissah (http://orcid.org/0000-0002-4484-3814)
Joong-Sun Lee (http://orcid.org/0000-0002-6976-6472)
Hiroyuki Suzuki (http://orcid.org/0000-0002-5028-5388)
Mie Nakamura (http://orcid.org/0000-0001-6706-2247)
Takashi Obi (http://orcid.org/0000-0001-9430-2728)

References

1. Japanese Nursing Association. Nursing for the older people in Japan. 2. Nursing for the Older People: Current situation and challenges [Internet]. Tokyo, Japan: Japanese Nursing Association; 2013 [cited at 2019 Apr 1]. Available from: https://www.nurse.or.jp/jna/english/pdf/info-02.pdf.
2. Obi T, Ishmatova D, Iwasaki N. Promoting ICT innovations for the ageing population in Japan. Int J Med Inform 2013;82:e47-62.
3. Maruyama I. The new direction of primary care in Japan. Japan Med Assoc J 2013;56(6):465-7.
4. Fujimoto M, Miyazaki K, von Tunzelmann N. Complex systems in technology and policy: telemedicine and telecare in Japan. J Telemed Telecare 2000;6(4):187-92.
5. Ministry of Health, Labour and Welfare. Guidelines for the security management of health information systems edition 4.2. Tokyo, Japan: Ministry of Health, Labour and Welfare; 2013.
6. Park A, Chang H, Lee KJ. Action research on development and application of Internet of Things services in hospital. Healthc Inform Res 2017;23(1):25-34.
7. Lee JD, Yoon TS, Chung SH, Cha HS. Service-oriented security framework for remote medical services in the Internet of Things environment. Healthc Inform Res 2015;21(4):271-82.
8. Kumar P, Lee HJ. Security issues in healthcare applications using wireless medical sensor networks: a survey. Sensors (Basel) 2012;12(1):55-91.
9. Fukuda K, Obi T, Nagata K, Suzuki H, Taira N, Ohyama N. A study on utilizing the public certification service for individuals in the qualification of medical insurance. In: 2016 Life Intelligence and Office Information Systems (LIOS); Tokyo, Japan. p. 1-5.
10. Obi T, Fujita K, Ohyama N. A study on functionality expansion and medical application of new public Certification Service for Individuals. In: Proceedings of the 31st Symposium on Cryptography and Information Security (SCIS); 2014 Jan 21-24; Kagoshima, Japan. p. 29-34.
11. Ministry of Internal Affairs and Communication. About public personal certification system. Tokyo, Japan: Ministry of Internal Affairs and Communication; 2018.
12. Sufi F, Khalil I, Tari Z. A cardiod based technique to identify cardiovascular diseases using mobile phones and body sensors. In: Proceedings of 2010 Annual International Conference of the IEEE Engineering in Medicine and Biology; 2010 Aug 31-Sep 4; Buenos Aires, Argentina. p. 5500-3.
13. Dey AK. Understanding and using context. Pers Ubiquitous Comput 2001;5(1):4-7.
14. Hristova A, Bernardos AM, Casar JR. Context-aware services for ambient assisted living: a case-study. In: Proceedings of 2008 First International Symposium on Applied Sciences on Biomedical and Communication Technologies; 2008 Oct 25-28; Aalborg, Denmark. p. 1-5.
15. Viswanathan H, Chen B, Pompili D. Research challenges in computation, communication, and context awareness for ubiquitous healthcare. IEEE Commun Mag 2012;50(5):92-9.
16. Paganelli F, Spinicci E, Giuli D. ERMHAN: a context-aware service platform to support continuous care networks for home-based Assistance. Int J Telemed Appl 2008;2008:867639.
17. Sun J, Reddy CK. (2013, August). Big data analytics for healthcare. In: Proceedings of the 19th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining; 2013 Aug 11-14; Chicago, IL. p. 1525.
18. International Standardization Organization. ISO 17090-3:2008 Health informatics - Public key infrastructure [Internet]. Geneva, Switzerland: International Standardization Organization; 2008 [cited at 2019 Apr 1]. Available from: https://www.iso.org/obp/ui/#iso:std:iso:17090:-3:ed-1:v1:en.
19. Tanaka K, Yoshida M, Yamamoto R. Secure remote access for web based clinical information system using policy control of pcs and healthcare PKI authentication. In: Proceedings of the 12th World Congress on Health (Medical) Informatics, Building Sustainable Health Systems; 2007 Aug 20-24; Brisbane, Australia. p. 1644-6.
20. Tripathi MM, Joshi NK. Big data issues in medical

healthcare. In: Intelligent Communication, Control and Devices. Singapore: Springer; 2018, p. 1757-65.

21. Choi HK, Shin KE, Kim H. A healthcare information system for secure delivery and remote management of medical records. IEICE Trans Inf Syst 2016;99(4):883-90.

22. Bauer AM, Rue T, Munson SA, Ghomi RH, Keppel GA, Cole AM, et al. Patient-oriented health technologies: patients' perspectives and use. J Mob Technol Med 2017;6(2):1-10.